Algebra

Xiaolong Pan

March 21, 2023

Contents

1 General topology **15**

1.1 Topological structures . . . 15
- 1.1.1 Topological spaces . . . 15
- 1.1.2 Base of topologies . . . 16
- 1.1.3 Neighborhoods . . . 19
- 1.1.4 Closure, interior and boundary . . . 20

1.2 Continuous functions . . . 22
- 1.2.1 Semicontinuity . . . 22
- 1.2.2 Continuous functions . . . 24
- 1.2.3 Initial topologies . . . 27
- 1.2.4 Final topologies . . . 28
- 1.2.5 Subspaces of a topological space . . . 30

1.3 Quotient spaces and quotient maps . . . 32
- 1.3.1 Quotient spaces and maps . . . 32
- 1.3.2 Quotient of a subspace . . . 36
- 1.3.3 Hausdorff condition of quotient spaces . . . 37
- 1.3.4 Direct limit of topological spaces . . . 38

1.4 Product of topological spaces . . . 39
- 1.4.1 Product spaces . . . 39
- 1.4.2 Sections and projections . . . 41
- 1.4.3 Inverse limit of topological spaces . . . 43

1.5 Connectedness . . . 44
- 1.5.1 Connected spaces . . . 44
- 1.5.2 Path connectedness . . . 48
- 1.5.3 Components and locally connectedness . . . 51
- 1.5.4 Path components . . . 53

1.6 Countablity and separation axoims . . . 54

1.7 Nets and filters . . . 55
- 1.7.1 Nets . . . 55
- 1.7.2 Filters . . . 57
- 1.7.3 Construction of filters . . . 60
- 1.7.4 Limit of filters . . . 62

1.8 Compactness . . . 64
- 1.8.1 Limit point compactness and sequencially compactness . . . 66
- 1.8.2 General characterization of compactness . . . 69
- 1.8.3 Inverse limit of compact spaces . . . 70

1.8.4 Aezelá-Ascoli theorem . . . 71
1.8.5 Compactification . . . 74
1.9 Local compactness . . . 77
1.9.1 Continuous functions . . . 79
1.9.2 One-point compactification . . . 81
1.9.3 Stone-Weierstrass theorem . . . 83
1.9.4 Metrizability . . . 86
1.10 Proper maps . . . 87
1.10.1 Proper maps . . . 87
1.10.2 Proper maps . . . 88
1.11 Baire Spaces . . . 91
1.11.1 Nowhere dense sets and meager sets . . . 91
1.11.2 Baire category theorem . . . 95
1.12 Topological manifolds . . . 96
1.12.1 Definition of manifolds . . . 96
1.12.2 Manifolds with boundary . . . 98
1.12.3 Adjunction spaces . . . 100
1.13 Paracompactness . . . 103
1.13.1 Paracompact spaces . . . 103
1.13.2 Partitions of unity . . . 109

2 Uniform structures **113**
2.1 Uniform spaces . . . 113
2.1.1 Uniformly continuous functions . . . 117
2.1.2 Construction of uniform structures . . . 118
2.2 Complete spaces . . . 121
2.2.1 Cauchy filters . . . 121
2.2.2 Complete spaces . . . 124
2.2.3 Product and inverse limit of complete spaces . . . 125
2.2.4 Extension of uniformly continuous functions . . . 128
2.2.5 Completion of uniform spaces . . . 129
2.2.6 The Hausdorff space associated with a uniform space . . . 131
2.2.7 Completion of subspaces and product spaces . . . 132
2.3 Compact space and uniform spaces . . . 133
2.3.1 Uniformity for compact Hausdorff spaces . . . 133
2.3.2 Compactness of uniform spaces . . . 135

3 Topological groups and rings **137**
3.1 Topological groups . . . 137
3.1.1 Topologies on groups . . . 137
3.1.2 Topological subgroups . . . 141
3.1.3 Group actions . . . 143
3.1.4 Product and quotient of topological groups . . . 147
3.1.5 $\mathcal{S}$-topologies . . . 152
3.1.6 Metrizability . . . 154

3.2 Complete topological groups . . . 156
3.2.1 Uniformity on topological groups . . . 157
3.2.2 Complete groups . . . 158
3.2.3 Completion of Hausdorff groups . . . 160
3.2.4 Completeness of commutative topological groups . . . 162
3.3 Topological group with operators, topological rings, modules and fields . . . 163
3.3.1 Topological group with operators . . . 163
3.3.2 Topological direct sum of stable subgroups . . . 164
3.3.3 Topological rings and modules . . . 165
3.3.4 Topological division ring and fields . . . 170
3.3.5 Inverse limits of topological groups and rings . . . 171

4 Topologies encountered in algebraic geometry 179
4.1 Irreducibility . . . 179
4.1.1 Irredicible topological spaces . . . 179
4.1.2 Noetherian topological spaces . . . 181
4.1.3 Generic points . . . 183
4.2 Krull dimension . . . 183
4.2.1 Krull dimension of a topological space . . . 183
4.2.2 Codimension of a closed subset . . . 185

5 Integral domains 189
5.1 Prime and irreducible elements . . . 189
5.2 Domains with factorizations . . . 190
5.3 Greatest common divisors and Bézout domains . . . 191
5.4 Unique factorization in polynomial rings . . . 194
5.5 A prime ideal principle . . . 199
5.6 Some results on UFDs and PIDs . . . 201
5.7 Exercise . . . 204

6 Chain conditions 207
6.1 General properties . . . 207
6.2 Noetherian rings . . . 211
6.3 Artin rings . . . 212
6.4 Exercise . . . 215

7 Linear algebras 219
7.1 Modules and diagrams . . . 219
7.1.1 Finitely generated modules . . . 219
7.1.2 Exact sequence and the snake lemma . . . 221
7.1.3 Exercise . . . 225
7.2 Flat modules . . . 228
7.2.1 M-flat modules . . . 228
7.2.2 Flat modules . . . 230
7.2.3 Intersection properties . . . 234
7.2.4 Extension of scalars and flatness . . . 235

7.2.5 Finitely presented modules . . . 236
7.2.6 Structure of flat modules . . . 244
7.3 Faithfully flat modules . . . 245
7.3.1 Extension of scalars and faithfully flatness . . . 247
7.3.2 Faithfully flat rings . . . 249
7.4 Injective modules . . . 252
7.4.1 Injective modules . . . 252
7.4.2 Injective modules and cogenerators . . . 254
7.4.3 Injective hull of modules . . . 256

8 Homological algebras for modules 261
8.1 Complexes of modules . . . 261
8.1.1 Complexes of A-modules . . . 261
8.1.2 Long exact homological sequence . . . 264
8.1.3 Homotopies . . . 266
8.1.4 Splitting complexes . . . 267
8.1.5 Cone and cylinder of a morphism of complexes . . . 269
8.1.6 Euler-Poincaré characteristic . . . 272
8.1.7 The de Rham complex . . . 274
8.2 Resolutions . . . 277
8.2.1 Resolutions of modules . . . 277
8.2.2 The canonical free resolution . . . 278
8.2.3 The canonical injective resolution . . . 279
8.2.4 Finitely generated resolutions . . . 280
8.2.5 Minimal projective resolutions . . . 281
8.2.6 Graded resolutions . . . 282
8.2.7 The standard resolution . . . 282
8.2.8 Resolutions and Grothendieck groups . . . 284
8.3 Tensor product . . . 284
8.3.1 Tensot product of complexes . . . 284
8.3.2 Tensor products and homotopies . . . 287
8.3.3 The twisted product and its properties . . . 289
8.3.4 The long exact sequence of twisted products . . . 292
8.3.5 Künneth formula . . . 294
8.4 Modules of extensions . . . 296
8.4.1 The Hom complex of complexes . . . 296
8.4.2 Hom complex and homotopies . . . 298
8.5 Koszul complex . . . 299
8.5.1 The Koszul complex associated with a linear form . . . 299
8.5.2 The canonical Koszul complex of $S(E)$ . . . 303
8.5.3 Koszul complexes and alternating maps . . . 304
8.5.4 Koszul complexes and completely secant sequences . . . 306
8.5.5 Extension class associated with a regular sequence . . . 313

9 Field Theories 317

9.1 Field extensions . . . 317
9.1.1 Basic definitions of field extensions . . . 317
9.1.2 Simple, finite, and algebraic extensions . . . 319
9.1.3 Algebraic closure . . . 327
9.1.4 Embeddings and their extensions . . . 329
9.1.5 Splitting fields and normal extensions . . . 332
9.1.6 Separable extensions and linearly disjointness . . . 336
9.1.7 Exercise . . . 354
9.2 Galois theory . . . 358
9.2.1 Galois connections . . . 358
9.2.2 The Galois correspondence . . . 363
9.2.3 Closed elements in the Galois correspondence . . . 366
9.2.4 The Krull topology on Galois group . . . 369
9.2.5 Normal subgroups and normal extensions . . . 372
9.2.6 Galois groups of lifting and composites . . . 376
9.2.7 Exercise . . . 380
9.3 Applications of Galois theory . . . 381
9.3.1 The Galois group of a polynomial . . . 382
9.3.2 The Galois groups of some polynomials . . . 388
9.3.3 Geometric impossibilities . . . 391
9.3.4 The fundamental theorem of algebra . . . 396
9.3.5 Finite fields . . . 396
9.3.6 Cyclotomic polynomials and fields . . . 401
9.3.7 Cyclic extensions . . . 404
9.3.8 Solvable and radical extensions . . . 410
9.3.9 Solvability of polynomial equations by radicals . . . 413
9.3.10 Exercise . . . 416
9.4 Transcendental extensions . . . 421
9.4.1 Transcendental basis . . . 421
9.4.2 Simple transcendantal extension and Lüroth's theorem . . . 426

10 Localizations **431**
10.1 Prime ideals and maximal ideals . . . 431
10.1.1 Prime ideals . . . 431
10.1.2 Nilradical and Jacobson radical . . . 432
10.1.3 Coprime ideals . . . 433
10.1.4 Local rings and semilocal rings . . . 434
10.1.5 Operations on ideals . . . 436
10.1.6 Exercise . . . 439
10.2 Rings and modules of fractions . . . 442
10.2.1 Definition of rings of fractions . . . 442
10.2.2 Modules of fractions . . . 445
10.2.3 Change of multiplicative subset . . . 448
10.2.4 Properties of the localization operation . . . 452
10.2.5 Ideals under localization . . . 453

10.2.6 Modules of fractions of tensor products and Hom sets . . . 456
10.3 Local rings and passing from local to global . . . 457
10.3.1 Local rings . . . 457
10.3.2 Modules over a local ring . . . 459
10.3.3 Passing from local to global . . . 462
10.4 The spectrum of a ring . . . 465
10.4.1 The space Spec(A) . . . 465
10.4.2 Functoriality of the spactrum . . . 470
10.4.3 The support of a module . . . 473
10.4.4 Clopen subsets of the spectrum . . . 476
10.4.5 Glueing properties of localization . . . 478
10.5 Finitely generated projective modules . . . 482
10.5.1 Local characterization . . . 482
10.5.2 Rank of finitely generated projective modules . . . 484
10.5.3 Projective modules of rank **1** . . . 486
10.5.4 Non-degenerate submodules and invertible submodules . . . 487
10.5.5 The class group of invertible submodules . . . 490
10.5.6 Exercise . . . 491

11 Graded rings and filtrations **495**
11.1 Graduation on rings and modules . . . 495
11.1.1 Graded ring and graded module . . . 495
11.1.2 Graduation on tensor products and Hom sets . . . 503
11.1.3 Graduation by an ordered group . . . 505
11.1.4 Graded rings of type $\mathbb{Z}$ . . . 507
11.2 Filtration and topologies . . . 512
11.2.1 Filtrated rings and modules . . . 512
11.2.2 The associated graded module . . . 514
11.2.3 Homomorphism compatible with filtrations . . . 516
11.3 Filtrations and completions . . . 517
11.3.1 Complete filtered groups . . . 518
11.3.2 Completion of filtered rings and modules . . . 521
11.3.3 Lifting properties of the associated graduation . . . 527
11.4 The adic topology on Noetherian rings . . . 533
11.4.1 Good filtrations . . . 533
11.4.2 The adic topology on Noetherian rings . . . 536
11.4.3 The adic completion of a Noetherian ring . . . 537
11.4.4 Zariski rings . . . 540
11.5 Lifting in complete rings . . . 544
11.5.1 Strongly relatively prime polynomials . . . 544
11.5.2 Restricted power series and Hensel's lemma . . . 546
11.5.3 System of equations in complete rings . . . 550
11.6 Flatness of graded modules . . . 555
11.7 Exercise . . . 559

12 Associated prime ideals and primary decomposition **563**
12.1 Associated prime ideals of a module . . . 563
12.1.1 Definition of associated prime ideals . . . 563
12.1.2 Associated prime ideal of localizations . . . 565
12.1.3 Associated prime ideals and supports . . . 565
12.1.4 Associated prime ideals of modules over Noetherian rings . . . 566
12.2 Primary decomposition . . . 568
12.2.1 Primary submodules . . . 568
12.2.2 Primary decompositions . . . 569
12.2.3 The localization of a primary decomposition . . . 572
12.2.4 Module of finite length . . . 573
12.2.5 Extension of scalars . . . 576
12.2.6 Primary decomposition of graded modules . . . 579

13 Integral dependence **583**
13.1 Integral elements . . . 583
13.1.1 The integral closure of a ring . . . 586
13.1.2 Examples of integrally closed domains . . . 587
13.1.3 Completely integrally closed domains . . . 589
13.1.4 The integral closure of a ring of fractions . . . 590
13.1.5 Norms and traces of integral elements . . . 592
13.1.6 Integers over a graded ring . . . 596
13.1.7 The lift of prime ideals . . . 598
13.2 Group action on algebras . . . 604
13.2.1 Group acting on an algebra . . . 604
13.2.2 Decomposition group and inertial group . . . 605
13.2.3 Applications for integrally closed domains . . . 610
13.3 Finite generated algebras over a field . . . 613
13.3.1 The Nullstellensatz . . . 617
13.3.2 Jacobson rings . . . 618
13.4 Exercise . . . 621

14 Valuation rings **623**
14.1 Valuation rings of fields . . . 623
14.2 Ordered groups and valuations . . . 626
14.2.1 Valuations of rank one . . . 629
14.2.2 Discrete valuation rings . . . 631
14.3 Compare valuation rings of a field . . . 633
14.4 Dependent valuations and induced topology . . . 636
14.5 Completion of valued fields . . . 643
14.5.1 Archimedean complete fields . . . 644
14.5.2 Non-archimedean complete fields . . . 648
14.6 Extensions of valuation rings . . . 652
14.6.1 Ramification index and inertial degree . . . 652
14.6.2 Prolongations of a valuation . . . 654

14.6.3 Henselian fields . . . 657
14.6.4 The fundamental inequality . . . 661
14.7 Exercise . . . 667

15 Krull domains and divisors **671**
15.1 Krull domains . . . 671
15.1.1 Fractional ideals . . . 671
15.1.2 The monoid structure on $\mathfrak{D}(A)$ . . . 673
15.1.3 Krull domains . . . 675
15.1.4 Essential valuations for a Krull domain . . . 676
15.1.5 Approximation theorem for essential valuations . . . 678
15.1.6 Prime ideals of height **1** in a Krull domain . . . 679
15.1.7 Permanence properties of Krull domains . . . 680
15.1.8 Divisor classes in a Krull domain . . . 682
15.1.9 Dedekind domains . . . 685
15.1.10 The Krull-Akizuki theorem . . . 688
15.1.11 Unique factorization domains . . . 690
15.2 Modules over integrally closed Noetherian domains . . . 694
15.2.1 Lattices . . . 695
15.2.2 Duality and reflexive modules . . . 698
15.2.3 Local construction of reflexive modules . . . 701
15.2.4 Divisors attached to finite generated torsion modules . . . 705
15.2.5 Divisor classes attached to a finite generated module . . . 708
15.2.6 Properties relative to finite field extensions . . . 711
15.2.7 Modules over Dedekind domains . . . 715

16 Dimension **717**
16.1 Dimension of rings and modules . . . 717
16.1.1 Dimension of a ring . . . 717
16.1.2 Dimension of a finitely generated module . . . 720
16.1.3 Cycle associated with a module . . . 720
16.1.4 Exercise . . . 722
16.2 Dimension of algebras . . . 728
16.2.1 Dimension and the going-down property . . . 728
16.2.2 Dimension of a finitely generated algebra . . . 729
16.2.3 Dimension of finitely generated algebras over fields . . . 731
16.2.4 Exercise . . . 736
16.3 Dimension of Noetherian rings . . . 740
16.3.1 Dimension of a quotient ring . . . 740
16.3.2 Dimension and secant sequences . . . 742
16.3.3 Extension of scalars . . . 747
16.3.4 Exersise . . . 751
16.4 Hilbert-Samuel series . . . 752
16.4.1 Poincaré series of a graded module on a polynomial ring . . . 754
16.4.2 Hilbert-Samuel series of a good-filtered module . . . 757

16.5 Regular local rings . . . 765
16.5.1 Regularity of a local ring . . . 765
16.5.2 Quotients of regular local rings . . . 768
16.5.3 Eisenstein polynomials . . . 769
16.6 Dimension and graded rings . . . 772
16.6.1 Dimension and chains of homogeneous ideals . . . 773
16.6.2 Dimension of graded modules . . . 776
16.6.3 Dimension and graded algebras . . . 779
16.7 Multiplicity . . . 781
16.7.1 Multiplicity of a module relative to an ideal . . . 781
16.7.2 Multiplicity and base change . . . 783
16.7.3 Multiplicity and secant sequences . . . 785
16.7.4 Exercise . . . 789

17 Complete Noetherian local rings **791**
17.1 Witt vectors and Witt rings . . . 791
17.1.1 Witt polynomials . . . 791
17.1.2 The ring of Witt vectors . . . 795
17.1.3 Filtration and topology of the Witt ring . . . 798
17.1.4 The Witt ring with characteristic p . . . 802
17.2 Cohen rings . . . 804
17.2.1 p-rings . . . 804
17.2.2 Existence and uniqueness of p-rings . . . 808
17.2.3 Multiplicative representatives . . . 809
17.2.4 Structure of Noetherian complete local rings . . . 811
17.2.5 Coefficient fields . . . 812
17.3 Integral closure of complete local rings . . . 814
17.3.1 Japanese rings . . . 814
17.3.2 Nagata rings . . . 818

18 Depth **823**
18.1 Homological definition of depth . . . 823

19 Sheaves and cohomology of sheaves **825**
19.1 Sheaves of sets . . . 825
19.1.1 Presheaves and sheaves . . . 825
19.1.2 Stalks of presheaves and sheaves . . . 827
19.1.3 Sheafification . . . 831
19.1.4 Direct and inverse images of sheaves . . . 833
19.1.5 Open immersions and closed immersions . . . 837
19.1.6 Glueing sheaves . . . 840
19.1.7 Preheaves and sheaves over a basis . . . 842
19.1.8 The category of presheaves and sheaves . . . 844
19.2 Sheaf of modules . . . 849
19.2.1 Presheaf of moudles . . . 849

19.2.2 Sheaf of moudles . . . 850
19.2.3 Sheafification of presheaves of modules . . . 850
19.2.4 Continuous maps . . . 851
19.2.5 Supports of modules and sections . . . 854
19.2.6 Modules generated by sections . . . 855
19.2.7 Tensor product . . . 856
19.2.8 Internal Hom . . . 859
19.2.9 The abelian category of sheaves of modules . . . 860
19.3 Ringed spaces . . . 864
19.3.1 Ringed spaces, $\mathscr{A}$-modules, and $\mathscr{A}$-algebras . . . 864
19.3.2 Direct image of $\mathscr{A}$-modules . . . 868
19.3.3 Inverse image of a $\mathscr{B}$-module . . . 870
19.3.4 Relations of direct images and inverse images . . . 872
19.3.5 Open immersions and representable natrual transformations . . . 875
19.4 Quasi-coherent sheaves and coherent sheaves . . . 876
19.4.1 Quasi-coherent sheaves . . . 876
19.4.2 Sheaves of finite type . . . 878
19.4.3 Coherent sheaves . . . 881
19.4.4 Locally free sheaves . . . 884

20 Cohomology group of sheaves **893**
20.1 Definition of sheaf cohomology . . . 893
20.2 Flasque sheaves . . . 894
20.3 Locality of cohomology . . . 897

21 Čech cohomology **901**
21.1 The Čech cohomology group with respect to a covering . . . 901
21.2 Čech cohomology as a functor on presheaves . . . 904
21.3 The Čech cohomology groups . . . 905
21.4 Long exact sequence of Čech-cohomology . . . 906
21.4.1 General case . . . 906
21.4.2 Paracompact space . . . 908
21.5 Čech resolution and Leray Acyclic Theorem . . . 909
21.6 Čech vs. Sheaf cohomology . . . 913

22 The language of schemes **917**
22.1 Affine schemes . . . 917
22.1.1 Sheaves associated with a module . . . 917
22.1.2 Functorial properties of the associated sheaf . . . 922
22.1.3 Quasi-coherent sheaves over affine schemes . . . 925
22.2 General schemes . . . 930
22.2.1 Schemes and morphisms of schemes . . . 930
22.2.2 Local schemes . . . 933
22.2.3 Shemes over a scheme . . . 935
22.2.4 Quasi-coherent sheaves on schemes . . . 936

22.2.5 Noetherian schemes and locally Noetherian schemes . . . 938
22.3 Product of schemes . . . 940
22.3.1 Product of schemes . . . 941
22.3.2 Base change of schemes . . . 943
22.3.3 Tensor product of quasi-coherent sheaves . . . 946
22.3.4 Scheme valued points . . . 948
22.3.5 Surjective morphisms . . . 952
22.3.6 Radical morphisms . . . 953
22.3.7 Fibers of morphisms . . . 955
22.3.8 Universally open and universally closed morphisms . . . 956
22.4 Subschemes and immersions . . . 960
22.4.1 Subschemes . . . 960
22.4.2 Immersions of schemes . . . 962
22.4.3 Inverse image of subschemes . . . 964
22.4.4 Local immersions and local isomorphisms . . . 967
22.4.5 Nilradical and associated reduced scheme . . . 968
22.4.6 Reduced scheme structure on closed subsets . . . 973
22.5 Separated schemes and morphisms . . . 975
22.5.1 Diagonal and graph of a morphism . . . 975
22.5.2 Separated morphisms and schemes . . . 979
22.5.3 Criterion of separated morphisms . . . 981
22.6 Finiteness conditions for morphisms . . . 984
22.6.1 Quasi-compact and quasi-separated morphisms . . . 985
22.6.2 Morphisms of finite type and of finite presentation . . . 991
22.6.3 Algebraic schemes . . . 998
22.6.4 Local determination of morphisms . . . 1001
22.6.5 Direct image of quasi-coherent sheaves . . . 1003
22.6.6 Extension of quasi-coherent sheaves . . . 1004
22.6.7 Scheme-theoretic image . . . 1006
22.7 Rational maps over schemes . . . 1008
22.7.1 Rational maps and rational functions . . . 1008
22.7.2 Defining domain of a rational map . . . 1011
22.7.3 Sheaf of rational functions . . . 1013
22.7.4 Torsion sheaves and torsion-free sheaves . . . 1014
22.7.5 Separation criterion for integral schemes . . . 1016
22.8 Formal schemes . . . 1019
22.8.1 Formal affine schemes and morphisms . . . 1019
22.8.2 Morphisms of formal schemes . . . 1022
22.8.3 Inductive limits of schemes . . . 1026
22.8.4 Formal completion of schemes . . . 1030

23 Global properties of morphisms of schemes 1035
23.1 Affine morphisms . . . 1035
23.1.1 Schemes affine over a scheme . . . 1035
23.1.2 Affine S-scheme associated with an $\mathcal{O}_S$-algebra . . . 1037

23.1.3 Quasi-coherent sheaves over affine S-schemes . . . 1039
23.1.4 Base change of affine S-schemes . . . 1042
23.1.5 Vector bundles . . . 1044
23.2 Homogeneous specturm of graded algebras . . . 1048
23.2.1 Localization of graded rings . . . 1048
23.2.2 The homogeneous specturm of a graded ring . . . 1050
23.2.3 Sheaf associated with a graded module . . . 1055
23.2.4 Graded S-module associated with a sheaf . . . 1059
23.2.5 Functorial properties of $\mathrm{Proj}(S)$ . . . 1064
23.2.6 Closed subschemes of $\mathrm{Proj}(S)$ . . . 1068
23.3 Homogeneous spectrum of sheaves of graded algebras . . . 1070
23.3.1 Homogeneous spectrum of a graded $\mathscr{O}_Y$-algebra . . . 1070
23.3.2 Sheaves associated with a graded $\mathscr{S}$-module . . . 1074
23.3.3 Graded $\mathscr{S}$-module assocaited with a sheaf . . . 1076
23.3.4 Functorial properties of $\mathrm{Proj}(\mathscr{S})$ . . . 1080
23.3.5 Closed subschemes of $\mathrm{Proj}(\mathscr{S})$ . . . 1083
23.3.6 Morphisms into $\mathrm{Proj}(\mathscr{S})$ . . . 1084
23.4 Projective bundles and ample sheaves . . . 1090
23.4.1 Projective bundles . . . 1090
23.4.2 Morphisms into $\mathbb{P}(\mathscr{E})$ . . . 1092
23.4.3 The Segre morphism . . . 1095
23.4.4 Very ample sheaves . . . 1097
23.4.5 Ample sheaves . . . 1102
23.4.6 Relatively ample sheaves . . . 1107
23.5 Quasi-affine, proper, and projective morphisms . . . 1110
23.5.1 Quasi-affine morphisms . . . 1110
23.5.2 Serre's criterion on affineness . . . 1113
23.5.3 Quasi-projective morphisms . . . 1116
23.5.4 Universally closed and proper morphisms . . . 1117
23.5.5 Projective morphisms . . . 1120
23.5.6 Chow's lemma . . . 1122
23.6 Integral morphisms and finite morphisms . . . 1126
23.6.1 Integral and finite morphisms . . . 1126
23.6.2 Quasi-finite morphisms . . . 1129
23.6.3 Integral closure of a scheme . . . 1131
23.6.4 Determinant of an endomorphism of $\mathscr{O}_X$-modules . . . 1134
23.6.5 Norm of an invertible sheaf . . . 1138
23.6.6 Application: a criterion of amplitude . . . 1142
23.6.7 Chevally's theorem . . . 1144
23.7 Valuative criterion . . . 1146
23.7.1 Remainders for valuation rings . . . 1146
23.7.2 Valuative criterion of separation . . . 1148
23.7.3 Valuative criterion of properness . . . 1149
23.7.4 Algebraic curves . . . 1153
23.8 Blow up of schemes, projective cones and closures . . . 1158

23.8.1 Blow up of schemes . . . 1158
23.8.2 Homogenization of graded rings . . . 1163
23.8.3 Projective cones . . . 1168
23.8.4 Functorial properties . . . 1173
23.8.5 Blunt cones over a homogeneous specturm . . . 1175
23.8.6 Blow up of projective cones . . . 1178
23.8.7 Ample sheaves and contractions . . . 1181
23.8.8 Quasi-coherent sheaves over the projective cone . . . 1182

24 Cohomology of coherent sheaves over schemes 1187
24.1 Cohomology of affine schemes . . . 1187
24.1.1 Čech cohomology and Koszul complex . . . 1187
24.1.2 Cohomology of affine schemes . . . 1189
24.1.3 Application to cohomology of schemes . . . 1190
24.2 Coholomogical study of projective morphisms . . . 1194
24.2.1 Cohomology associated with an invertible sheaf . . . 1194
24.2.2 The coherence theorem for projective morphisms . . . 1197
24.2.3 Applications to associated sheaves of graded modules . . . 1199
24.2.4 Euler characteristic and Hilbert polynomial . . . 1202
24.2.5 Cohomological criterion for ampleness . . . 1203
24.3 The finiteness theorem for proper morphisms . . . 1203
24.3.1 The dévissage lemma . . . 1203
24.3.2 The finiteness theorem for proper morphisms . . . 1204

Chapter 1

General topology

1.1 Topological structures

1.1.1 Topological spaces

Definition 1.1.1. *A **topological structure** (or, more briefly, a **topology**) on a set X is a structure given by a set $\mathcal{T}$ of subsets of X, having the following properties:*

(O1) $\varnothing, X \in \mathcal{T}$.

(O2) Every union of sets of $\mathcal{T}$ is a set of $\mathcal{T}$.

(O3) Every finite intersection of sets of $\mathcal{T}$ is a set of $\mathcal{T}$.

*The sets of $\mathcal{T}$ are called **open sets** of the topological structure defined by $\mathcal{T}$ on X.*

A **topo space** is a set endowed with a topological structure. The elements of a topological space are often called points. When a topology has been defined on a set X, this set is said to be the set undering the topological space X.

Example 1.1.2. If X is any set, the collection of all subsets of X is a topology on X; it is called the **discrete topology**. The collection consisting of X and $\varnothing$ only is also a topology on X; we shall call it the **indiscrete topology**, or the **trivial topology**.

Example 1.1.3. Let X be a set; let $\mathcal{T}_{fc}$ be the collection of all subsets U of X such that U^c either is finite or is all of X. Then $\mathcal{T}_{fc}$ is a topology on X, called the **finite complement topology**. Both X and $\varnothing$ are in $\mathcal{T}_{fc}$, since X^c is finite and $\varnothing^c$ is all of X. If $\{U_\alpha\}$ is an indexed family of nonempty elements of $\mathcal{T}_{fc}$, to show that $\bigcap_\alpha U_\alpha$ is in $\mathcal{T}_{fc}$, we compute

$$\left(\bigcup_\alpha U_\alpha\right)^c = \bigcap_\alpha U_\alpha^c.$$

The latter set is finite because each set U_α^c is finite. If $U_1, \ldots, U_n$ are nonempty elements of $\mathcal{T}_{fc}$, to show that $\bigcap_{i=1}^n U_i$ is in $\mathcal{T}_{fc}$, we compute that

$$\left(\bigcap_{i=1}^n U_\alpha\right)^c = \bigcup_{i=1}^n U_\alpha^c.$$

The latter set is a finite union of finite sets and, therefore, finite.

Similarly, let $\mathcal{T}_{cc}$ be the collection of all subsets U of X such that U^c either is countable or is all of X. Then $\mathcal{T}_{cc}$ is a topology on X, called the **countable complement topology** on X.

Definition 1.1.4. *Suppose that $\mathcal{T}_1$ and $\mathcal{T}_2$ are two topologies on a given set X. If $\mathcal{T}_1 \supseteq \mathcal{T}_2$, we say that $\mathcal{T}_1$ is **finer** than $\mathcal{T}_2$; if $\mathcal{T}_1$ properly contains $\mathcal{T}_2$, we say that $\mathcal{T}_1$ is **strictly finer** than $\mathcal{T}_2$. We also say that $\mathcal{T}_2$ is **coarser** than $\mathcal{T}_1$, or **strictly coarser**, in these two respective situations. We say $\mathcal{T}_1$ is **comparable** with $\mathcal{T}_2$ if either $\mathcal{T}_1 \subseteq \mathcal{T}_2$ or $\mathcal{T}_2 \subseteq \mathcal{T}_1$.*

1.1.2 Base of topologies

For each of the examples in the preceding part, we were able to specify the topology by describing the entire collection $\mathcal{T}$ of open sets. Usually this is too difficult. In most cases, one specifies instead a smaller collection of subsets of X and defines the topology in terms of that.

Definition 1.1.5. *If X is a set, a base for a topology on X is a collection $\mathcal{B}$ of subsets of X (called **base elements**) such that*

(B1) For each $x \in X$, there is at least one base element B containing x.

(B2) If x belongs to the intersection of two base elements B_1 and B_2, then there is a base element B_3 containing x such that $B_3 \subseteq B_1 \cap B_2$.

If $\mathcal{B}$ satisfies these two conditions, then we define the topology $\mathcal{T}$ generated by $\mathcal{B}$ as follows: A subset U of X is said to be open in X (that is, to be an element of $\mathcal{T}$) if for each $x \in U$, there is a base element $B \in \mathcal{B}$ such that $x \in B$ and $B \subseteq U$. Note that each base element is itself an element of $\mathcal{T}$. We now check that the collection $\mathcal{T}$ is indeed a topology on X.

Proposition 1.1.6. *The collection $\mathcal{T}$ induced by a base $\mathcal{B}$ is a topology on X.*

Proof. If U is the empty set, it satisfies the defining condition of openness vacuously. Likewise, X is in $\mathcal{T}$, since for each $x \in X$ there is some base element B containing x and contained in X. Now let us take an indexed family $(U_\alpha)_{\alpha \in A}$, of elements of $\mathcal{T}$ and consider $U = \bigcup_\alpha U_\alpha$. Given $x \in U$, there is an index α such that $x \in U_\alpha$. Since U_α is open, there is a base element B such that $x \in B \subseteq U_\alpha$. Then $x \in B \subseteq U$, so that U is open, by definition.

Now let us take two elements U_1 and U_2 of $\mathcal{T}$ and show that $U_1 \cap U_2$ belongs to $\mathcal{T}$. Given $x \in U_1 \cap U_2$, choose a base element B_1 containing x such that $B_1 \subseteq U_1$; choose also a base element B_2 containing x such that $B_2 \subseteq U_2$. The second condition for a base enables us to choose a base element B_3 containing x such that $B_3 \subseteq B_1 \cap B_2$. Then $x \in B_3$ and $B_3 \subseteq U_1 \cap U_2$, so $U_1 \cap U_2$ belongs to $\mathcal{T}$, by definition. □

Example 1.1.7. Let $\mathcal{B}$ be the collection of all circular regions (interiors of circles) in the plane. Then $\mathcal{B}$ satisfies both conditions for a base. In the topology generated by $\mathcal{B}$, a subset U of the plane is open if every x in U lies in some circular region contained in U.

Example 1.1.8. Let $\mathcal{B}$ be the collection of all rectangular regions (interiors of rectangles) in the plane, where the rectangles have sides parallel to the coordinate axes. Then $\mathcal{B}$ satisfies both conditions for a base. In this case, the condition (B2) is trivial, because the intersection of any two base elements is itself a base element (or empty). As we shall see later, the base $\mathcal{B}$ generates the same topology on the plane as the base given in the preceding example.

Example 1.1.9. If X is any set, the collection of all one-point subsets of X is a base for the discrete topology on X.

Another way of describing the topology generated by a base is given in the following lemma:

Lemma 1.1.10. *Let X be a set and $\mathcal{B}$ a base for a topology $\mathcal{T}$ on X. Then $\mathcal{T}$ equals the collection of all unions of elements of $\mathcal{B}$.*

Proof. Given a collection of elements of $\mathcal{B}$, they are also elements of $\mathcal{T}$. Because $\mathcal{T}$ is a topology, their union is in $\mathcal{T}$. Conversely, given $U \in \mathcal{T}$, choose for each $x \in U$ an element B_x of $\mathcal{B}$ such that $x \in B_x \subseteq U$. Then $U = \bigcup_{x \in U} B_x$, so U equals a union of elements of $\mathcal{B}$. □

This lemma states that every open set U in X can be expressed as a union of base elements. This expression for U is not, however, unique. Thus the use of the term "base" in topology differs drastically from its use in linear algebra, where the equation expressing a given vector as a linear combination of base vectors is unique. We have described in two different ways how to go from a base to the topology it generates. Sometimes we need to go in the reverse direction, from a topology to a base generating it. Here is one way of obtaining a base for a given topology; we shall use it frequently.

Proposition 1.1.11. *Let X be a topological space. Suppose that $\mathcal{B}$ is a collection of open sets of X such that for each open set U of X and each x in U, there is an element B of $\mathcal{B}$ such that $x \in B \subseteq U$. Then $\mathcal{B}$ is a base for the topology of X.*

Proof. We must show that $\mathcal{B}$ is a base. The first condition for a base is easy: Given $x \in X$, since X is itself an open set, there is by hypothesis an element B of $\mathcal{B}$ such that $x \in B \subseteq X$. To check the second condition, let x belong to $B_1 \cap B_2$, where B_1 and B_2 are elements of $\mathcal{B}$. Since B_1 and B_2 are open, so is $B_1 \cap B_2$. Therefore, there exists by hypothesis an element B_3 in $\mathcal{B}$ such that $x \in B_3 \subseteq B_1 \cap B_2$.

Let $\mathcal{T}$ be the collection of open sets of X; we must show that the topology $\mathcal{T}'$ generated by $\mathcal{B}$ equals the topology $\mathcal{T}$. First, note that if U belongs to $\mathcal{T}$ and if $x \in U$, then there is by hypothesis an element B of $\mathcal{B}$ such that $x \in B \subseteq U$. It follows that U belongs to the topology $\mathcal{T}'$, by definition. Conversely, if W belongs to the topology $\mathcal{T}'$, then W equals a union of elements of $\mathcal{B}$, by the preceding lemma. Since each element of B belongs to $\mathcal{T}$ and $\mathcal{T}$ is a topology, W also belongs to $\mathcal{T}$. □

When topologies are given by bases, it is useful to have a criterion in terms of the bases for determining whether one topology is finer than another. One such criterion is the following:

Proposition 1.1.12. *Let $\mathcal{B}_1$ and $\mathcal{B}_2$ be bases for the topologies $\mathcal{T}_1$ and $\mathcal{T}_2$, respectively, on X. Then the following are equivalent:*

(i) $\mathcal{T}_1$ is finer than $\mathcal{T}_2$.

(ii) For each $x \in X$ and each base element $B_2 \in \mathcal{B}_2$ containing x, there is a base element $B_1 \in \mathcal{B}_1$ such that $x \in B_1 \subseteq B_2$.

Proof. Assume (ii). Given an element U of $\mathcal{T}_2$, we wish to show that $U \in \mathcal{T}_1$. Let $x \in U$. Since $\mathcal{B}_2$ generates $\mathcal{T}_2$, there is an element $B_2 \in \mathcal{B}_2$ such that $x \in B_2 \subseteq U$. Condition (ii) tells us there exists an element $B_1 \in \mathcal{B}_1$ such that $x \in B_1 \subseteq B_2$. Then $x \in B_1 \subseteq U$, so $U \in \mathcal{T}_1$, by definition.

Conversely, assume (i). We are given $x \in X$ and $B_2 \in \mathcal{B}_2$, with $x \in B_2$. Now $\mathcal{B}_2$ belongs to $\mathcal{T}_2$ by definition and $\mathcal{T}_2 \subseteq \mathcal{T}_1$ by condition (i); therefore, $B \in \mathcal{T}_1$. Since $\mathcal{T}_1$ is generated by $\mathcal{B}_1$, there is an element $B_1 \in \mathcal{B}_1$ such that $x \in B_1 \subseteq B_2$. □

We now define three topologies on the real line $\mathbb{R}$, all of which are of interest.

Example 1.1.13. If $\mathcal{B}$ is the collection of all open intervals in the real line,

$$(a, b) = \{x \in \mathbb{R} : a < x < b\}$$

the topology generated by $\mathcal{B}$ is called the standard topology on the real line. Whenever we consider $\mathbb{R}$, we shall suppose it is given this topology unless we specifically state otherwise. If $\mathcal{B}'$ is the collection of all half-open intervals of the form

$$[a, b) = \{x \in \mathbb{R} : a \leq x < b\},$$

where $a < b$, the topology generated by $\mathcal{B}'$ is called the lower limit topology on $\mathbb{R}$. When $\mathbb{R}$ is given the lower limit topology, we denote it by $\mathbb{R}_l$. Finally let K denote the set of all numbers of the form $1/n$, for $n \in \mathbb{Z}_+$, and let $\mathcal{B}_K$ be the collection of all open intervals (a, b), along with all sets of the form $(a, b) \setminus K$. The topology generated by $\mathcal{B}_K$ will be called the K-topology on $\mathbb{R}$. When $\mathbb{R}$ is given this topology, we denote it by $\mathbb{R}_K$.

It is easy to see that all three of these collections are bases; in each case, the intersection of two base elements is either another base element or is empty. The relation between these topologies is the following:

Proposition 1.1.14. *The topologies of $\mathbb{R}_l$ and $\mathbb{R}_K$ are strictly finer than the standard topology on $\mathbb{R}$, but are not comparable with one another.*

Proof. Let $\mathcal{T}$, $\mathcal{T}_l$, and $\mathcal{T}_K$ be the topologies of $\mathbb{R}$, $\mathbb{R}_l$, and $\mathbb{R}_K$, respectively. Given a base element (a, b) for $\mathcal{T}$ and a point x of (a, b), the base element $[x, b)$ for $\mathcal{T}_l$ contains x and lies in (a, b). On the other hand, given the base element $[x, d)$ for $\mathcal{T}_l$, there is no open interval (a, b) that contains x and lies in $[x, d)$. Thus $\mathcal{T}_l$ is strictly finer than $\mathcal{T}$.

A similar argument applies to $\mathbb{R}_K$. Given a base element (a, b) for $\mathcal{T}$ and a point x of (a, b), this same interval is a base element for $\mathcal{T}_K$ that contains x. On the other hand, given the base element $B = (-1, 1) \setminus K$ for $\mathcal{T}_K$ and the point 0 of B, there is no open interval that contains 0 and lies in B.

Finally, given the base element $[x, d)$ for $\mathcal{T}_l$, there is no base element of $\mathcal{T}_K$ that contains x and lies in $[x, d)$, so $\mathcal{T}_K$ is not finer than $\mathcal{T}_l$. Conversely, given the base element $B = (-1, 1) \setminus K$ for $\mathcal{T}_K$ and the point 0 of B, there is no interval $[a, b)$ that contains 0 and lies in B. Thus $\mathcal{T}_l$ is not finer than $\mathcal{T}_K$. □

Example 1.1.15. Let X be a totally ordered set; assume X has more than one element. Let $\mathcal{B}$ be the collection of all sets of the following types:

(a) All open intervals (a, b) in X.

(b) All intervals of the form $[a_0, b)$, where a_0 is the smallest element (if any) of X.

(c) All intervals of the form $(a, b_0]$, where b_0 is the largest element (if any) of X.

The collection $\mathcal{B}$ is a base for a topology on X, which is called the **order topology**.

A question may occur to us at this point. Since the topology generated by a base $\mathcal{B}$ may be described as the collection of arbitrary unions of elements of $\mathcal{B}$, what happens if we start with a given collection of sets and take finite intersections of them as well as arbitrary unions? This question leads to the notion of a subbase for a topology.

Definition 1.1.16. *A **subbase** $\mathcal{S}$ for a topology on X is a collection of subsets of X whose union equals X. The topology generated by the subbase $\mathcal{S}$ is defined to be the collection $\mathcal{T}$ of all unions of finite intersections of elements of $\mathcal{S}$.*

We must of course check that $\mathcal{T}$ is a topology. For this purpose it will suffice to show that the collection $\mathcal{B}$ of all finite intersections of elements of $\mathcal{S}$ is a base. Given $x \in X$, it belongs to an element of $\mathcal{S}$ and hence to an element of $\mathcal{B}$; this is the first condition for a base. The second condition is trivial since the intersection of two elements of $\mathcal{B}$ again belongs to $\mathcal{B}$.

1.1.3 Neighborhoods

Let X be a topological space and A any subset of X. A **neighbourhood of A** is any subset of X which contains an open set containing A. The neighbourhoods of a subset $\{x\}$ consisting of a single point are also called **neighbourhoods of the point x**.

Proposition 1.1.17. *A set A is a neighbourhood of each of the points of a set B if and only if it is a neighborhood of B. It particular, a set is open if and only if it is a neighborhood of each of its points.*

Proof. It is clear that every neighbourhood of a subset B of X is also a neighbourhood of each subset of B; in particular, it is a neighbourhood of each point of B. Conversely, suppose A is a neighbourhood of each of the points of a set B, and let V be the union of the open sets contained in A; then $V \subseteq A$, and since each point of B belongs to an open set contained in A, we have $B \subseteq V$; but V is open by virtue of (O2), hence A is a neighbourhood of B. □

Remark 1.1.1. The everyday sense of the word "neighbourhood" is such that many of the properties which involve the mathematical idea of neighbourhood appear as the mathematical expression of intuitive properties; the choice of this term thus has the advantage of making the language more expressive. For this purpose it is also permissible to use the expressions "sufficiently near" and "as near as we please" in some statements. For example, Proposition 1.1.17 can be stated in the following form: a set A is open if and only if, for each $x \in A$, all the points sufficiently near x belong to A. More generally, we shall say that a property holds for all points sufficiently near a point x, if it holds at all points of some neighbourhood of x.

Let us denote by $\mathfrak{U}(x)$ the set of all neighbourhoods of x. The sets $\mathfrak{U}(x)$ have the following properties:

(U1) Every subset of X which contains a set belonging to $\mathfrak{U}(x)$ itself belongs to $\mathfrak{U}(x)$.

(U2) Every finite intersection of sets of $\mathfrak{U}(x)$ belongs to $\mathfrak{U}(x)$.

(U3) Every element of $\mathfrak{U}(x)$ contains x.

(U4) If V belongs to $\mathfrak{U}(x)$, then there is a set $W \in \mathfrak{U}(x)$ such that, for each $y \in W$, V belongs to $\mathfrak{U}(y)$.

These four properties of the sets $\mathfrak{U}(x)$ are characteristic. To be precise, we have:

Proposition 1.1.18. *If to each element $x \in X$ there corresponds a set $\mathfrak{U}(x)$ of subsets of X such that the properties (U1), (U2), (U3) and (U4) are satisfied, then there is a unique topological structure on X such that, for each $x \in X$, $\mathfrak{U}(x)$ is the set of neighbourhoods of x in this topology.*

Proof. By Proposition 1.1.17, if there is a topology on X satisfying these conditions, the set of open sets for this topology is necessarily the set $\mathcal{T}$ of subsets A of X such that for each $x \in A$ we have $A \in \mathcal{B}(X)$; hence the uniqueness of this topology if it exists.

Now we prove that the set $\mathcal{T}$ is a topology on X. It is clear that $\mathcal{T}$ satisfies the axoim (O1). It satisfies axioms (O2) and (O3) because: for (O2), this follows immediately from (U1), and for (O3), from (U2). It remains to show that, in the topology defined by $\mathcal{T}$, $\mathcal{B}(x)$ is the set of neighbourhoods of x for each $x \in X$.

It follows from (U1) that every neighbourhood of x belongs to $\mathfrak{U}(x)$. Conversely, let V be a set belonging to $\mathcal{B}(x)$, and let U be the set of points $y \in X$ such that $V \in \mathcal{B}(y)$; if we can show that $x \in U$, $U \subseteq V$ and $U \in \mathcal{T}$, then the proof will be complete.

We have $x \in U$ since $V \in \mathfrak{U}(x)$; also $U \subseteq V$, for every point $y \in U$ belongs to V by reason of (U3) and the hypothesis $V \in \mathfrak{U}(y)$. It remains to show that $U \in \mathcal{T}$, i.e. that $U \in \mathfrak{U}(y)$ for each $y \in U$; now if $y \in U$ then by (U4) there is a set $W \in \mathfrak{U}(y)$ such that for each $z \in W$ we have $V \in \mathfrak{U}(z)$; since $V \in \mathfrak{U}(z)$ means that $z \in U$, it follows that $W \subseteq U$, and therefore, by (U1) that $U \in \mathfrak{U}(y)$. □

Proposition 1.1.18 shows that a topology on X can be defined by means of the sets $\mathfrak{U}(x)$ of neighbourhoods of points of X, subject only to the axioms (U1), (U2) , (U3) and (U4).

Definition 1.1.19. *In a topological space X, a **fundamental system of neighbourhoods** of a point x (resp. of a subset A of X) is any set $\mathfrak{B}$ of neighbourhoods of x (resp. A) such that for each neighbourhood V of x (resp. of A) there is a neighbourhood $W \in \mathfrak{B}$ such that $W \subseteq V$.*

If $\mathfrak{B}$ is a fundamental system of neighbourhoods of a subset A of X, then every finite intersection of sets of $\mathfrak{B}$ contains a set of $\mathfrak{B}$. In fact, as we will see, a neighborhood base of x is just a filterbase for the neighborhood filter $\mathfrak{U}(x)$.

Proposition 1.1.20. *If X is a topological space, then for a set $\mathcal{B}$ of open subsets of X to be a base of the topology of X it is necessary and sufficient that for each $x \in X$ the set of $V \in \mathcal{B}$ such that $x \in V$ is a fundamental system of neighbourhoods of X.*

Proof. It is clear that the condition is necessary. Conversely, if it is satisfied, then given any open set U and any $x \in U$ there is an open set $V_x \in \mathcal{B}$ such that $x \in V_x \subseteq U$. The union of the sets V_x for $x \in U$ is therefore equal to U. This completes the proof. □

1.1.4 Closure, interior and boundary

Definition 1.1.21. *In a topological space X, a point x is said to be an **interior point** of a subset A of X if A is a neighbourhood of x. The set of interior points oj A is called the interior of A and is denoted by* $\operatorname{Int} A$.

According to the definition, a point x is an interior point of A if there is an open set contained in A which contains x; it follows that $\operatorname{Int} A$ is the union of all the open sets contained in A, and hence is the largest open set contained in A. Every point which is interior to the complement of a set A is said to be an **exterior point** of A, and the set of these points is called the **exterior** of A in X; a point $x \in X$ which is an exterior point of A is therefore characterized by the property that x has a neighbourhood which does not meet A.

Now we define the closure of a subset $A \subseteq X$.

Definition 1.1.22. *The **closure** of a subset A of a topological space X is the set of all points $x \in X$ such that every neighbourhood of x meets A, and is denoted by $\overline{A}$.*

Every point which is not in the closure of A is exterior to A, and conversely; thus we have the formulae (which are duals of each other)

$$\overline{A}^c = \operatorname{Int} A^c, \quad (\operatorname{Int} A)^c = \overline{A^c}.$$

Hence, to any proposition on interiors of sets, there corresponds by duality a proposition on closures, and vice versa. In particular, the closure of a set A is the smallest closed set which contains A.

Proposition 1.1.23. *Let U be an open set in X; then for every subset A of X, we have $U \cap \overline{A} \subseteq \overline{U \cap A}$.*

Proof. For suppose $x \in U \cap \overline{A}$; then if V is any neighbourhood of x, $V \cap U$ is a neighbourhood of x, since U is open; hence $V \cap U \cap A$ is not empty and therefore x lies in the closure of $U \cap A$. □

If x lies in the closure of $\overline{A}$ but not in A, then every neighbourhood of x contains a point of A other than x; but if $x \in A$ it can happen that x has a neighbourhood which contains no point of A except x. We say then that x is an **isolated point** of A. In particular, x is isolated in the whole space X if and only if $\{x\}$ is an open set.

Example 1.1.24. Let X be the real line $\mathbb{R}$. If $A = (0, 1]$, then $\overline{A} = [0, 1]$, for every neighborhood of 0 intersects A, while every point outside $[0, 1]$ has a neighborhood disjoint from A. Similar arguments apply to the following subsets of X: If $B = \{1/n : n \in \mathbb{Z}_+\}$, then $\overline{B} = \{0\} \cup B$. If $C = \{0\} \cup (1, 2)$, then $\overline{C} = \{0\} \cup [1, 2]$. If $\mathbb{Q}$ is the set of rational numbers, then $\overline{\mathbb{Q}} = \mathbb{R}$. If $\mathbb{Z}_+$ is the set of positive integers, then $\overline{\mathbb{Z}}_+ = \mathbb{Z}_+$. If $\mathbb{R}_+$ is the set of positive reals, then the closure of R+ is the set $\mathbb{R}_+ \cup \{0\}$.

Example 1.1.25. Consider the subspace $A = (0, 1]$ of the real line $\mathbb{R}$. The set $B = (0, 1/2)$ is a subset of A; its closure in $\mathbb{R}$ is the set $[0, 1/2]$, and its closure in A is the set $[0, 1/2] \cap A = (0, 1/2]$.

Definition 1.1.26. *In a topological space X, a point x is said to be a **boundary point** of a set A if x lies in the closure of A and in the closure of A^c. The set of boundary points of A is called the **boundary** of A, denoted by ∂A.*

The boundary of A is therefore the set $\overline{A} \cap \overline{A^c}$, which is closed. A boundary point x of A is characterized by the property that every neighbourhood of x contains at least one point of A and at least one point of A^c; x may or may not belong to A. The boundary of A is the same as the boundary of A^c. The interior of A, the exterior of A and the boundary of A are mutually disjoint and their union is the whole space X.

Now we prove some basic properties of closures and interiors.

Proposition 1.1.27. *Let A, B be subsets of a topological space X. Then*

(a) $\operatorname{Int}(A \cap B) = (\operatorname{Int} A) \cap (\operatorname{Int} B)$ *and* $\overline{A \cup B} = \overline{A} \cup \overline{B}$.

(b) If $A \subseteq B$ *then* $\overline{A} \subseteq \overline{B}$ *and* $\operatorname{Int} A \subseteq \operatorname{Int} B$.

(c) For a family $(A_i)_{i \in I}$ *of subsets of* X*, we have*

$$\overline{\bigcap_{i \in I} A_i} \subseteq \bigcap_{i \in I} \overline{A_i}, \quad \overline{\bigcup_{i \in I} A_i} \supseteq \bigcup_{i \in I} \overline{A_i}$$

and

$$\operatorname{Int}\Big(\bigcup_{i \in I} A_i\Big) \supseteq \bigcup_{i \in I} \operatorname{Int} A_i, \quad \operatorname{Int}\Big(\bigcap_{i \in I} A_i\Big) \subseteq \bigcap_{i \in I} \operatorname{Int} A_i.$$

Proof. Part (b) and (c) are clear by definition, so we only prove (a). Since $A \cap B$ is contained in A and B, it is clear that $\operatorname{Int}(A \cap B) \subseteq \operatorname{Int}(A) \cap \operatorname{Int}(B)$. Conversely, if $x \in \operatorname{Int}(A) \cap \operatorname{Int}(B)$, then there are open sets U, V in X such that $x \in U \subseteq A$ and $x \in V \subseteq B$. Then $x \in U \cap V \subseteq A \cap B$, hence $x \in \operatorname{Int}(A \cap B)$. This proves $\operatorname{Int}(A \cap B) = (\operatorname{Int} A) \cap (\operatorname{Int} B)$, and the other part follows from duality. □

There is yet another way of describing the closure of a set, a way that involves the important concept of limit point, which we consider now.

If A is a subset of the topological space X and if x is a point of X, we say that x is a limit point of A if every neighborhood of x intersects A in some point other than x itself. Said differently, x is a limit point of A if it belongs to the closure of $A \setminus \{x\}$. The point x may lie in A or not; for this definition it does not matter.

Example 1.1.28. Consider the real line $\mathbb{R}$. If $A = (0, 1]$, then the point 0 is a limit point of A and so is the point $1/2$. In fact, every point of the interval $[0, 1]$ is a limit point of A, but no other point of $\mathbb{R}$ is a limit point of A.

If $B = \{1/n : n \in \mathbb{Z}_+\}$, then 0 is the only limit point of B. Every other point x of $\mathbb{R}$ has a neighborhood that either does not intersect B at all, or it intersects B only in the point x itself. If $C = \{0\} \cup (1, 2)$, then the limit points of C are the points of the interval $[1, 2]$. If $\mathbb{Q}$ is the set of rational numbers, every point of $\mathbb{R}$ is a limit point of $\mathbb{Q}$. If $\mathbb{Z}_+$ is the set of positive integers, no point of $\mathbb{R}$ is a limit point of $\mathbb{Z}_+$. If $\mathbb{R}_+$ is the set of positive reals, then every point of $\{0\} \cup \mathbb{R}_+$ is a limit point of $\mathbb{R}_+$.

It follows from the definition of closure that the following result is valid.

Proposition 1.1.29. *Let A be a subset of the topological space X; let A' be the set of all limit points of A. Then $\overline{A} = A \cup A'$.*

Corollary 1.1.30. *A subset of a topological space is closed if and only if it contains all its limit points.*

1.2 Continuous functions

1.2.1 Semicontinuity

Recall the usual topology of $\mathbb{R}$ has a subbase $S = \{(a, +\infty) : a \in \mathbb{R}\} \cup \{(-\infty, a) : a \in \mathbb{R}\}$. Therefore a function $f : X \to \mathbb{R}$ is continuous if and only if $f^{-1}((a, +\infty))$ and $f^{-1}((-\infty, a))$ are open for every $a \in \mathbb{R}$. This motivates the following definition:

Definition 1.2.1. *Let X be a topological space. A function $f : X \to \mathbb{R}$ is called* ***lower semicontinuous*** *at x if for any $\varepsilon > 0$ there exists a neighborhod U of x such that $f(U) \subseteq (f(x) - \varepsilon, +\infty)$, and* ***lower semicontinuous*** *if $f^{-1}((a, +\infty))$ is open for every $a \in \mathbb{R}$. A similar terminology is addressed for* ***upper semicontinuous****.*

It is clear that f is continuous at x if and only if f is lower and upper semicontinuous at x, and f is continuous if and only if f is lower and upper semicontinuous. Now we collect some properties of semicontinuity.

Proposition 1.2.2. *Let X be a topological space and $f : X \to \mathbb{R}$ be a function. Then*

(a) f is lower (upper) semicontinuous if and only if f is lower (upper) semicontinuous at every $x \in X$.

(b) f is lower semicontinuous if and only if $-f$ is upper semicontinuous.

(c) If $\mathscr{F}$ is a family of lower semicontinuous functions, then $g(x) = \sup_{f \in \mathscr{F}} f(x)$ is lower semicontinuous.

(d) A finite sum of lower semicontinuous functions is lower semicontinuous

(b) If X is compact and $f : X \to \mathbb{R}$ is lower semicontinuous. Then f attains its minimum on X.

Proof. If f is lower semicontinuous, then for any $x \in X$ and $\varepsilon > 0$, the set $f^{-1}((f(x) - \varepsilon, +\infty))$ is open. Since x is contained in it, we can find a neighborhood U of x such that $U \subseteq f^{-1}((f(x) + \varepsilon, +\infty))$. Therefore f is lower semicontinuous at x. The converse is done similarly. This proved (a).

For (b), just note that $(-f)^{-1}((-\infty, a)) = f^{-1}((-a, +\infty))$, so $(-f)$ is upper semicontinuous if and only if f is lower semicontinuous.

Now assume that $\mathscr{F}$ is a family of lower semicontinuous functions, then for any $a \in \mathbb{R}$ and $f \in \mathscr{F}$, the set $\{x : f(x) > a\}$ is open. Since we have

$$\{x : g(x) > a\} = \bigcup_{f \in \mathscr{F}} \{x : f(x) > a\},$$

we see the left side is also open, therefore g is lower semicontinuous.

Let f and g be lower semicontinuous functions, then for every $a \in \mathbb{R}$, we observe that

$$\begin{aligned}\{x : f(x) + g(x) > a\} = \{x : f(x) > a - g(x)\} &= \bigcup_{r \in \mathbb{Q}} \Big(\{x : f(x) > r\} \cap \{x : a - g(x) < r\}\Big) \\ &= \bigcup_{r \in \mathbb{Q}} \Big(\{x : f(x) > r\} \cap \{x : g(x) > a - r\}\Big).\end{aligned}$$

Therefore the left side is open, and so $f + g$ is also lower semicontinuous.

Finally, if f is lower semicontinuous and X is compact. Then an open cover of X is given by the collection $\{f^{-1}((a, +\infty)) : a \in \mathbb{R}\}$, hence has a finite subcover. This means $f(X)$ has a lower bound. Let α be the infimum of $f(X)$, and assume that f does not attain α. Then the collection $\{f^{-1}((\alpha + 1/n, +\infty)) : n \in \mathbb{N}\}$ is an open cover of X, which does not have a finite subcover. This is a contradiction. □

Proposition 1.2.3. *Let X be a topological space and $A \subseteq X$ be a subset. Then*

(a) A is open if and only if χ_A is lower semicontinuous.

(b) A is closed if and only if χ_A is upper semicontinuous.

Proof. This follows from the observations

$$A = \chi_A^{-1}((0, +\infty)), \quad A^c = \chi_A^{-1}((-\infty, 1)),$$

so A is open if and only if χ_A is lower semicontinuous, and A^c is open if and only if χ_A is upper semicontinuous. □

Proposition 1.2.4. *Let X be a topological space and $f : X \to \mathbb{R}$. Let $x \in X$. Then*

(a) f is lower semicontinuous at x if and only if $f(x) \leq \underline{\lim}\, f(x_\alpha)$ for every net $\{x_\alpha\}$ converging to x.

(b) f is upper semicontinuous at x if and only if $f(x) \geq \overline{\lim}\, f(x_\alpha)$ for every net $\{x_\alpha\}$ converging to x.

Proof. If f is lower semicontinuous at x, then for any $\varepsilon > 0$, ther exists a neighborhood U of x such that $f(U) \subseteq f^{-1}((f(x) - \varepsilon, +\infty))$. This then implies $\underline{\lim}\, f(x_\alpha) \geq f(x) - \varepsilon$, and since ε is arbitrary, that $\underline{\lim}\, f(x_\alpha) \geq f(x)$. Conversely, if $f(x) \leq \underline{\lim}\, f(x_\alpha)$, let $\{x_\alpha\}$ be the neighborhood net converging to x. Then for any $\varepsilon > 0$, there exist an index α_0 such that $f(x_\alpha) > f(x) - \varepsilon$ for any $\alpha \leq \alpha_0$. This then means f is lower semicontinuous at x. The claim for upper semicontinuous is proved simialrly. □

Example 1.2.5 (Rank function is lower continuous). Let rank : $\mathcal{M}_{mn}(\mathbb{R}) \to \mathbb{N} \subseteq \mathbb{R}$ be the rank function, then rank is lower continuous.

In fact, the set

$$M_r = \{A \in \mathcal{M}_{mn}(\mathbb{R}) : \operatorname{rank}(A) > r\}$$

is open in $\mathcal{M}_{mn}(\mathbb{R})$ since if $\operatorname{rank}(A) > r$, then A has a invertible squre submatrix with order $> r$. By the continuity of determinant, there is an neighborhood U of A in $\mathcal{M}_{mn}(\mathbb{R})$ such that for any matrix $B \in U$, the squre submatrix of B at the same place is invertible. This implies $\operatorname{rank}(B) > r$, thus $U \subseteq M_r$.

1.2.2 Continuous functions

Definition 1.2.6. *A mapping f of a topological space X into a topological space Y is said to be* ***continuous at a point*** *$x_0 \in X$ if, given any neighbourhood V of $f(x_0)$ in Y, there is a neighbourhood U of x_0 in X such that the relation $x \in U$ implies $f(x) \in V$.*

The relation "for each $x \in U$, $f(x) \in V$" is equivalent to $f(U) \subseteq V$ or again to $U \subseteq f^{-1}(V)$; in view of the neighbourhood axiom (U1) we see that the above definition is equivalent to the following: $f : X \to Y$ is said to be continuous at the point x_0 if, for each neighbourhood V of $f(x_0)$ in Y, $f^{-1}(V)$ is a neighbourhood of x_0 in X. Moreover, it is sufficient that $f^{-1}(V)$ is a neighbourhood of x_0 for each neighbourhood V belonging to a fundamental system of neighbourhoods of $f(x_0)$ in Y.

Proposition 1.2.7. *Let f be a mapping of a topological space X into a topological space Y. If f is continuous at x, and if x lies in the closure of a subset A of X, then $f(x)$ lies in the closure of $f(A)$.*

Proof. Let V be a neighbourhood of $f(x)$ in Y. Since f is continuous at x, $f^{-1}(V)$ is a neighbourhood of x in X. Hence $f^{-1}(V)$ meets A, from which it follows that V meets $f(A)$, and therefore $f(x)$ is in the closure of $f(A)$. □

Proposition 1.2.8. *Let X, Y, Z be three topological spaces; let f be a mapping of X into Y, continuous at $x \in X$; let g be a mapping of Y into Z, continuous at $f(x)$. Then the composition $h = g \circ f : X \to Z$ is continuous at x.*

Proof. Let W be a neighbourhood of $h(x) = g(f(x))$ in Z. Since g is continuous at $f(x)$ it follows that $g^{-1}(W)$ is a neighbourhood of $f(x)$ in Y. But f is continuous at x, hence $f^{-1}(g^{-1}(W)) = h^{-1}(W)$ is a neighbourhood of x in X, and therefore h is continuous at x. □

Definition 1.2.9. *A mapping of a topological space X into a topological space Y is said to be* ***continuous on X*** *(or just continuous) if it is continuous at each point of X.*

Example 1.2.10 (Example of continuous maps).

(a) The identity mapping of a topological space X onto itself is continuous.

(b) A constant map of a topological space into a topological space is continuous.

(c) Every mapping of a discrete space into a topological space is continuous.

Theorem 1.2.11. *Suppose X and Y are topological spaces, and $f : X \to Y$ is any map. Then the following statements are equivalent:*

(i) f is continuous on X.

(ii) For every subset A of X, $f(\overline{A}) \subseteq \overline{f(A)}$.

(iii) For every subset B of Y, $f^{-1}(\operatorname{Int} B) \subseteq \operatorname{Int} f^{-1}(B)$.

(iv) The inverse image under f of every closed subset of Y is a closed subset of X.

(v) The inverse image under f of every open subset of Y is an open subset of X.

Also, for f to be continuous, it is sufficient that (v) holds for bases of Y.

Proof. We have already seen (i) implies (ii). To see (ii) implies (iv), let F be a closed subset of Y and let $E = f^{-1}(F)$; then by hypothesis

$$f(\overline{E}) \subseteq \overline{f(E)} \subseteq F$$

hence $\overline{E} \subseteq f^{-1}(F) = E$, so that E is closed. By virtue of the relation $f^{-1}(Y \setminus U) = X \setminus f^{-1}(U)$ for every subset U of Y, (iv) implies (v).

Now suppose that (v) is satisfied. Then for any subset B of Y, $f^{-1}(\operatorname{Int} B)$ is open in X and contained in $f^{-1}(B)$, hence $f^{-1}(\operatorname{Int} B) \subseteq \operatorname{Int} f^{-1}(B)$. Finally, assume (iii) and let x be any point of X and B be any neighbourhood of $f(x)$ in Y; then there exists an open set W in Y such that $f(x) \in W \subseteq B$, and thus $f^{-1}(W) \subseteq \operatorname{Int} f^{-1}(W) \subseteq \operatorname{Int} f^{-1}(B)$. This means $f^{-1}(B)$ is a neigbourhood of x, which proves (i). The last remark is obvious, so the proof is completed. □

One may also wonder when do the converse inclusions in Theorem 1.2.11(ii) and (iii) hold. In fact, we have the following result.

Proposition 1.2.12. *Suppose X and Y are topological spaces, and $f : X \to Y$ is any map.*

(a) f is closed if and only if $f(\overline{A}) \supseteq \overline{f(A)}$ for all $A \subseteq X$.

(b) f is open if and only if $f^{-1}(\operatorname{Int} B) \supseteq \operatorname{Int} f^{-1}(B)$ for all $B \in Y$.

Proof. If f is a closed map, then $f(\overline{A})$ is a closed subset in Y containing $f(A)$. This implies $\overline{f(A)} \subseteq f(\overline{A})$. Conversely, if $\overline{f(A)} \subseteq f(\overline{A})$ holds, so that for closed subset A,

$$f(A) = f(\overline{A}) \supseteq \overline{f(A)},$$

then $f(A)$ is closed.

If f is open, let $x \in \operatorname{Int} f^{-1}(B)$ and U be an open set such that $x \in U \subseteq f^{-1}(B)$. Then $f(U)$ is an open set contained in B, hence $f(x) \in \operatorname{Int}(B)$, and $x \in f^{-1}(\operatorname{Int} B)$. Conversely, let U be open in X; if $f(U)$ is not open, then there is $x \in U$ such that $f(x) \notin \operatorname{Int} f(U)$. That is, $x \notin f^{-1}(\operatorname{Int} f(U))$. Since $f^{-1}(\operatorname{Int} f(U)) \supseteq \operatorname{Int} f^{-1}(f(U))$, we then get $x \notin \operatorname{Int} f^{-1}(f(U))$. But $\operatorname{Int} f^{-1}(f(U))$ contains U, this is a contradiction. □

Proposition 1.2.13 (Properties of continuous maps).

(a) If $f : X \to Y$ and $g : Y \to Z$ are two continuous mappings, then $g \circ f : X \to Z$ is continuous.

(b) For a bijection f of a topological space X onto a topological space Y to be a homeomorphism, it is necessary and nifficient that f and the inverse of f are continuous (or, as is also said, that f is bicontinuous).

Proof. The first assertion is an immediate consequence of Proposition 1.2.8; the second follows from Theorem 1.2.11 and the definition of a homeomorphism. □

Theorem 1.2.11 shows that we may take the continuous mappings as morphisms of topological structures; from now on, we shall assume that we have made this choice of morphisms. In accordance with the general definitions, this allows us to define an ordering on the set of topologies on a given set X, which coincides with our definition of comparability of topologies. The criteria for a mapping to be continuous give the following criterion:

Proposition 1.2.14. *Given two topologies $\mathcal{T}_1$ and $\mathcal{T}_2$ on a set X, the following statements are equivalent:*

(i) $\mathcal{T}_1$ is finer than $\mathcal{T}_2$.

(ii) For each $x \in X$, each neighbourhood of X for $\mathcal{T}_2$ is a neighbourhood of x for $\mathcal{T}_1$.

(iii) For each subset A of X, the closure of A in $\mathcal{T}_1$ is contained in the closure of A in $\mathcal{T}_2$.

(iv) Every subset of X which is closed in $\mathcal{T}_2$ is closed in $\mathcal{T}_1$.

(v) Every subset of X which is open in $\mathcal{T}_2$ is closed in $\mathcal{T}_1$.

1.2.3 Initial topologies

Proposition 1.2.15. *Let X be a set, let $(Y_i)_{i\in I}$ be a family of topological spaces, and for each $i \in I$ let f_i be a mapping of X into Y_i. Let $\mathcal{S}$ be the set of subsets of X of the form $f_i^{-1}(U_i)$, where $i \in I$ and U_i is open in Y_i. Then $\mathcal{S}$ is a subbase of a topology $\mathcal{T}$ on X which is the initial topological structure on X for the family $(f_i)_{i\in I}$ and in particular is the coarsest topology on X for which the mappings f_i are continuous. More precisely, if g is a mapping of a topological space Z into X, then g is continuous at a point $z \in Z$ (with X carrying the topology $\mathcal{T}$) if and only if each of the functions $f_i \circ g$ is continuous at z.*

Proof. The topology $\mathcal{T}$ is just that induced by the subbase $\int$. We shall prove the last assertion of the proposition, which implies the others by reason of the general properties of initial structure. In the first place, the definition of $\mathcal{S}$ shows that the f_i are continuous on X; hence, if g is continuous at z, so are the mappings $f_i \circ g$. Conversely, suppose that all the mappings $f_i \circ g$ are continuous at z, and let U be a neighbourhood of $g(z)$ in X; by definition, there is a finite subset J of I, and for each $i \in J$ an open subset V_i of Y_i such that V contains the set $\bigcap_{i=1}^n f_i^{-1}(V_i)$ and $g(z)$ belongs to this set. It follows that

$$g^{-1}(U) \supseteq g^{-1}\Big(\bigcap_{i=1}^{n} f_i^{-1}(V_i)\Big) = \bigcap_{i\in J}(f_i \circ g)^{-1}(V_i)$$

and the hypothesis implies that each of the sets $(f_i \circ g)^{-1}(V_i)$ is a neighbourhood of z in Z; hence $g^{-1}(V)$ is also a neighbourhood of z in Z. This completes the proof. □

The topology $\mathcal{T}$ is called the **initial topology** induced by the family $(f_i)_{i\in I}$. It is clear that if $\mathcal{B}_i$ is a base of the topology of Y_i; then the set $\mathcal{S}'$ of subsets of X of the form $f_i^{-1}(B_i)$ for $i \in I$ and $B_i \in \mathcal{B}_i$ for each $i \in I$ is also a subbase of the topology $\mathcal{T}$.

The general properties of initial structures imply in particular the following transitivity property:

Proposition 1.2.16. *Let X be a set, $(Z_\beta)_{\beta\in J}$ a family of topological spaces, $(J_\alpha)_{\alpha\in I}$ a partition of B and $(Y_\alpha)_{\alpha\in I}$ a family of sets indexed by I. For each $\alpha \in I$, let g_α be a mapping of X into Y_α; and for each $\beta \in J_\alpha$, let $h_{\beta\alpha}$ be a mapping of Y_α into Z_β, and put $f_\beta = h_{\beta\alpha} \circ g_\alpha$.*

$$X \xrightarrow{g_\alpha} Y_\alpha \xrightarrow{h_{\beta\alpha}} Z_\beta$$

If each Y_α carries the initial topology induced by $(h_{\beta\alpha})_{\beta\in J_\alpha}$ then the initial topology on X induced by $(f_\beta)_{\beta\in J}$ is the same as the initial topology induced by $(g_\alpha)_{\alpha\in I}$.

Example 1.2.17 (Example of initial topologies).

(a) Let X be a set, Y a topological space, f a mapping of X into Y; the initial topology $\mathcal{T}$ on X induced by f is called the **inverse image** under f of the topology of Y. It follows from Proposition 1.2.15 and the formula for the inverse image of a union and an intersection that the open (resp. closed) sets in the topology $\mathcal{T}$ are the inverse images under f of the open (resp. closed) sets of Y; consequently, for each $x \in X$, the sets $f^{-1}(W)$, where W runs through a neighbourhoods base of $f(x)$ in Y, form a fundamental system of neighbourhoods of x in the topology $\mathcal{T}$. Later we shall study, under the name of induced topology,

the particular case in which X is a subset of Y and f is the canonical injection $X \to Y$; X, with the induced topology, is then called a **subspace** of Y.

(b) Every family $(\mathcal{T}_i)_{i\in I}$ of topologies on a set X has a **least upper bound** $\mathcal{T}$ in the ordered set of all topologies on X, i.e. there exists a topology on X which is coarsest among all the topologies on X which are finer than each of the $\mathcal{T}_i$. To see this we may apply Proposition 1.2.15, taking Y_i to be the set X with the topology $\mathcal{T}_i$ and f_i to be the identity map $X \to X$. Then $\mathcal{T}$ is the initial topology induced by $(f_i)_{i\in I}$.

(c) Let $\mathcal{S}$ be an arbitrary set of subsets of a set X, not necessarily covers X. Amongst the topologies on X for which the sets of $\mathcal{S}$ are open, there is a topology $\mathcal{T}$ which is coarser than all the others and which is called the topology generated by $\mathcal{S}$: For each set $U \in \mathcal{S}$ let $\mathcal{T}_U$ be the topology whose open sets are $\emptyset$, U and X; then $\mathcal{T}$ is just the least upper bound of the topologies $\mathcal{T}_U$. By Proposition 1.2.15, if $\mathcal{B}$ is the set of finite intersections of sets belonging to $\mathcal{S}$, then $\mathcal{B}$ is a base of the topology $\mathcal{T}$. Note that, if we take $\mathcal{S}' = \mathcal{S} \cup \{X\}$, then $\mathcal{T}$ is exactly the topology generated by $\mathcal{S}'$ as a subbase. In view of this, we may also make abuse of language and say $\mathcal{S}$ is a *subbase* of $\mathcal{T}$.

(d) Let $(X_i)_{i\in I}$ be a family of topological spaces. The initial topology induced on the product space $X = \prod_{i\in I} X_i$ by the projections $\pi_i : X \to X_i$ is called the product of the topologies of the X_i's; we shall study it in more detail later.

1.2.4 Final topologies

Proposition 1.2.18. *Let X be a set, let $(Y_i)_{i\in I}$ be a family of topological spaces, and for each $i \in I$ let f_i be a mapping of Y_i into X. Let $\mathcal{T}$ be the set of subsets U of X such that $f_i^{-1}(U)$ is open in Y, for each $i \in I$. Then $\mathcal{T}$ is the final structure on X for the family (f_i), and in particular $\mathcal{T}$ is the finest topology on X for which the mappings f_i are continuous. In other words, if g is a mapping of X into a topological space Z, then g is continuous (with X carrying the topology $\mathcal{T}$) if and only if each of the mappings $g \circ f_i$ is continuous.*

Proof. It is immediately verified that $\mathcal{T}$ satisfies the axioms (O1) and (O2). We shall prove the last assertion of the proposition, which implies the other assertions by reason of the general properties of final structures. It is clear that the f_i are continuous in the topology $\mathcal{T}$, by the definition of $\mathcal{T}$; hence if g is continuous, so is each mapping $g \circ f_i$. Conversely, suppose that each $g \circ f_i$ is continuous, and let V be an open set in Z; by hypothesis, $f_i^{-1}(g^{-1}(V))$ is open in Y_i for each $i \in I$; hence $g^{-1}(V) \in \mathcal{T}$, and the proof is complete. □

The topology in Proposition 1.2.18 is called the **final topology** induced by (f_i). It follows from definition that a subset F of X is closed in this topology if and only if $f_i^{-1}(F)$ is closed for all $i \in I$. The general properties of final structures imply the following transitivity property:

Proposition 1.2.19. *Let X be a set, $(Z_\beta)_{\beta\in J}$ a family of topological spaces, $(J_\alpha)_{\alpha\in I}$ a partition of J and $(Y_\alpha)_{\alpha\in I}$ a family of sets indexed by I. For each $\alpha \in I$, let g_α be a mapping of Y_α into X; and for each $\beta \in J_\alpha$, let $h_{\alpha\beta}$ be a mapping of Z_β into Y_α, and put $f_\beta = g_\alpha \circ h_{\alpha\beta}$.*

$$Z_\beta \xrightarrow{h_{\alpha\beta}} Y_\alpha \xrightarrow{g_\alpha} X$$

If each Y_α carries the final topology induced by $(h_{\alpha\beta})_{\beta\in J_\alpha}$ then the final topology on X induced by $(f_\beta)_{\beta\in J}$ is the same as the final topology induced by $(g_\alpha)_{\alpha\in I}$.

Example 1.2.20 (Example of final topologies).

(a) Let X be a topological space, R an equivalence relation on X, $Y = X/R$ the quotient set of X with respect to the relation R, $\pi : X \to Y$ the canonical mapping. The final topology on Y induced by π is called the **quotient** of the topology of X by the relation R; we shall study it in more detail later.

(b) Every family $(\mathcal{T}_i)_{i\in I}$ of topologies on a set X has a greatest lower bound $\mathcal{T}$ in the set of all topologies on X, i.e. $\mathcal{T}$ is the finest of all the topologies on X which are coarser than each of the $\mathcal{T}$. To see this we may apply Proposition 1.2.18, taking Y_i to be the set X with the topology $\mathcal{T}_i$ and f_i to be the identity mapping $Y_i \to X$. Then the collection $\mathcal{T}$ is given by the intersection of all $\mathcal{T}_i$. It is also called the **intersection** of the topologies $\mathcal{T}_i$.

(c) Let $(X_i)_{i\in I}$ be a family of topological spaces and $X = \coprod_{i\in I} X_i$ be the coproduct of X_i's; for each $i \in I$, let ι_i be the canonical (injective) mapping of X_i into X. The final topology $\mathcal{T}$ on X induced by the mappings ι_i is called the **coproduct** of the topologies of the X_i and X with this topology is said to be the **coproduct** of the topological spaces X_i. Let us identify each of the X_i with a subset of X by means of ι_i; then a set $A \subseteq X$ is open (resp. closed) in the topology $\mathcal{T}$ if and only if each of the sets $A \cap X_i$ is open (resp. closed) in X_i. In particular, each of the X_i is both open and closed.

The following proposition generalizes the situation of coproducts of a family of topological spaces.

Proposition 1.2.21. *Let X be a set, $(X_i)_{i\in I}$ a family of subsets of X. Suppose each X_i carries a topology $\mathcal{T}_i$ such that for each pair of indices (i, j):*

(a) $X_i \cap X_j$ is open (resp. closed) in each of the topologies $\mathcal{T}_i$ and $\mathcal{T}_j$.

(b) The topologies induced on $X_i \cap X_j$ by $\mathcal{T}_i$ and $\mathcal{T}_j$ coincide.

Let $\mathcal{T}$ be the final topology on X induced by the inclusions $\iota_i : X_i \to X$, then for each $i \in I$ the subset X_i is open (resp. closed) in X in the topology $\mathcal{T}$ and the topology induced by $\mathcal{T}$ on X_i coincides with $\mathcal{T}_i$.

Proof. In view of Proposition 1.2.18, it is enough to show that for each i and each subset A_i of X_i, the following statements are equivalent:

(i) A_i is open (resp. closed) in the topology $\mathcal{T}_i$.

(ii) For each $j \in I$, $A_i \cap X_j$ is open (resp. closed) in the topology $\mathcal{T}_j$.

It is clear that (ii) implies (i) by taking $j = i$. Conversely, if (i) is satisfied, then $A_i \cap X_j$ is open (resp. closed) in $X_i \cap X_j$ for the topology $\mathcal{T}_{ij}$ induced on $X_i \cap X_j$ by $\mathcal{T}_i$; but $\mathcal{T}_{ij}$ is also the topology induced on $X_i \cap X_j$ by $\mathcal{T}_j$; hence $A_i \cap X_j$ is also the intersection of $X_i \cap X_j$ with a subset $B_j \subseteq X_j$ which is open (resp. closed) in the topology $\mathcal{T}_j$. Since $X_i \cap X_j$ is also open (resp. closed) in $\mathcal{T}_j$, so is $A_i \cap X_j$. This completes the proof. □

1.2.5 Subspaces of a topological space

Let A be a subset of a topological space X. We have defined the topology induced on A by the topology of X as the inverse image of the latter under the canonical injection $A \to X$. An equivalent definition is as follows:

Definition 1.2.22. *Let A be a subset of a topological space X. The topology induced on A by the topology of X is that in which the open sets are the intersections with A of open sets of X. The set A with this topology is called a* ***subspace*** *of X.*

By the transitivity of initial topology (or from definition) we see that, if $B \subseteq A \subseteq X$, the subspace B of X is identical with the subspace B of the subspace A of X. If $\mathcal{S}$ is a subbase (resp. base) of the topology of X, its trace $\mathcal{S}_A$ on A is a subbase (resp. a base) of the topology induced on A.

In all questions which involve the elements or subsets of A, it is essential to distinguish carefully between their properties as points (resp. subsets) of X, and their properties as points (resp. subsets) of the subspace A. We shall make this distinction by using the phrases "in A", "with respect to A, or "relative to A" to refer to properties in the latter category (possibly contrasting them with the phrases "in X", "with respect to X", "relative to X").

An open set of the subspace A need not be open in X, and a closed subset of A need not be closed. For these two conditions to be true, we have the following result.

Proposition 1.2.23. *Let A be a subspace of a topological space X.*

(a) In order that every set which is open in A should be open in X it is necessary and sufficient that A is open in X.

(b) In order that every set which is closed in A should be closed in X it is necessary and sufficient that A is closed in X.

(c) Every neighbourhood of x relative to A is a neighbourhood of x relative to X if and only if A is a neighbourhood of x in X.

Proof. The condition in (a) is necessary, since A is open in A, and it is sufficient by virtue of (O2) and the definition of subspace topology. The other parts can be proved simialrly. □

Now let X be an ordered set in the order topology, and let A be a subset of X. The order relation on X, when restricted to A, makes A into an ordered set. However, the resulting order topology on A need not be the same as the topology that A inherits as a subspace of X. We give one example where the subspace and order topologies on A agree, and two examples where they do not.

Example 1.2.24. Consider the subset $A = [0, 1]$ of the real line $\mathbb{R}$, in the subspace topology. The subspace topology has as basis all sets of the form $(a, b) \cap A$, where (a, b) is an open interval in $\mathbb{R}$. Such a set is of one of the following types:

$$(a,b) \cap A = \begin{cases} (a,b) & \text{if } a \text{ and } b \text{ are in } A, \\ [0,b) & \text{if only } b \text{ is in } A, \\ (a,1] & \text{if only } a \text{ is in } A, \\ A \text{ or } \varnothing & \text{if neither } a \text{ nor } b \text{ is in } A. \end{cases}$$

By definition, each of these sets is open in A. But sets of the second and third types are not open in the larger space $\mathbb{R}$.

Note that these sets form a basis for the order topology on A. Thus, we see that in the case of the set $A = [0, 1]$, its subspace topology (as a subspace of $\mathbb{R}$) and its order topology are the same.

Example 1.2.25. Let A be the subset $[0, 1) \cup \{2\}$ of $\mathbb{R}$. In the subspace topology on A the singleton $\{2\}$ is open, because it is the intersection of the open set $(3/2, 5/2)$ with A. But in the order topology on A, the set $\{2\}$ is not open. Any basis element for the order topology on A that contains 2 is of the form $(a, 2]$ for some $a \in A$; such a set necessarily contains points of A less than 2.

Example 1.2.26. Let $I = [0, 1]$. The dictionary order on $I \times I$ is just the restriction to $I \times I$ of the dictionary order on the plane $\mathbb{R} \times \mathbb{R}$. However, the dictionary order topology on $I \times I$ is not the same as the subspace topology on $I \times I$ obtained from the dictionary order topology on $\mathbb{R} \times \mathbb{R}$! For example, the set $\{1/2\} \times (1/2, 1]$ is open in $I \times I$ in the subspace topology, but not in the order topology since $(1/2, 1)$ is not the biggest point of $I \times I$ in dictionary order. The set $I \times I$ in the dictionary order topology will be called the **ordered square**.

Proposition 1.2.27. *If A and B are two subsets of a topological space X, and $B \subseteq A$, then the closure of B in the subspace A is the intersection with A of the closure $\overline{B}$ of B in X.*

Proof. If $x \in A$, every neighbourhood of x in A is of the form $V \cap A$, where V is a neighbourhood of x in X. Since $V \cap B = (V \cap A) \cap B$, it follows that x lies in the closure of B with respect to A if and only if x lies in the closure of B with respect to X. □

Corollary 1.2.28. *A subset B of A is dense in A if and only if $\overline{B} \supseteq A$ in X, if and only if $\overline{B} = \overline{A}$.*

Corollary 1.2.29. *It follows that if A, B, C are three subsets of X such that $C \subseteq B \subseteq A$, and if B is dense in A, and C is dense in B, then C is dense in A.*

Proposition 1.2.30. *Let A be a dense subset of a topological space X; then for each $x \in A$ and each neighbourhood V of x relative to A, the closure $\overline{V}$ of V in X is a neighbourhood of x in X.*

Proof. Since C is a neigbourhood of x relative to A, there exists an open subset U of X such that $x \subseteq U \cap A \subseteq V$. Then since U is open, by Proposition 1.1.23 we have

$$\overline{V} \supseteq \overline{U \cap A} \supseteq U \cap \overline{A} = U,$$

whence $\overline{V}$ is a neigbourhood of x in X. □

Now we consider continuity with respect to subspaces. Let X and Y be two topological spaces, f a mapping of X into Y, B a subset of Y which contains $f(X)$. The definition of the induced topology as an initial topology shows that f is continuous at $x \in X$ if and only if the mapping of X into the subspace B of Y, having the same graph as f, is continuous at x.

Now let A be a subset of X; if f is continuous at $x \in A$ (resp. continuous on X), its restriction $f|_A$ is a mapping of the subspace A into Y, which is continuous at x (resp. continuous on A). We shall sometimes say that a mapping $f : X \to Y$ is continuous relative to A at $x \in A$ (resp. continuous relative to A) if its restriction $f|_A$ is continuous at x (resp. continuous on A).

It should be noted that $f|_A$ can be continuous without f being continuous at any point of X; an example of this phenomenon is provided by the characteristic function χ_A of a subset A of X which is such that both A and its complement are dense in X. The function χ_A, being regarded as a mapping of X into the discrete space $\{0, 1\}$ is not continuous at any point of X, but its restriction to A is constant and therefore continuous.

On the other hand, if A is a neighbourhood in X of a point $x \in A$, and if $f : X \to Y$ is such that $f|_A$ is continuous at x, then f is continuous at x; for each neighbourhood of x in A is a neighbourhood of x in X (local character of continuity).

To conlude, we give a condition in which the openness of a subset of X can be detected by an cover of X by subspaces.

Proposition 1.2.31. *Let $(A_i)_{i\in I}$ be a family of subsets of a topological space X, such that one of the following properties holds:*

(a) the interiors of A_i's cover X;

(b) $(A_i)_{i\in I}$ is a locally finite closed covering of X.

Then a subset of X is open (resp. closed) in X if and only if each of its intersection with A_i is open (resp. closed) in A_i.

Proof. Clearly if U is open (resp. closed) in X, then $U \cap A_i$ is open (resp. closed) in A_i. Conversely, suppose first that condition (a) is satisfied; since $U^c \cap A_i = A_i \setminus (U \cap A_i)$, it is enough, by duality, to consider the case in which each of the $U \cap A_i$ is open with respect to A_i. In this case $U \cap \operatorname{Int} A_i$ is open in $\operatorname{Int} A_i$ for each $i \in I$, and therefore open in X; and since $U = \bigcup_{i\in I}(U \cap \operatorname{Int} A_i)$ by hypothesis, it follows that U is open in X.

Now suppose that (b) is satisfied and let $F \subseteq X$; by duality again, we need only consider the case in which each of the $F \cap A_i$ is closed in A_i and therefore closed in X. Since the family $(F \cap A_i)$ is locally finite and $F = \bigcup_{i\in I}(F \cap A_i)$, it follows from Lemma 1.13.2 that F is closed in X. □

1.3 Quotient spaces and quotient maps

1.3.1 Quotient spaces and maps

Let X be a topological space, R an equivalence relation on X. Recall that the quotient space of X by R is the quotient set X/R with the quotient topology induced by the canonical map $\pi : X \to X/R$. Unless the contrary is expressly stated, whenever we speak of X/R as a topological space, it is to be understood that we mean the quotient space of X by R. We shall often say that this topological space is the space obtained by identifying the points of X which belong to the same equivalence class mod R.

By the definition of quotient topology, the open sets in X/R are the sets $U \subseteq X/R$ such that $\pi^{-1}(U)$ is open in X. In other words, the open (resp. closed) sets in X/R are in one-to-one correspondence with the open (resp. closed) subsets of X which are *saturated* with respect to R and are the canonical images of these subsets. (Recall that a subset $U \subseteq X$ is **saturated** with respect to a equivalent relation if it is a union of equivalent classes, or equivalently $U = \pi^{-1}(\pi(U))$.)

From the characterization of final topology and transitivity, we get the following results for quotient topology.

Proposition 1.3.1. *Let X be a topological space, R an equivalence relation on X, π the canonical mapping of X onto X/R; then a mapping f of X/R into a topological space Y is continuous if and only if $f \circ \pi$ is continuous on X.*

Proposition 1.3.2 (Transitivity of quotient spaces). *Let R and S be two equivalence relations on a topological space X such that $R \subseteq S$, and let S/R be the quotient equivalence relation on the quotient space X/R. Then the canonical biJection $(X/R)/(S/R) \to X/S$ is a homeomorphism.*

Note that, Proposition 1.3.1 also shows that there is a one-to-one correspondence between the continuous mappings of X/R into Y and the continuous maps of X into Y which are constant on each equivalence class mod R.

Example 1.3.3. Consider the equivalence relation mod $\mathbb{Z}$ on the real line $\mathbb{R}$; the quotient space of $\mathbb{R}$ by this relation is called the one-dimensional torus and is denoted by $\mathbb{T}$. The equivalence class of a point $x \in \mathbb{R}$ consists of all the points $x + n$, where n runs through the set $\mathbb{Z}$ of integers. By Proposition 1.3.1, there is a one-to-one correspondence between the continuous functions on $\mathbb{T}$ and the continuous functions on $\mathbb{R}$ which are periodic with period 1.

Corollary 1.3.4. *Let X, Y be two topological spaces, R (resp. S) an equivalence relation on X (resp. Y), and let $f : X \to Y$ be a continuous mapping which is compatible with the equivalence relations R and S. Then the mapping $\tilde{f} : X/R \to Y/S$ induced by f is continuous.*

Proof. Let π_R and π_S be the canonical projection of R and S. To prove the claim, let V be a open subset of Y/S, so that $\pi_S^{-1}(V)$ is open in Y. Then from the following commutative diagram

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "\pi_R"'] & Y \arrow[d, "\pi_S"] \\ X/R \arrow[r, "\tilde{f}"] & Y/S \end{tikzcd}$$

and the continuity of f, we conlude that $f^{-1}(\pi_S^{-1}(V)) = \pi_R^{-1}(\tilde{f}^{-1}(V))$ is open in X, whence $\tilde{f}^{-1}(V)$ is open in X/R. This proves the corollary. □

Now using the notation of quotient topologies, we can establish a canonical decomposition of a continuous map. To be more precise, let X and Y be two topological spaces, $f : X \to Y$ a continuous map, R the equivalence relation $f(x) = f(y)$ on X. Consider the canonical decomposition

$$\begin{tikzcd} X \arrow[r, "\pi"] \arrow[rrr, bend right, "f"'] & X/R \arrow[r, "\tilde{f}"] & f(X) \arrow[r, "\iota"] & Y \end{tikzcd}$$

where π is the canonical (surjective) mapping of X onto the quotient space X/R, ι is the canonical injection of the subspace $f(X)$ into Y, and $\tilde{f}$ is the bijection associated with f. It is immediately seen that $\tilde{f}$ is continuous (by Corollary 1.3.4). But the bijection $\tilde{f}$ is not necessariry a homeomorphism.

Proposition 1.3.5. *Let $f = \pi \circ \tilde{f} \circ \iota$ be the canonical decomposition of a continuous mapping $f : X \to Y$, and let R denote the equivalence relation $f(x) = f(y)$. Then the following three conditions are equivalent:*

(i) $\tilde{f}$ is a homeomorphism of X/R onto $f(X)$.

(ii) The image under f of every open set which is saturated with respect to R is an open set in the subspace $f(X)$.

(iii) The image under f of every closed set which is saturated with respect to R is a closed set in the subspace $f(X)$.

Proof. Since $\tilde{f}$ is bijective, it is a homeomorphism if and only if $\tilde{f}$ is open or closed. Now note that an open subset of X/R is the image under π of a saturated open subset of X, so the claim follows. □

Example 1.3.6. Let X be a topological space and $(X_i)_{i\in I}$ a covering of X. Since for each $i \in I$ we have an inclusion $\iota_i : X_i \to X$, we can consider the coproduct $\widetilde{X} = \coprod_{i\in I} X_i$ and get a map $\Phi : \widetilde{X} \to X$. If we identify each X_i as a subspace of $\widetilde{X}$, then Φ is a homeomorphism when restricted to each X_i. Let R be the equivalence relation $\Phi(x) = \Phi(y)$; the quotient space $\tilde{X}/R$ is thus obtained by "pasting together" the overlaps of X_i's.

Consider the bijection $\phi : \widetilde{X}/R \to X$ associated with Φ, which is always continuous. In general ϕ is not a homeomorphism, as is shown by the example in which each X_i consists of a single point and X is not discrete.

However, if the interiors of the X_i cover X, or if $(X_i)_{i\in I}$ is a locally finite closed covering of X, then ϕ is a homeomorphism: for if U is any open subset of Y which is saturated with respect to R, then $\Phi(U)$ is open in X because for each $i \in I$ the set

$$\Phi(U) \cap X_i = \iota_i(U \cap Y_i)$$

is open in X_i since Φ_i is a homeomorphism on each X_i, hence $\Phi(U)$ is open by Proposition 1.2.31.

The following proposition gives a simple sufficient condition for $\tilde{f}$ to be a homeomorphism:

Proposition 1.3.7. *Let $f : X \to Y$ be a continuous surjection, and let R denote the equivalence relation $f(x) = f(y)$. If there is a continuous section $s : Y \to X$ associated with f, then the mapping $\tilde{f} : X/R \to Y$ associated with f is a homeomorphism, and s is a homeomorphism of Y onto the subspace $s(Y)$ of X.*

Proof. If $\pi : X \to X/R$ is the canonical mapping, then $\tilde{f}$ and $\pi \circ s$ are bijective, continuous and inverse to each other; likewise s and the restriction of f to $s(Y)$ are bijective, continuous and inverse to each other. These prove the claim. □

If R is an equivalence relation on a topological space X and $\pi : X \to X/R$ is the canonical mapping, a continuous section $s : X/R \to X$ associated with f is also called a **continuous section** of X with respect to R; the subspace $s(X/R)$ of X is then homeomorphic to X/R. If we are given $s(X/R)$, then s is uniquely determined; $s(X/R)$ is often called, by abuse of language, a **(continuous) section** of X with respect to R.

Now let X and Y be topological spaces, and $q : X \to Y$ be a map. Then q is called a **quotient map** if it is surjective and Y has the quotient topology induced by q. Once q is known to be

surjective, to say it is a quotient map is the same as saying that V is open in Y if and only if $q^{-1}(V)$ is open in X. It is immediate from the definition that every quotient map is continuous.

Proposition 1.3.8. *Let $f : X \to Y$ be a continuous surjection. If f is an open map, or a closed map, then f is an quotient map.*

Proof. Suppose that f is an open map. Let U be a subset of Y. By continuity, if U is open in Y then $f^{-1}(U)$ is open in X. On the other hand, since f is a surjection, we have $f(f^{-1}(U)) = U$. Hence $f^{-1}(U)$ is open if and only if U is open. A similar proof applies with open replaced by closed. □

It is easy to see a composition of quotient maps is a quotient map; this fact follows from the equation

$$p^{-1}(q^{-1}(U)) = (q \circ p)^{-1}(U).$$

On the other hand, products of maps do not behave well; the cartesian product of two quotient maps need not be a quotient map. One needs further conditions on either the maps or the spaces in order for this statement to be true. One such, a condition on the spaces, is called local compactness. Another, a condition on the maps, is the condition that both the maps p and q be open maps. In that case, it is easy to see that $p \times q$ is also an open map, so it is a quotient map.

Example 1.3.9. A product of quotient maps need not to be a quotient map. Let $\pi : \mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$ be the quotient map and let $h = \pi \times \mathrm{id} : \mathbb{Q} \times \mathbb{Q} \to (\mathbb{Q}/\mathbb{Z}) \times \mathbb{Q}$. Let $r_0 = 1$ and for each non-zero $n \in \mathbb{N}$ let $r_n = \sqrt{2}/|n|$—thus r_n is irrational and $r_n \to 0$ as $n \to \infty$. Let A_n be any open subset of $[n, n+1] \times \mathbb{R}$ such that the closure of A_n meets $\{n, n+1\} \times \mathbb{R}$ in the two points (n, r_n) and (n, r_{n+1}). Let A be the union of these sets A_n, $n \in \mathbb{N}$, and let $B = \overline{A} \cap (\mathbb{Q} \times \mathbb{Q})$. Then B is closed in $\mathbb{Q} \times \mathbb{Q}$ and saturated with respect to h. By our construction of r_n, we see that in $(\mathbb{Q}/\mathbb{Z}) \times \mathbb{Q}$ the point $(\pi(0), 0)$ belongs to the closure of $h(B)$, so $h(B)$ is not closed. This then implies that h is not a quotient map.

Figure 3.1.1: The open subset A_n.

On the other hand, we have the following result for coproducts.

Proposition 1.3.10. *Let $(X_\alpha)_{\alpha \in A}$ and $(Y_\alpha)_{\alpha \in A}$ be topological spaces and for each $\alpha \in A$ let $p_\alpha : X_\alpha \to Y_\alpha$ be a quotient map. Then the map*

$$p : \coprod_\alpha X_\alpha \to \coprod_\alpha Y_\alpha$$

which coincides with p_α on X_α is a quotient map.

Proof. Let V be an subset in $\coprod_\alpha Y_\alpha$, then by the definition of p, we have

$$p^{-1}(V) = \bigcup_\alpha p_\alpha^{-1}(V \cap Y_\alpha),$$

so $p^{-1}(V) \cap X_\alpha = p_\alpha^{-1}(V \cap Y_\alpha)$. The claim now follows from by the definition of coproduct topology and the fact that each p_α is a quotient map. □

1.3.2 Quotient of a subspace

Let X be a topological space, A a subspace of X, and π the canonical map $X \to X/R$ of an equivalence relation R on X. Let R_A be the relation induced by R on A, and $\pi|_A = \iota \circ \tilde{\pi} \circ \pi_A$ be the canonical decomposition of $\pi|_A$, so that we have a commutative diagram

$$\begin{tikzcd} A \arrow[r, "\pi_A"] \arrow[rrr, bend right, "\pi|_A"'] & A/R_A \arrow[r, "\tilde{\pi}"] & \pi(A) \arrow[r, "\iota"] & X/R \end{tikzcd}$$

Proposition 1.3.11. *The canonical bijection $\tilde{\pi} : A/R_A \to \pi(A)$ is continuous. Furthermore, the following three statements are equivalent:*

(i) $\tilde{\pi}$ is a homeomorphism.

(ii) Every open subset of A which is saturated with respect to R_A is the intersection with A of an open subset of X which is saturated with respect to R.

(iii) Every closed subset of A which is saturated with respect to R_A is the intersection with A of a closed subset of X which is saturated with respect to R.

Proof. Note that A/R_A carries the quotient topology induced by π_A, and $\pi(A)$ carries the subspace topology induced by X/R. Now the claim follows from Proposition 1.3.5: if U is an open subset of A which is saturated with respect to R_A, and $\tilde{\pi}(U) = \pi(U)$ is the intersection with $\pi(A)$ of an open subset V of X/R, then U is the intersection with A of the open subset $\pi^{-1}(V)$ of X, which is saturated with respect to R; and conversely, if U is the intersection with A of an open subset W which is saturated with respect to R, then $\pi(U)$ is the intersection of $\pi(A)$ and $\pi(W)$, which is open in X/R. □

Corollary 1.3.12. *If A is an open (resp. closed) subset of X which is saturated with respect to R, then the canonical mapping $\tilde{\pi} : A/R_A \to \pi(A)$ is a homeomorphism.*

Proof. If A is open (resp. closed) in X and saturated with respect to R, and if $B \subseteq A$ is open (resp. closed) in A and saturated with respect to R_A, then B is open (resp. closed) in X and saturated with respect to R. □

Corollary 1.3.13. *If there is a continuous mapping $\varphi : X \to A$ such that $\varphi(x) \equiv x \bmod R$ for each $x \in X$, then $\pi(A) = X/R$ and the canonical mapping $\tilde{\pi} : A/R_A \to X/R$ is a homeomorphism.*

Proof. Since each equivalence class mod R meets A, the canonical image of $\pi(A)$ in X/R is the whole of X/R; on the other hand, if U is open in A and is saturated with respect to R_A, it follows from the hypothesis that $\varphi^{-1}(U)$ is the set obtained by saturating U with respect to R; since φ is continuous, $\varphi^{-1}(U)$ is open in X. The corollary follows from this fact by virtue of Proposition 1.3.11. □

Example 1.3.14. Let R denote the equivalence relation $x = y \bmod \mathbb{Z}$ on the real line $\mathbb{R}$ and let I denote the closed interval $[0, 1]$; I contains at least one point of each equivalence class mod R. The canonical mapping of I/R_I onto the torus $\mathbb{T}$ is a homeomorphism; for if F is closed in I (and hence in $\mathbb{R}$), in order to saturate F with respect to the relation R we have to take the union of the closed sets $F + n$ for all $n \in \mathbb{Z}$, which evidently form a locally finite family, so that their union is closed; the assertion follows from this. We remark that I/R_I is obtained by identifying the points 0 and 1 in I.

1.3.3 Hausdorff condition of quotient spaces

Typically, to prove that a given quotient space is Hausdorff, one has to resort to the definition. For open quotient maps, however, we have the following criterion.

Proposition 1.3.15. *Suppose $q : X \to Y$ is an open quotient map. Then Y is Hausdorff if and only if the set $\mathcal{R} := \{(x_1, x_2) : q(x_1) = q(x_2)\}$ is closed in $X \times X$.*

Proof. First assume Y is Hausdorff. If $(x_1, x_2) \notin \mathcal{R}$, then there are disjoint neighborhoods V_1 of $q(x_1)$ and V_2 of $q(x_2)$, and it follows that $q^{-1}(V_1) \times q^{-1}(V_2)$ is a neighborhood of (x_1, x_2) that is disjoint from $\mathcal{R}$. Thus $\mathcal{R}$ is closed. (This implication does not require the assumption that q is open.)

Conversely, assume $\mathcal{R}$ is closed. Given distinct points $y_1, y_2 \in Y$, choose $x_1, x_2 \in X$ such that $q(x_i) = y_i$. Because $(x_1, x_2) \notin \mathcal{R}$, there is a product neighborhood $U_1 \times U_2$ of (x_1, x_2) in $X \times X$ that is disjoint from $\mathcal{R}$. Since q is open, $q(U_1)$ and $q(U_2)$ are disjoint neighborhoods of y_1 and y_2, respectively. □

Corollary 1.3.16. *Suppose $\sim$ is an equivalence relation on a space X. If the quotient map $X \to X/\sim$ is an open map, then $X/\sim$ is Hausdorff if and only if $\sim$ is a closed subset of $X \times X$.*

Theorem 1.3.17. *Suppose X is a compact Hausdorff space and $q : X \to Y$ is a quotient map. Then the following are equivalent.*

(a) Y is Hausdorff.

(b) q is a closed map.

(c) The set $\mathcal{R} = \{(x_1, x_2) : q(x_1) = q(x_2)\}$ is closed in $X \times X$.

Proof. The implicaton $(a) \Rightarrow (b)$ is immediate by closed map lemma, and $(a) \Rightarrow (c)$ is proved just as in Proposition 1.3.15. Next we prove $(b) \Rightarrow (a)$. Assuming q is a closed map, we begin by showing that its fibers are compact. Every point $y \in Y$ is the image of some $x \in X$, and since $\{x\}$ is a closed subset of X, it follows that $\{y\} = q(\{x\})$ is a closed subset of Y. Thus by continuity, the fiber $q^{-1}(\{y\})$ is closed in X and hence compact.

To prove that Y is Hausdorff, suppose y_1 and y_2 are distinct points of Y. Then we can prove the disjoint compact subsets $q^{-1}(y_1)$ and $q^{-1}(y_2)$ of X have disjoint neighborhoods U_1 and U_2, respectively. Define subsets $W_1, W_2 \subseteq Y$ by

$$W_i = Y - q(X - U_i) = \{y \in Y : q^{-1}(y) \subseteq U_i\}$$

Then $y_i \in W_i$ for each i by construction, and W_1 and W_2 are disjoint because U_1 and U_2 are. To complete the proof, the fact that q is closed implies that W_i is open.

Finally, we prove $(c) \Rightarrow (a)$. Assuming that $\mathcal{R}$ is closed, we start again by showing that q has compact fibers. Given $y \in Y$ and $x \notin q^{-1}(y)$, let x_1 be any point in $q^{-1}(y)$. (Such a point exists because q is surjective.) Because $\mathcal{R}$ is closed and $(x, x_1) \notin \mathcal{R}$, there is a product neighborhood $U_1 \times U_2$ of (x_1, x) that is disjoint from $\mathcal{R}$. It follows that U_2 is a neighborhood of x disjoint from $q^{-1}(y)$, for if x_2 were a point in $U_2 \cap q^{-1}(y)$, then (x_1, x_2) would lie in $\mathcal{R} \cap (U_1 \times U_2)$, which is empty. Thus $q^{-1}(y)$ is closed in X and hence compact.

Now let y_1 and y_2 be distinct points in Y. As before, there are disjoint open subsets $U_1 \supseteq q^{-1}(y_1)$ and $U_2 \supseteq q^{-1}(y_2)$, and we define W_1, W_2 as before. These are disjoint sets containing y_1 and y_2, respectively, so we need only show they are open. Because q is a quotient map, W_i is open if and only if $q^{-1}(W_i)$ is open, which is the case if and only if $X - q^{-1}(W_i)$ is closed. From the definition of W_i, it follows that

$$\begin{aligned} X - q^{-1}(W_i) &= \{x \in X : q(x) \notin W_i\} = \{x \in X : q^{-1}(q(x)) \nsubseteq U_i\} \\ &= \{x \in X : \exists x \in X - U_i \text{ such that } q(x) = q(\tilde{x})\} \\ &= \pi_1(\mathcal{R} \cap (X \times X - U_i)) \end{aligned}$$

where $\pi_1 : X \times X \to X$ is the projection on the first factor. Observe that π_1 is a closed map by the closed map lemma. Our hypothesis on $\mathcal{R}$ implies that $\mathcal{R} \cap (X \times X - U_i)$ is closed in $X \times X$, and therefore $X - q^{-1}(W_i)$ is closed in X. □

1.3.4 Direct limit of topological spaces

Let $(X_\alpha)_{\alpha \in I}$ be a family of sets, and let X be the set which is the coproduct of the X_α. We shall identify each X_α with a subset of X by means of the canonical injection $\iota_\alpha : X_\alpha \to X$.

Let R be an equivalence relation on X such that each equivalence class of R has at most one element in each X_α; for each pair of indices (α, β) let $A_{\alpha\beta}$ be the subset of X_α consisting of the elements x for which there is an element $y \in X_\beta$ which belongs to the equivalence class of x. Clearly to each $x \in A_{\alpha\beta}$ there is a unique $y \in X_\beta$ which is congruent to x mod R; the mappings $\phi_{\beta\alpha} : A_{\alpha\beta} \to A_{\beta\alpha}$ so defined satisfy the following conditions:

(a) For each $\alpha \in I$, $\phi_{\alpha\alpha}$ is the identity mapping of $A_{\alpha\alpha} = X_\alpha$.

(b) For each triple of indices (α, β, γ) of I and each $x \in A_{\alpha\beta} \cap A_{\alpha\gamma}$, we have $\phi_{\beta\alpha}(x) \in A_{\beta\gamma}$ and $\phi_{\gamma\alpha}(x) = \phi_{\gamma\beta}(\phi_{\beta\alpha}(x))$.

Conversely, suppose that for each pair of indices (α, β) we are given a subset $A_{\alpha\beta}$ of X_α and a mapping $\phi_{\beta\alpha} : A_{\alpha\beta} \to A_{\beta\alpha}$ satisfying the conditions (a) and (b) above. It follows first of all from (b) applied to the triples (α, β, α) and (β, α, β) that $\phi_{\alpha\beta} \circ \phi_{\beta\alpha}$ (resp. $\phi_{\beta\alpha} \circ \phi_{\alpha\beta}$) is the restriction of $\phi_{\alpha\alpha}$ (resp. $\phi_{\beta\beta}$) to $A_{\alpha\alpha}$ (resp. $A_{\beta\beta}$); hence we deduce from (a) that $\phi_{\beta\alpha}$ and $\phi_{\alpha\beta}$

are bijections which are mverses of each other. Now let R be the relation "there exist α, β such that $x \in A_{\alpha\beta}$, $y \in A_{\beta\alpha}$ and $y = \phi_{\beta\alpha}(x)$". It follows from (a) and what precedes that R is reflexive and symmetric; on the other hand, if

$$x \in A_{\alpha\beta}, \quad y = \phi_{\beta\alpha}(x) \in A_{\beta\alpha} \cap A_{\beta\gamma}, \quad z = \phi_{\gamma\beta}(y) \in A_{\gamma\beta},$$

then also $x = \phi_{\alpha\beta}(y)$ and by (b) we have $z = \phi_{\gamma\alpha}(x)$; thus R is transitive, and so is an equivalence relation on X. It follows also from (a) and from the definition of R that each equivalence class mod R has at most one element in each of the sets X_α, and that $A_{\alpha\beta}$ is the set of all $x \in X_\alpha$ for which there is an element $y \in X_\beta$ congruent to x mod R. We say that the quotient set X/R is obtained by pasting together the X_α along the $A_{\alpha\beta}$ by means of the bijections $\phi_{\beta\alpha}$. If $\pi : X \to X/R$ is the canonical mapping, the restriction of π to each X_α is a bijection of X_α onto $\pi(X_\alpha)$.

Now suppose that each X_α is a topological space, and let $\mathcal{T}_\alpha$ be its topology. Let $\mathcal{T}$ be the finest topology on the set X/R for which the mappings $\pi \circ \iota_\alpha$ are continuous; then $\mathcal{T}$ is the quotient by R of the topology on X which is the coproduct of the topologies $\mathcal{T}_\alpha$. We say that the topological space X/R (with the topology $\mathcal{T}$) is obtained by pasting together the topological spaces X_α along the $A_{\alpha\beta}$ by means of the bijections $\phi_{\beta\alpha}$. The open (resp. closed) subsets of X/R are thus the canonical images of the subsets B of X which are saturated with respect to R and are such that $B \cap X_\alpha$ is open (resp. closed) in X_α for each $\alpha \in I$.

Since the restriction of π to each X_α is a bijection onto the subset $\pi(X_\alpha)$ of X/R, we can transport the topology $\mathcal{T}_\alpha$ to $\pi(X_\alpha)$ by means of this bijection, so that $\pi(X_\alpha)$ carries a topology $\widetilde{\mathcal{T}}_\alpha$ and the topology $\mathcal{T}$ on X/R is the finest for which the canonical injections $\pi(X_\alpha) \to X/R$ are continuous. In general, the topology induced by $\mathcal{T}$ on $\pi(X_\alpha)$ is coarser than $\widetilde{\mathcal{T}}_\alpha$, but not identical with the latter; even if the $\phi_{\beta\alpha}$ are homeomorphisms. However, it follows from Proposition 1.2.21 that, with the preceding notation:

Proposition 1.3.18. *Suppose that the $\phi_{\beta\alpha}$ are homeomorphisms and that each $A_{\alpha\beta}$ is open (resp. closed) in X_α; then each $\pi(X_\alpha)$ is open (resp. closed) in X/R and the restriction of π to X_α is a homeomorphism of X_α onto the subspace $\pi(X_\alpha)$ of X/R.*

1.4 Product of topological spaces

1.4.1 Product spaces

Definition 1.4.1. *Given a family $(X_i)_{i\in I}$ of topological spaces, the **product space** of this family is the product set $X = \prod_{i\in I} X_i$ with the initial topology induced by the projections $\pi_i : X \to X_i$. The spaces X_i are called the factors of X.*

By virtue of Proposition 1.2.15, the product topology on X has as a base the set of finite intersections of sets of the form $\pi_i^{-1}(U_i)$, where U_i is open in X_i; these sets are products $\prod_{i\in I} U_i$, where U_i is open in X_i for each i and $U_i = X_i$ for all but a finite number of indices These sets will be called **elementary sets**.

If $\mathcal{B}_i$ is a base of the topology of X_i for each $i \in I$, it is clear that the elementary sets $\prod_i B_i$ such that $B_i = X_i$ for all but finitely many indices form another base of the product topology. The elementary sets of this type which contain a given point $x \in X$ thus form a fundamental system of neighbourhoods of x.

If I is a finite set, the construction of the product topology from the topologies of the factors X_i is simpler: the elementary sets are just products $\prod_{i\in I} U_i$ where U_i is any open subset of X_i for each $i \in I$.

Example 1.4.2. The product $\mathbb{R}^n$ of n spaces identical with the real line $\mathbb{R}$ is called real number space of n dimensions; $\mathbb{R}^2$ is also called the real plane. Likewise, starting from the rational line $\mathbb{Q}$, we define the rational number space of n dimensions $\mathbb{Q}^n$ (rational plane for $n = 2$). The topology of the space $\mathbb{R}^n$ has as a base the set of all products of n open intervals in $\mathbb{R}$, which are called open boxes of n dimensions. The open boxes which contain a point $x \in \mathbb{R}^n$ form a fundamental system of neighbourhoods of this point. Likewise the products of n closed intervals in $\mathbb{R}$ are called closed boxes of n dimensions. The closed boxes to which x is interior also form a fundamental system of neighbourhoods of x. There are analogous results for $\mathbb{Q}^n$.

Proposition 1.4.3. *Let $f = (f_i)$ be a mapping of a topological space Y into a product space $X = \prod_{i\in I} X_i$. Then f is continuous at a point $y \in Y$ if and onlY if f_i is continuous at y for each $i \in I$.*

Proof. Since $f_i = f \circ \pi_i$, this is a special case of Proposition 1.2.15. □

Corollary 1.4.4. *Let $(X_i)_{i\in I}$ and $(Y_i)_{i\in I}$ be two families of topological spaces with tke same set of indices. For each $i \in I$, let f_i be a mapping of X_i into Y_i. In order that the product mapping $f : (x_i) \to (f_i(x_i))$ should be continuous at a point $a = (a_i)$, it is necessary and sufficient that f_i is continuous at a_i for each $i \in I$.*

Proof. The map f can be written as $x \mapsto (f_i(\pi_i(x)))$, so that by Proposition 1.4.3 the condition is sufficient. Conversely, for each $j \in I$ let g_j be the mapping of X_j into $\prod_{i\in I} X_i$ such that $\pi_j(g_j(x)) = x_j$ and $\pi_i(g_j(x)) = a_i$ for $i \neq j$. Then g_j is continuous at the point a_j, by Proposition 1.4.3. Since $f_j = \pi_j \circ f \circ g_j$, it follows that if f is continuous at a then f_j is continuous at a_j. □

Corollary 1.4.5. *Let X, Y be two topological spaces. In order that a mapping $f : X \to Y$ should be continuous it is necessary and sufficient that the mapping $g : x \mapsto (x, f(x))$ is a homeomorphism of X onto the graph $\Gamma(f)$ (considered as a subspace of the product space $X \times Y$).*

Proof. Since $f = \pi_2 \circ g$, the condition is sufficient. It is also necessary, for if f is continuous, then g is bijective and continuous (Proposition 1.4.3) and the inverse of g is the restriction of π_1 to $\Gamma(f)$, which is continuous. □

Proposition 1.4.6 (Associativity of topological products). *Let $(X_i)_{i\in I}$ be a family of topological spaces, $(I_\kappa)_{\kappa\in K}$ a partition of the set I, and for each $\kappa \in K$ let $X_\kappa = \prod_{i\in I_\kappa} X_i$. Then the canonical mapping of the product space $\prod_{i\in I} X_i$ onto the product space $\prod_{\kappa\in K} X_\kappa$ is a homeomorphism.*

Proof. This is a special case of the transitivity of initial topologies. □

Corollary 1.4.7. *Let $\sigma \in \mathfrak{S}_I$ be a permutation of the set I. Then the mapping $(x_i) \mapsto (x_{\sigma(i)})$ is a homeomorphism of $\prod_{i\in I}$ onto $\prod_{i\in I} X_{\sigma(i)}$.*

Proof. Take $K = I$ and $I_i = \{\sigma(i)\}$ in the previous proposition. □

Finally, we show that, the general concept of initial topologies can be defined using product spaces and product topology.

Proposition 1.4.8. *Let X be a set, $(Y_i)_{i\in I}$ a family of topological spaces, and for each $i \in I$ let f_i be a mapping of X into Y_i. Let f be the mapping $x \mapsto (f_i(x))$ of X into $Y = \prod_{i\in I} Y_i$. Then the initial topology on X induced by (f_i) is the inverse image under f of the topology induced on $f(X)$ by the product topology on Y.*

Proof. This is another application of the transitivity of initial topologies. □

Corollary 1.4.9. *For each $i \in I$ let A_i be a subspace of X_i. Then the topology induced on $A = \prod_{i\in I} A_i$ by the product topology on $\prod_{i\in I} X_i$ is the product of the topologies of the subspaces A_i.*

Proof. Let ι_i be the canonical injection $A_i \to X_i$ and apply Proposition 1.4.8 to the mappings $f_i = \iota_i \circ \pi_i$. □

There is another topology on the product space $X = \prod_{i\in I} X_i$ called the box topology, whose open sets are defined to be the product of open subsets in X_i. The box topology turns out to have too many open sets, for example, Proposition 1.4.3 does not hold for it.

Example 1.4.10. Consider $\mathbb{R}^\omega$, the countably infinite product of $\mathbb{R}$ with itself. That is, $\mathbb{R}^\omega = \prod_{n\in\mathbb{Z}_+} X_n$, where $X_n = \mathbb{R}$ for each n. Let us define a function $f : \mathbb{R} \to \mathbb{R}^\omega$ by the equation

$$f(x) = (x, x, \dots, x, \dots).$$

Each of the coordinate functions $f_n : \mathbb{R} \to \mathbb{R}$ is continuous; therefore, the function f is continuous if $\mathbb{R}^\omega$ is given the product topology. But f is not continuous if $\mathbb{R}^\omega$ is given the box topology. Consider, for example, the basis element

$$B = \prod_{n\in\mathbb{Z}_+} (-1/n, 1/n),$$

for the box topology. We assert that $f^{-1}(B)$ is not open in $\mathbb{R}$: If $f^{-1}(B)$ contains some interval $(-\delta, \delta)$ about the point 0, then we must have $(-\delta, \delta) \subseteq (-1/n, 1/n)$ for each n, whence $\delta = 0$, a contradiction.

1.4.2 Sections and projections

Proposition 1.4.11. *Let X and Y be topological spaces. Then*

(a) for each $a \in X$, the map $y \mapsto (a, y)$ is a homeomorphism from Y to the subspace $\{a\} \times Y$ of $X \times Y$;

(b) for each $b \in Y$, the map $x \mapsto (x, b)$ is a homeomorphism from X to the subspace $X \times \{b\}$ of $X \times Y$.

Proof. Since π_Y, restricted to $\{a\} \times Y$, is a continuous inverse of the given map in (a), this is a particular case of Corollary 1.4.4 applied to the constant function $x \mapsto a$. The same proof applies to (b). □

Note that the mapping $y \mapsto (a, y)$ is a continuous section with respect to the equivalence relation $\pi_X(z) = \pi_X(z')$ in $X \times Y$; the quotient space of $X \times Y$ by this equivalence relation is therefore homeomorphic to Y.

Corollary 1.4.12. *The section $A(x)$ of an open (resp. closed) set A of the product $X \times Y$ at an arbitrary point $x \in X$ is open (resp. closed) in Y.*

Using Corollary 1.4.4, we also get the following useful fact.

Proposition 1.4.13. *The projection of $X \times Y$ onto either factor is an open map.*

Proof. Let U be open in $X \times Y$, then we have

$$\pi_X(U) = \bigcup_{y \in Y} U(y), \quad \pi_Y(U) = \bigcup_{x \in X} U(x),$$

and the proposition follows from the Corollary 1.4.12. □

Note that the projection of a closed subset of $X \times Y$ onto a factor need not be closed. For example, in the real plane $\mathbb{R}^2$, the hyperbola whose equation is $xy = 1$ is a closed set, but both its projections are equal to the complement of the point 0 in $\mathbb{R}$. and this is not a closed set.

Proposition 1.4.14. *Let X, Y and Z be three topological spaces, f a mapping of the product space $X \times Y$ into Z. If f is continuous at the point $(a, b) \in X \times Y$, then the partial mapping $y \mapsto f(a, y)$ of Y into Z is continuous at the point b.*

Proof. This mapping is the composition of f and the mapping $y \mapsto (a, y)$; hence the result follows from Proposition 1.4.11. □

Proposition 1.4.14 is often expressed by saying that a continuous function of two variables is continuous with respect to each of them separately.

Example 1.4.15. It is possible for all the partial mappings determined by a map $f : X \times Y \to Z$ to be continuous without f being continuous. For example if f is the mapping of the real plane $\mathbb{R}^2$ into $\mathbb{R}$ defined by

$$f(x, y) = \begin{cases} \dfrac{xy}{x^2 + y^2} & (x, y) \neq (0, 0), \\ 0 & (x, y) = (0, 0). \end{cases}$$

Then all the partial mappings are continuous; but f is not continuous at $(0, 0)$.

Proposition 1.4.16. *In a product space $\prod_{i \in I} X_i$ the closure of a product of sets $\prod_{i \in I} A_i$ is the same as the product A_i of their closures.*

Proof. Suppose that $a = (a_i)$ lies in the closure of $\prod_{i \in I} A_i$; then for each $j \in I$, $a_j = \pi_j(a)$ is in the closure of A_j because of the continuity of π_j and therefore $a \in \prod_{i \in I} \overline{A}_i$. Conversely, let $b = (b_i) \in \prod_{i \in I} \overline{A}_i$ and let $\prod_{i \in I} U_i$ be any elementary set containing b; for each $i \in I$, U_i contains a point $x_i \in A_i$; hence $\prod_{i \in I} U_i$ contains the point $(x_i) \in \prod_{i \in I} A_i$ and therefore b lies in the closure of $\prod_{i \in I} A_i$. □

Corollary 1.4.17. *A product $\prod_{i \in I} A_i$ of non-empty sets is closed in the product space $\prod_{i \in I}$ if and only if A_i is closed in X_i for each $i \in I$.*

Remark 1.4.1. Note that if I is finite, a product $\prod_{i \in I} A_i$ is open provided that A_i is open in X_i for each $i \in I$; but this is no longer so if I is infinite.

As an application of Proposition 1.4.16, we give a certain family of dense subsets in a product space.

Proposition 1.4.18. *Let $a = (a_i)$ be any point of a product space $X = \prod_{i \in I} X_i$; then the set D of points $x \in X$ such that $\pi_i(x) = a_i$ except for a finite number of indices i is dense in X.*

Proof. For each $x \in X$ and each elementary set $U = \prod_{i \in I} U_i$ which contains x, we have $U_i = X_i$ except for indices i belonging to a finite subset of J; if we take $y_i = x_i$ for $i \notin J$ and $y_i = a_i$ for $i \in J$, it is clear that $y = (y_i) \in D$ and $y \in U$; hence the result. □

1.4.3 Inverse limit of topological spaces

Let I be a partially ordered (but not necessarily directed) set, in which the order relation is written as $\preceq$. For each $\alpha \in I$, let X_α be a topological space, and for each pair (α, β) such that $\alpha \preceq \beta$ let $f_{\alpha\beta}$ be a mapping of X_β into X_α. We say that $(X_\alpha, f_{\alpha\beta})$ is an inverse system of topological spaces if:

(a) $(X_\alpha, f_{\alpha\beta})$ is an inverse system of sets;

(b) Each $f_{\alpha\beta}$ is continuous.

Let X denote the set $\varprojlim X_\alpha$ and for each $\alpha \in I$ let f_α be the canonical mapping $X \to X_\alpha$; then the initial topology induced by the f_α's is said to be the inverse limit (with respect to the $f_{\alpha\beta}$) of the topologies of the X_α and the set X with this topology is called the inverse limit of the inverse system of topological spaces $(X_\alpha, f_{\alpha\beta})$. Whenever we speak of $\varprojlim X_\alpha$ as a topological space, it is always to be understood that the topology of this space is the inverse limit of the topologies of the X_α unless the contrary is expressly stated.

The set X is the subset of the product $\prod_\alpha X_\alpha$ consisting of those points x such that

$$\pi_\alpha(x) = f_{\alpha\beta}(\pi_\beta(x)).$$

whenever $\alpha \preceq \beta$. It follows from Proposition 1.4.8 that the inverse limit of the topologies of the X_α is the same as the topology induced on X by the topology of the product space $\prod_\alpha X_\alpha$. If, for each $\alpha \in I$, A_α is a subspace of X_α such that the $(A_\alpha, f_{\alpha\beta}|_{A_\beta})$ form an inverse system of subsets of the X_α, then it is clear that the topological space $\varprojlim A_\alpha$ is a subspace of $\varprojlim X_\alpha$.

Let $(Y_\alpha, g_{\alpha\beta})$ be another inverse system of topological spaces indexed by the same set I, and for each $\alpha \in I$ let $\varphi_\alpha : X_\alpha \to Y_\alpha$ be a continuous mapping such that (φ_α) is an inverse system of mappings; then $\varphi = \varprojlim \varphi_\alpha$ is a continuous mapping of $X = \varprojlim X_\alpha$ into $Y = \varprojlim Y_\alpha$. For if g_α is the canonical mapping $Y \to Y_\alpha$, we have $g_\alpha \circ \varphi = \varphi_\alpha \circ f_\alpha$, so that $g_\alpha \circ \varphi$ is continuous for each $\alpha \in I$, and so φ is continuous.

Finally, suppose I is a directed set, and let J be a cofinal subset of I; let $\widetilde{X}$ be the inverse limit of the inverse system of topological spaces $(X_\alpha, f_{\alpha\beta})_{\alpha,\beta \in J}$. Then the canonical bijection $\psi : X \to \widetilde{X}$ is a homeomorphism. For we have $\pi_\alpha(\psi(x)) = \pi_\alpha(x)$ for each $\alpha \in J$, hence ψ is continuous; and if ϕ is the inverse of ψ, then for each $\alpha \in I$ there exists $\beta \in J$ such that $\alpha \preceq \beta$, and therefore $\pi_\alpha(\phi(z)) = f_{\alpha\beta}(\pi_\beta(z))$, which shows that ϕ is continuous, since the $f_{\alpha\beta}$'s are continuous.

Proposition 1.4.19. *Let I be a directed set and J a cofinal subset of I. Let $(X_\alpha, f_{\alpha\beta})$ be an inverse system of topological spaces indexed by I; let $X = \varprojlim X_\alpha$ and let $f_\alpha : X \to X_\alpha$ be the canonical mapping. Then the family of sets $f_\alpha^{-1}(U_\alpha)$, where α runs through J and U_α runs through a base $\mathcal{B}_\alpha$ of the topology of X_α for each $\alpha \in J$, is a base of the topology of X.*

Proof. We know that the finite intersections of sets of the form $f_\alpha^{-1}(U_\alpha)$, $\alpha \in I$, U_α open in X_α form a base of the topology of X. If $\alpha_1, \ldots, \alpha_n$ is a finite family of indices of I, then there exists $\beta \in J$ such that $\alpha_i \preceq \beta$ for $1 \leq i \leq n$; hence $f_{\alpha_i} = f_{\alpha_i\beta} \circ f_\beta$; if we put $U_\beta = \bigcap_{i=1}^n f_{\alpha_i\beta}^{-1}(U_{\alpha_i})$, then

$$f_\beta^{-1}(U_\beta) = \bigcap_{i=1}^n f_{\alpha_i}^{-1}(U_{\alpha_i}).$$

But U_β is open and is therefore a union of sets belonging to $\mathcal{B}_\beta$. Hence the result. □

Corollary 1.4.20. *Let A be a subset of X and let $A_\alpha = f_\alpha(A)$ for each $\alpha \in I$. Then:*

(a) The A_α (resp. the $\overline{A}_\alpha$) form an inverse system of subsets of the X_α, and $\overline{A} = \bigcap_\alpha f_\alpha^{-1}(\overline{A}_\alpha) = \varprojlim \overline{A}_\alpha$.

(b) If A is closed in X then $A = \varprojlim A_\alpha = \varprojlim \overline{A}_\alpha$.

Proof. The first assertion of (a) follows from the relations $f_\alpha = f_{\alpha\beta} \circ f_\beta$ for $\alpha \preceq \beta$ and from the continuity of the f_α. Let A' denote $\bigcap_\alpha f_\alpha^{-1}(\overline{A}_\alpha)$, then it is clear that A' is closed and contains A, so that $\overline{A} \subseteq A'$. Conversely, let $x \in A'$; we have to show that x lies in the closure of A. By virtue of Proposition 1.4.19, it is enough to prove that every neighbourhood of x which is of the form $f_\alpha^{-1}(U_\alpha)$, with $\alpha \in I$ and U_α open in X_α meets A. Now, by hypothesis, $f_\alpha(x) \in U_\alpha$, and since $f_\alpha(x) \in \overline{A}_\alpha$ we have $U_\alpha \cap A_\alpha \neq \varnothing$, which means $A \cap f_\alpha^{-1}(A_\alpha) \neq \varnothing$.

To establish (b) it is enough to remark that, without any restriction on A, we have $A \subseteq \varprojlim A_\alpha \subseteq \varprojlim \overline{A}_\alpha$; now if A is closed, then from (a) we have $A = \varprojlim \overline{A}_\alpha$, so the claim follows. □

Example 1.4.21. Let I be a directed set and $(X_\alpha)_{\alpha \in I}$ a family of subsets of a set Y, such that $X_\alpha \supseteq X_\beta$ whenever $\alpha \preceq \beta$. For each $\alpha \in I$ let $\mathcal{T}_\alpha$ be a topology on X_α such that $\mathcal{T}_\alpha$ is finer than the topology induced on X_α by $\mathcal{T}_\beta$ whenever $\alpha \preceq \beta$. If we take $f_{\alpha\beta}$ to be the canonical injection $X_\beta \to X_\alpha$ for $\alpha \preceq \beta$, then $\varprojlim X_\alpha$ may be identified canonically with the intersection X of the X_α, with the topology which is the least upper bound of the topologies induced on X by the $\mathcal{T}_\alpha$.

1.5 Connectedness

1.5.1 Connected spaces

The definition of connectedness for a topological space is a quite natural one. One says that a space can be "separated" if it can be broken up into two "globs"–disjoint open sets. Otherwise, one says that it is connected. From this simple idea much follows.

Definition 1.5.1. *Let X be a topological space. A **separation** of X is a pair U, V of disjoint nonempty open subsets of X whose union is X. The space X is said to be connected if there does not exist a separation of X.*

Connectedness is obviously a topological property, since it is formulated entirely in terms of the collection of open sets of X. Said differently, if X is connected, so is any space homeomorphic to X.

For a subspace A of a topological space X, there is another useful way of formulating the definition of connectedness:

Lemma 1.5.2. *If A is a subspace of X, a separation of A is a pair of disjoint nonempty sets U and V whose union is A, neither of which contains a limit point of the other. The space A is connected if there exists no separation of A.*

Proof. Suppose first that U and V form a separation of A. Then U is both open and closed in A. The closure of U in A is the set $\overline{U} \cap A$ (where $\overline{U}$ as usual denotes the closure of U in X). Since U is closed in A, $U = \overline{U} \cap A$; or to say the same thing, $\overline{U} \cap V = \varnothing$. Since $\overline{U}$ is the union of U and its limit points, V contains no limit points of U. A similar argument shows that U contains no limit points of V.

Conversely, suppose that U and V are disjoint nonempty sets whose union is A, neither of which contains a limit point of the other. Then $\overline{U} \cap V = \varnothing$ and $\overline{V} \cap U = \varnothing$; therefore, we conclude that $\overline{U} \cap A = U$ and $\overline{V} \cap A = V$. Thus both U and V are closed in A, and since $U \cup V = A$, they are open in A as well. □

Example 1.5.3. Let X denote a two-point space in the indiscrete topology. Obviously there is no separation of X, so X is connected.

Example 1.5.4. Let A denote the subspace $[-1, 0) \cup (0, 1]$ of the real line $\mathbb{R}$. Each of the sets $[-1, 0)$ and $(0, 1]$ is nonempty and open in A (although not in $\mathbb{R}$); therefore, they form a separation of A. Alternatively, note that neither of these sets contains a limit point of the other. (They do have a limit point 0 in common, but that does not matter.)

Example 1.5.5. A subspace of $\mathbb{R}$ is connected if and only if it is an interval: Clearly intervals are connected. Now suppose X is connected in $\mathbb{R}$ and is not an interval. Then there are $x, y \in X$ and $z \notin X$ such that $x < z < y$. We set

$$O_1 = (-\infty, z) \cap X, \quad O_2 = X \cap (z, +\infty)$$

Then O_1 and O_2 is a separation of X, and since $x \in O_1$, $y \in O_2$ they are both nonempty. This is a contradiction since X is connected, hence X is an interval.

Example 1.5.6. Let X be the subspace $[-1, 1]$ of the real line. The sets $[-1, 0]$ and $(0, 1]$ are disjoint and nonempty, but they do not form a separation of X, because the first set is not open in X. Alternatively, note that the first set contains a limit point, 0, of the second. Indeed, there exists no separation of the space $[-1, 1]$.

Example 1.5.7. The rationals $\mathbb{Q}$ are not connected. Indeed, the only connected subspaces of $\mathbb{Q}$ are the one-point sets: If A is a subspace of $\mathbb{Q}$ containing two points p and q, one can choose an irrational number α lying between p and q, and write A as the union of the open sets

$$A = (A \cap (-\infty, \alpha)) \cup (A \cap (\alpha, +\infty)).$$

Example 1.5.8. Consider the following subset of the plane $\mathbb{R}^2$:

$$X = \{(x, y) \in \mathbb{R}^2 : y = 0\} \cup \{(x, y) : x > 0 \text{ and } xy = 1\}.$$

Then X is not connected; indeed, the two indicated sets form a separation of X because neither contains a limit point of the other.

We have given several examples of spaces that are not connected. How can one construct spaces that are connected? We shall now prove some useful properties of connectedness, and later use them to construct connected topological spaces. First, we give another criterion for connectedness which is quite simple but useful.

Proposition 1.5.9. *A topological space X is connected if and only if every continuous map $f : X \to \{0, 1\}$ is constant, with the space $\{0, 1\}$ given the discrete topology.*

Proof. Clearly if f is not constant then $f^{-1}(0) \cup f^{-1}(1)$ is a separation of X. Conversely, if U and V form a separation of X then the characteristic function χ_U is nonconstant and continuous. □

Proposition 1.5.10 (Properties of Connected Spaces). *Let X be a topological space.*

(a) Suppose that U, V are disjoint open subsets of X. If A is a connected subset of X contained in $U \cup V$, then either $A \subseteq U$ or $A \subseteq V$.

(b) Suppose X is any space and $A \subseteq X$ is connected. If B is a subset such that $A \subseteq B \subseteq \overline{A}$, then it is connected. In particular, $\overline{A}$ is connected.

(c) Let $\{C_\alpha\}_{\alpha \in I}$ be a collection of connected subspaces of X with a point in common. Then $\bigcup_{\alpha \in I} C_\alpha$ is connected.

(d) Let $\{C_\alpha\}_{\alpha \in I}$ be a collection of connected subspaces of X with $C_\alpha \cap C_\beta \neq \varnothing$ for all $\alpha, \beta \in I$. Then $\bigcup_{\alpha \in I} C_\alpha$ is connected.

Proof. For (a), if A contained points in both U and V, then $A \cap U$ and $A \cap V$ would form a separation of A. To prove (b), suppose A is connected and $A \subseteq B \subseteq \overline{A}$. Suppose that $B = U \cup V$ is a separation of B. By part (a), the set A must lie entirely in U or in V; say $A \subseteq U$. Then $\overline{A} \subseteq \overline{U}$; since $\overline{U}$ and V are disjoint, B cannot intersect V. This contradicts the fact that V is a nonempty subset of B.

For part (c), let p be a point that is contained in C_α for every α, and let $f : \bigcup_\alpha C_\alpha \to \{0, 1\}$ be a continuous function. Then f is constant when restricted to each C_α, since C_α is connected. Since C_α contains p for each α, it then follows that f is constant. This shows $\bigcup_\alpha C_\alpha$ is connected. Part (c) can be proved similarly. □

Corollary 1.5.11. *Let X be a topological space and $(A_n)_{n \in \mathbb{N}}$ be an infinite sequence of connected subspaces such that $A_n \cap A_{n+1} \neq \varnothing$ for all $n \geq 0$. Then the union $\bigcup_n A_n$ is connected.*

Proof. By induction on n we see immediately that the set $B_n = \bigcup_{i=1}^n A_i$ is connected for all n, by Proposition 1.5.10. The sets B_n have a non-empty intersection; hence their union, equal to $\bigcup_n B_n$, is connected by Proposition 1.5.10. □

Proposition 1.5.12. *The image of a connected space under a continuous map is connected.*

Proof. Let $f : X \to Y$ be a continuous map; let X be connected. We wish to prove the image space $f(X)$ is connected. Since the map obtained from f by restricting its range to the space is also continuous, it suffices to consider the case that f is surjective. Suppose that $Y = U \cup V$ is a separation of Y into two disjoint nonempty sets open in Y. Then $f^{-1}(U)$ and $f^{-1}(V)$ are disjoint sets whose union is X; they are open in X because f is continuous, and nonempty because f is surjective. Therefore, they form a separation of X, contradicting the assumption that X is connected. □

Corollary 1.5.13. *Every quotient space of a connected space is connected.*

As for Corollary 1.5.13, we have the following converse.

Proposition 1.5.14. *Let X be a topological space and R an equivalence relation on X. If the quotient space X/R is connected, and if each equivalence class of R is connected, then X is connected.*

Proof. Suppose X is not connected. Then there is a partition of X into two open sets U, V. The sets U, V are saturated with respect to R in view of Proposition 1.5.10(a). The canonical images of U and V are therefore open sets in X/R and form a partition of X/R; this contradicts the assumption that X/R is connected. □

Proposition 1.5.15. *Every product of connected spaces is connected. Conversely, if a product of non-empty spaces is connected, then each of the factors is connected.*

Proof. Let $(X_i)_{i\in I}$ be a family of topological spaces and $X = \prod_{i\in I} X_i$. Since the projection $\pi_i : X \to X_i$ is continuous and surjective, if X is connected then so is each X_i. Conversely, assume that each X_i is connected and let $f : X \to \{0,1\}$ be a continuous map, where $\{0,1\}$ is given the discrete topology. Let $a = (a_i)$ be any point of X, and for each $j \in I$ let $f_j : X_j \to \{0,1\}$ be the partial mapping defined by $f_j(x_j) = f((y_i))$, where $y_j = x_j$ and $y_i = a_i$ for $i \neq j$. Then f_j is continuous, so is constant since X_j is connected. It follows immediately by induction that $f(x) = f(a)$ for all points $x = (x_i)$ such that $x_i = a_i$ for all but finitely many indices of I. But these points form a dense subset of X by Proposition 1.4.18. Hence f is continuous on X and constant on a dense subset of X, and therefore constant on X. But this contradicts the definition of f. □

Now that, however, the result of Proposition 1.5.15 depends on the topology we endow with the product space $\prod_{i\in I} X_i$. If we consider the box topology, it turns out that $\prod_{i\in I} X_i$ may be not connected even though each X_i is.

Example 1.5.16. Consider the cartesian product $\mathbb{R}^\omega$ in the box topology. We can write $\mathbb{R}^\omega$ as the union of the set A consisting of all bounded sequences of real numbers, and the set B of all unbounded sequences. These sets are disjoint, and each is open in the box topology. For if $x = (x_n)$ is a point of $\mathbb{R}^\omega$, the open set

$$U = \bigcup_{n\in\mathbb{Z}_+} (x_n - 1/n, x_n + 1/n)$$

consists entirely of bounded sequences if x is bounded, and of unbounded sequences if x if unbounded. Thus, even though $\mathbb{R}$ is connected, $\mathbb{R}^\omega$ is not connected in the box topology.

Example 1.5.17. The set $\mathrm{O}(n)$ of all real orthogonal $n\times n$ matrices is not connected. The function $O(n) \to \{1,-1\}, A \mapsto \det A$ is continuous and surjective, since we have the formula

$$\det A = \sum_{\sigma\in\mathfrak{S}_n} (\operatorname{sign}\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)}$$

Since $\{1,-1\}$ has discrete topology, it follows that $\mathrm{O}(n)$ is not connected.

1.5.2 Path connectedness

The theorems of the preceding part show us how to construct new connected spaces out of given ones. But where can we find some connected spaces to start with? The best place to begin is the real line. We shall prove that $\mathbb{R}$ is connected, and so are the intervals and rays in $\mathbb{R}$. The fact that intervals and rays in $\mathbb{R}$ are connected may be familiar to you from analysis. We prove it again here, in generalized form. It turns out that this fact does not depend on the algebraic properties of $\mathbb{R}$, but only on its order properties. To make this clear, we shall prove the theorem for an arbitrary ordered set that has the order properties of $\mathbb{R}$. Such a set is called a **linear continuum**.

Definition 1.5.18. *A totally ordered set L having more than one element is called a* ***linear continuum*** *if the following hold:*

(a) L has the least upper bound property.

(b) If $x < y$, there exists z such that $x < z < y$.

Theorem 1.5.19. *If L is a linear continuum in the order topology, then L is connected, and so are intervals and rays in L.*

Proof. Recall that a subspace A of L is said to be convex if for every pair of points a, b of A with $a < b$, the entire interval $[a, b]$ of points of L lies in A. We prove that if A is a convex subspace of L, then A is connected.

So suppose that A is the union of the disjoint nonempty sets U and V, each of which is open in A. Choose $a \in U$ and $b \in V$; suppose for convenience that $a < b$. The interval $[a, b]$ of points of L is contained in A. Hence $[a, b]$ is the union of the disjoint sets

$$U_0 = U \cap [a, b], \quad V_0 = V \cap [a, b]$$

each of which is open in $[a, b]$ in the subspace topology, which is the same as the order topology. The sets U_0 and V_0 are nonempty because $a \in U_0$ and $b \in V_0$. Thus, U_0 and V_0 constitute a separation of $[a, b]$. Let $c = \sup U_0$. We show that c belongs neither to U_0 nor to V_0, which contradicts the fact that $[a, b]$ is the union of U_0 and V_0.

Suppose that $c \in A_0$. Then $c \neq b$, so either $c = a$ or $a < c < b$. But U_0 is open in $[a, b]$, so there must be some interval of the form $[c, e)$ contained in U_0. Because of order property (b) of the linear continuum L, we can choose a point z of L such that $c < z < e$. Then $z \in U_0$, contrary to the fact that c is an upper bound for U_0.

Suppose that $c \in B_0$. Then $c \neq a$, so either $c = b$ or $a < c < b$. In either case, it follows from the fact that V_0 is open in $[a, b]$ that there is some interval of the form $(d, c]$ contained in V_0. Since $(c, b]$ does not intersect U_0, we see that $(d, b] = (d, c] \cup (c, b]$ does not intersect U_0. Again, d is a smaller upper bound on U_0 than c, contrary to construction. □

Corollary 1.5.20. *The real line $\mathbb{R}$ is connected and so are intervals and rays in $\mathbb{R}$.*

As an application, we prove the intermediate value theorem of calculus, suitably generalized.

Theorem 1.5.21 (Intermediate value theorem). *Let $f : X \to Y$ be a continuous map, where X is a connected space and Y is an ordered set in the order topology. If a and b are two points of X and if r is a point of Y lying between $f(a)$ and $f(b)$, then there exists a point c of X such that $f(c) = r$.*

Proof. Assume the hypotheses of the theorem. The sets

$$U = f(X) \cap (-\infty, r) \quad \text{and} \quad V = f(X) \cap (r, +\infty)$$

are disjoint, and they are nonempty because one contains $f(a)$ and the other contains $f(b)$. Each is open in $f(X)$, being the intersection of an open ray in Y with $f(X)$. If there were no point c of X such that $f(c) = r$, then $f(X)$ would be the union of the sets U and V. Then U and V would constitute a separation of $f(X)$, contradicting the fact that the image of a connected space under a continuous map is connected. □

Example 1.5.22. One example of a linear continuum different from $\mathbb{R}$ is the ordered square. We check the least upper bound property. (The second property of a linear continuum is trivial to check.)

Let A be a subset of $I \times I$; let $\pi_1 : I \times I \to I$ be projection on the first coordinate; let $b = \sup \pi_1(A)$. If $b \in \pi_1(A)$, then A intersects the subset $\{b\} \times I$ of $I \times I$. Because $\{b\} \times I$ has the order type of I, the set $A \cap (\{b\} \times I)$ will have a least upper bound (b, c), which will be the least upper bound of A.

If $b \notin \pi_1(A)$, then $(b, 0)$ is the least upper bound of A; no element of the form (b', c) with $b' < b$ can be an upper bound for A, for then b' would be an upper bound for $\pi_1(A)$.

Example 1.5.23. If X is a well-ordered set, then $X \times [0, 1)$ is a linear continuum in the dictionary order. This set can be thought of as having been constructed by "fitting in" a set of the order type of $(0, 1)$ immediately following each element of X.

Connectedness of intervals in $\mathbb{R}$ gives rise to an especially useful criterion for showing that a space X is connected; namely, the condition that every pair of points of X can be joined by a path in X:

Definition 1.5.24. *Given points x and y of the space X, a **path** in X from x to y is a continuous map $p : [0, 1] \to X$ of the unit interval in the real line into X, such that $p(0) = x$ and $p(1) = y$. A space X is said to be **path-connected** if every pair of points of X can be joined by a path in X.*

It is easy to see that a path-connected space X is connected. Suppose $X = U \cup V$ is a separation of X. Let $p : [0, 1] \to X$ be any path in X. Being the continuous image of a connected set, the set $p([0, 1])$ is connected, so that it lies entirely in either U or V. Therefore, there is no path in X joining a point of U to a point of V, contrary to the assumption that X is path-connected. The converse does not hold: a connected space need not be path-connected.

Example 1.5.25. Define punctured Euclidean space to be the space $\mathbb{R}^n \setminus \{0\}$, where 0 is the origin in $\mathbb{R}^n$. If $n > 1$, this space is path-connected: Given x and y different from 0, we can join x and y by the straight-line path between them if that path does not go through the origin. Otherwise, we can choose a point z not on the line joining x and y, and take the broken-line path from x to z, and then from z to y.

Example 1.5.26. Being a linear continuum, the ordered square is connected. Let $x = (0, 0)$ and $y = (1, 1)$. We suppose there is a path $p : [0, 1] \to I_o^2$ joining x and y and derive a contradiction. The image set $p([0, 1])$ must contain every point (x, y) of I_o^2, by the intermediate value theorem. Therefore, for each $x \in I$, the set

$$U_x = p^{-1}(\{x\} \times (0, 1))$$

is a nonempty subset of $[0,1]$; by continuity, it is open in $[0,1]$. Choose, for each $x \in I$, a rational number r_x belonging to U_x. Since the sets U_x are disjoint, the map $x \mapsto r_x$ is an injective mapping of I into $\mathbb{Q}$. This contradicts the fact that the interval I is uncountable.

Example 1.5.27. Let S denote the following subset of the plane

$$S = \{(x, y) : 0 < x \leq 1 \text{ and } y = \sin(1/x)\}.$$

Because S is the image of the connected set $(0,1]$ under the continuous map $x \mapsto \sin(1/x)$, it is connected. Therefore, its closure $\bar{S}$ in $\mathbb{R}^2$ is also connected. The set $\bar{S}$ is a classical example in topology called the **topologist's sine curve**. It equals the union of S and the vertical interval $\{0\} \times [-1,1]$. We show that $\bar{S}$ is not path-connected.

Suppose there is a path $p : [a,b] \to \bar{S}$ beginning at the origin and ending at a point of S. The set of those t for which $p(t) \in \{0\} \times [-1,1]$ is closed, so it has a largest element c. Then $p : [c,b] \to \bar{S}$ is a path that maps c into the vertical interval $\{0\} \times [-1,1]$ and maps the other points of $[c,b]$ to points of S. Without loss of generality, we replace $[c,b]$ with $[0,1]$.

Let $p(t) = (x(t), y(t))$. Then $x(0) = 0$, while $x(t) > 0$ and $y(t) = \sin(1/x(t))$ for $t > 0$. We show there is a sequence of points $t_n \to 0$ such that $y(t_n) = (-1)^n$. Then the sequence $y(t_n)$ does not converge, contradicting continuity of p. To find t_n, we proceed as follows: Given n, choose u with $0 < u < x(1/n)$ such that $\sin(1/u) = (-1)^n$. Then use the intermediate value theorem to find t_n with $0 < t_n < 1/n$ such that $x(t_n) = u$.

Proposition 1.5.28. *Let X be a topological space. Let $\{C_\alpha\}_{\alpha \in I}$ be a collection of path-connected subspaces of X with a point in common. Then $\bigcup_\alpha C_\alpha$ is path-connected.*

Proof. Let $p \in \bigcap_\alpha C_\alpha$, then for each $x \in \bigcup_\alpha C_\alpha$, there is a path from x to p. This shows $\bigcup_\alpha C_\alpha$ is path-connected. □

Proposition 1.5.29. *The image of a path-connected space under a continuous map is path-connected.*

Proof. Let $f : X \to Y$ be a continuous map and X be path-connected. Let $a, b \in f(X)$, and choose $x, y \in X$ such that $f(x) = a$, $f(y) = b$. Then if $p : [0,1] \to X$ be a path from x to y, then it follows that $f \circ p$ is a path from a to b. Therefore $f(X)$ is path-connected. □

Proposition 1.5.30. *Every product of path-connected spaces is path-connected. Conversely, if a product of non-empty spaces is path-connected, then each of the factors is path-connected.*

Proof. Let $(X_i)_{i \in I}$ be a family of topological spaces and $X = \prod_{i \in I} X_i$. If X is path-connected, then since $X_i = \pi_i(X)$, we have X_i is path-connected for each $i \in I$. Conversely, assume that each X_i path-connected. Let $x = (x_i)_{i \in I}$, $y = (y_i)_{i \in I}$ be two points in X. By assumption, there exist continuous paths $p_i : [0,1] \to X_i$ with $\gamma_i(0) = x_i$ and $\gamma_i(1) = y_i$. By definition of product, there exists a unique continuous $p : [0,1] \to X$ such that $\pi_i \circ \gamma = \gamma_i$ for all $i \in I$. That makes p a path from x to y, so X is path-connected. □

Example 1.5.31. Let Ω be the first uncountable ordinal, and we use S_Ω to denote the set Ω together with the order topology. As a set, S_Ω consists of all countable ordinals. Let L denote the ordered set $S_\Omega \times [0,1)$ in the dictionary order, with its smallest element deleted. The set L is a classical example in topology called the **long line**. We now show that L is path-connected.

Pick any two points $x = (\alpha, s)$ and $y = (\beta, t)$ on the long line, with $x < y$. If $\alpha = \beta$, then $s < t$ and the long line interval $[x, y]$ is readily homeomorphic to the real interval $[s, t]$, so x, y are connected by a path. Otherwise, since α and β are countable ordinals, the long line interval $[x, y]$ is the union of (in increasing order) $\alpha \times [s, 1)$, then (at most) ountably many intervals of the form $\gamma \times [0, 1)$ with $\alpha < \gamma < \beta$, then $\beta \times [0, t]$, joined end to end. Again, this set is homeomorphic to a closed real interval, so that x, y are connected by a path.

1.5.3 Components and locally connectedness

Given a point x of a topological space X, the union of the connected subsets of X which contain x is connected; it is therefore the largest connected subset of X which contains x.

Definition 1.5.32. *The **component** (or **connected component**) of a point of a topological space X is the largest connected subset of X which contains this point. The components of a subset A of X are the components of the points of A, relative to the subspace A of X.*

If a space is connected, the component of each point is the whole space. A space X is said to be **totally disconnected** if the component of each point of X consists of the point alone. A subset A of X is totally disconnected if the subspace A of X is totally disconnected.

Proposition 1.5.33. *The component of any point in a topological space X is a closed set. The relation "y belongs to the component of x" is an equivalence relation R on X, and the equivalence classes are the components of X. The quotient space X/R is totally disconnected.*

Proof. If C is any component of X, it follows that $\overline{C}$ is a connected set containing C. Since components are maximal connected sets, $C = \overline{C}$, so C is closed.

Since the union of connected sets which have a point in common is connected, the relation R is transitive, hence is an equivalence relation (since it is obviously reflexive and symmetric) and the equivalence class of x with respect to R is the component of x. It remains to show that X/R is totally disconnected.

Let $\pi : X \to X/R$ be the canonical mapping, and let F be a closed set in X/R containing at least two distinct points; the inverse image $\pi^{-1}(F)$ of F is closed in X, saturated with respect to R, and contains at least two distinct components of X and hence is not connected. Hence there exist two non-empty disjoint closed sets B, C in X such that $B \cup C = \pi(F)$. The component of any point x of $\pi^{-1}(F)$ in $\pi(F)$ is the same as the component of x in X (by the definition of R) and therefore B and C, which are both open and closed in $\pi^{-1}(F)$, are saturated with respect to R. Hence $\pi(B)$ and $\pi(C)$ are closed in X/R, and $\pi(B) \cup \pi(C) = F$ and $\pi(B) \cap \pi(C) = \varnothing$; this shows that F is not connected and consequently that X/R is totally disconnected. □

Proposition 1.5.34. *In a product space $X = \prod_{i \in I} X_i$ the component of $x = (x_i)$ in X is the product of the components of x_i in the factors X_i*

Proof. This product set is connected by Proposition 1.5.15. Conversely, if C is a connected subset of X which contains x, then $\pi_i(C)$ is a connected set which contains x_i; since $C \subseteq \prod_i \pi_i(A)$, it follows that C is contained in the product of the components of the x_i's. □

Although components are always closed, they may not be open in general, so they do not necessarily disconnect the space. Consider the set $\mathbb{Q}^2$ of rational points in the plane, for

example: its components are single points, which are not open subsets. There is a condition, however, which ensure that all components are open.

Definition 1.5.35. *A topological space X is said to be* ***locally connected*** *if each point of X has a fundamental system of connected neighbourhoods.*

The existence, at each point x of a space X, of one connected neighbourhood of x by no means implies that X is locally connected. In particular, X can be connected but not locally connected. Conversely, a space can be locally connected but not connected (e.g. a discrete space which contains more than one point).

Example 1.5.36. The topologist's sine curve $\overline{S}$ is connected but not locally connected. In fact, any neigbourhood of points in $\{0\} \times [-1, 1]$ should intersect the set S, so is not connected.

Example 1.5.37. Consider $\mathbb{R}^2$ with its standard topology and let K be the set $\{1/n : n \in \mathbb{Z}_+\}$. The set C defined by:

$$C = (\{0\} \times [0, 1]) \cup (K \times [0, 1]) \cup ([0, 1] \times \{0\})$$

considered as a subspace of $\mathbb{R}^2$ equipped with the subspace topology is known as the comb space. The space C is not locally connected, as every neighborhood of points in $\{0\} \times [0, 1]$ is not connected. But it is easily seen to be path-connected.

Proposition 1.5.38. *A necessary and sufficient condition for a space X to be locally connected is that every component of an open set in X is open in X.*

Proof. Suppose that X is locally connected; let U be an open set in X; let C be a component of U. If x is a point of C, we can choose a connected neighborhood V of x such that $V \subseteq U$. Since V is connected, it must lie entirely in the component C of U. Therefore, C is open in X.

Conversely, suppose that components of open sets in X are open. Given a point x of X and a neighborhood U of x, let C be the component of U containing x. Now C is connected; since it is open in X by hypothesis, X is locally connected at x. □

The components of a locally connected space X therefore form a partition of X into open sets, and hence X is the coproduct of its components.

Corollary 1.5.39. *Let U be an open subset of a locally connected space X, and let V be a component of U. Then the boundary of V (relative to X) is contained in the boundary of U.*

Proof. Since V is open and closed in U, a boundary point of V (relative to X) cannot belong to U, for it would also be a bounadry point of V relative to U, and there is none. □

Proposition 1.5.40. *Every quotient space of a locally connected space is locally connected.*

Proof. Let X be a locally connected space, R an equivalence relation on X and $\pi : X \to X/R$ the canonical mapping of R. Let U be an open subset of X/R and C a component of U. Then $\pi^{-1}(C)$ is a union of components of $\pi^{-1}(U)$; for if $x \in \pi^{-1}(C)$ and if K is the component of x in $\pi^{-1}(U)$, then $\pi(K)$ is connected, is contained in U, and contains $\pi(x)$; hence $\pi(K) \subseteq C$ by the definition of C, and therefore $K \subseteq \pi^{-1}(C)$. Since X is locally connected and $\pi^{-1}(U)$ is open in X, it follows from Proposition 1.5.38 that $\pi^{-1}(C)$ is open in X; consequently C is open in X/R and hence, by Proposition 1.5.38 again, X/R is locally connected. □

Proposition 1.5.41. *Let $(X_i)_{i\in I}$ be a family of topological spaces and $X = \prod_{i\in I} X_i$ be the product space.*

(a) If X_i is connected for all but a finite number of indices $i \in I$. Then the product space X is locally connected.

(b) Conversely, if the product space X is locally connected, then each X_i is locally connected, and X_i is connected for all but a finite number of indices.

Proof. First assume (a), and let J be the finite subset of I such that X_i is not connected if and only if $i \in J$. Let $U = \prod_{i\in I} U_i$ be an elementary set containing a point $x = (x_i)$ of X and let K be the finite subset of I such that $U_i \neq X_i$ if and only if $i \in K$. Let $V_i = X_i$ for $i \in J \cup K$, and let V_i be a connected neighbourhood of x_i contained in V_i for $i \notin J \cup K$; then $V = \prod_{i\in I} V_i$ is connected (by Proposition 1.5.15) and is a neighbourhood of x contained in U. Hence X is locally connected.

Conversely, assume that X is locally connected. Let $a = (a_i)$ be a point of X and let V be a connected neighbourhood of a in X. Since we have $\pi_i(V) = X_i$ except for a finite number of indices, it follows that the X_i are connected, for all but a finite number of indices. On the other hand, for each $j \in I$, each $a_j \in X_j$ and each neighbourhood V_j of a_j in X_j, there is a point x of X such that $\pi_j(x) = a_j$, and

$$V = V_j \times \prod_{i\neq j} X_j$$

is a neighbourhood of x in X; V therefore contains a connected neighbourhood W of x, whose projection $\pi_j(W)$ is a connected neighbourhood of a_j contained in V_j (the projection is open). Hence each X_j is locally connected. □

1.5.4 Path components

We can also define an analogue of components with path-connectedness in place of connectedness. If X is any space, define a **path component** of X to be a maximal nonempty path-connected subset. The following properties of path compoenents are immediate.

Proposition 1.5.42 (Properties of Path Components). *Let X be any space.*

(a) The path components of X form a partition of X.

(b) Each path component is contained in a single component, and each component is a disjoint union of path components.

(c) Any nonempty path-connected subset of X is contained in a single path component.

Example 1.5.43. The topologist's sine curve $\bar{S}$ is a space that has a single component (since it is connected) and two path components. One path component is the curve S and the other is the vertical interval $V = \{0\} \times [-1, 1]$. Note that S is open in $\bar{S}$ but not closed, while V is closed but not open. If one forms a space from $\bar{S}$ by deleting all points of V having rational second coordinate, one obtains a space that has only one component but uncountably many path components.

Similarly, we say that a space X is **locally path-connected** if each point of X has a fundamental system of path-connected neigbourhoods. Since path-connectedness implies connectedness, every locally path-connected space is locally connected. We have the following analogue of Proposition 1.5.38.

Proposition 1.5.44. *A space X is locally path connected if and only if for every open set U of X, each path component of U is open in X.*

Proof. The proof is identically the same as that of Proposition 1.5.38, replacing "connected" by "path-connected". □

Proposition 1.5.45 (Properties of Locally Path-Connected Spaces). *Suppose X is a locally path-connected space, then the path components of X are equal to its components. In particular, X is connected if and only if it is path-connected.*

Proof. Let $x \in X$, and let C and P be the component and the path component containing x, respectively. By definition, we know that $P \subseteq C$ and C can be written as a disjoint union of path components, each of which is open in X. Suppose that $P \subsetneq C$, let Q denote the union of all the path components of X that are different from P and intersect C; each of them necessarily lies in C, so that $C = P \cup Q$. Because X is locally path connected, each path component of X is open in X. Therefore, P (which is a path component) and Q (which is a union of path components) are open in X, so they constitute a separation of C. This contradicts the fact that C is connected. □

1.6 Countablity and separation axoims

There are actually several countability properties that are useful. We begin with the weakest one.Let X be a topological space, we say that X is **first countable** if there exists a countable neighborhood base at each point. A topological space is said to be **second countable** if it admits a countable base for its topology. A topological space X is said to be **separable** if it contains a countable dense subset, and to be a **Lindelöf** space if every open cover of X has a countable subcover.

Theorem 1.6.1 (Properties of Second Countable Spaces). *Suppose that X is a second countable space. Then:*

(a) X is first countable.

(b) X is Lindelöf.

(c) X is separable.

Proof. Let $\mathcal{B}$ be a countable base for X. To prove (a), just note that for any $p \in X$, the elements of $\mathcal{B}$ that contain p form a countable neighborhood base at p.

Let $\{B_n\}$ be a countable base for X. For (b), let $\mathcal{U}$ be an open over of X and set

$$J := \{n \in \mathbb{N} : \exists U \in \mathcal{U}, B_n \subseteq U\}.$$

Let $\mathcal{B}' = \{B_n\}_{n \in J}$. The collection $\mathcal{B}'$ is countable, since it is indexed with a subset J of the positive integers. Furthermore, it covers X: Given a point $x \in X$, we can choose an element U of $\mathcal{U}$ containing x. Since U is open, there is a base element B_n such that $x \in B_n \subseteq U$. Because B_n lies in an element of $\mathcal{U}$, the index n belongs to the set J, so $B_n \in \mathcal{B}'$. Thus $\mathcal{B}'$ is a countable refinement of $\mathcal{U}$ that covers X, and hence $\mathcal{U}$ has a countable subcollection that covers X.

Finally, for (c), from each nonempty base element B_n, choose a point x_n. Let D be the set consisting of the points x_n. Then D is dense in X: Given any point x of X, every base element containing x intersects D, so x belongs to $\overline{D}$. □

The above theorem has a partial converse when X is a metric space.

Theorem 1.6.2. *Let X be a metrizable space. Then the following are equivalent:*

(a) X is second countable.

(b) X is separable.

(c) X is Lindelöf.

Proof. The implication $(a) \Rightarrow (b)$ and $(a) \Rightarrow (c)$ are done in Theorem 1.6.1. For $(b) \Rightarrow (a)$, let B be a countable dense subset of X. Then the collection

$$\mathcal{B} = \{B_{1/n}(x) : x \in X, n \in \mathbb{N}\}$$

is a countable base for X. Finally, if X is Lindelöf, for each fixed $n \in \mathbb{N}$ consider the collection

$$\mathcal{U}_n = \{B_{1/n}(x) : x \in X\}$$

This is a cover of X, hence has a countable subcover $\mathcal{U}'_n$. Now vary n, and let $\mathcal{U} = \bigcup_{n=1}^{\infty} \mathcal{U}'_n$. Then $\mathcal{U}$ is a base of X, and is countable. □

1.7 Nets and filters

1.7.1 Nets

A **directed set** is a set A equipped with a binary relation $\preceq$ such that

- $\alpha \preceq \alpha$ for all $\alpha \in A$;
- if $\alpha \preceq \beta$ and $\beta \preceq \gamma$, then $\alpha \preceq \gamma$;
- for any $\alpha, \beta \in A$ there exists $\gamma \in A$ such that $\alpha \preceq \gamma$ and $\beta \preceq \gamma$.

A **net** in a set X is a mapping $x : \alpha \mapsto x_\alpha$ from a directed set A into X. We shall usually denote such a mapping by $(x_\alpha)_{\alpha \in A}$, or just by (x_α) if A is understood, and we say that (x_α) is indexed by A.

Let X be a topological space and E a subset of X. A net $(x_\alpha)_{\alpha \in A}$ is **eventually in E** if there exists $\alpha_0 \in A$ such that $x_\alpha \in E$ for $\alpha \succeq \alpha_0$, and (x_α) is **frequently in E** if for every $\alpha \in A$ there exists $\beta \succeq \alpha$ such that $x_\beta \in E$. A point $x \in X$ is a **limit point** of (x_α) (or (x_α) converges to x) if for every neighborhood U of x, (x_α) is *eventually* in U, and x is a **cluster point** of (x_α) if for every neighborhod U of x, (x_α) is *frequently* in U.

The next propositions show that nets are a good substitute for sequences.

Proposition 1.7.1. *A topological space X is Hausdorff if and only if the limit of every convergent net is unique.*

Proof. If X is Hausdorff and (x_α) is a net converging to $x \in X$. Then for any $y \neq x$, there exists disjoint neighborhoods U, V such that $x \in U$, $y \in V$. If x_α also converges to y, then there exists β and β' such that $x_\alpha \in U$ for $\alpha \geq \beta$ and $x_\alpha \in V$ for $\alpha \geq \beta'$. Choose $\gamma \geq \beta$ and $\gamma \geq \beta'$, then $x_\gamma \in U \cap V = \varnothing$, which is a contradiction.

Conversely, if X is not Hausdorff, then there exists $x, y \in X$, $x \neq y$ such that $U \cap V \neq \varnothing$ for $U \in \mathfrak{U}(x)$ and $V \in \mathfrak{U}(y)$. Choose $x_{U,V} \in U \cap V$ for each $U \in \mathfrak{U}(x)$ and $V \in \mathfrak{U}(y)$, we then get a net $(x_{U,V})$ in X. It is clear that $(x_{U,V})$ converges to both x and y, thus the claim follows. □

Proposition 1.7.2. *If X is a topological space, $E \subseteq X$, and $x \in X$, then x is a limit point of E if and only if there is a net in $E \setminus \{x\}$ that converges to x, and $x \in \overline{E}$ if and only if there is a net in E that converges to x.*

Proof. If x is a limit point of E, let $\mathcal{N}$ be the set of neighborhoods of x, directed by reverse inclusion. For each $U \in \mathcal{N}$, pick $x \in (U \setminus \{x\}) \cap E$. Then x_U converges to x. Conversely, if $x_\alpha \in E \setminus \{x\}$ and $x_\alpha \to x$, then every punctured neighborhood of x contains some x_α, so x is an accumulation point of E. The second claim is then clear. □

Proposition 1.7.3. *If X and Y are topological spaces and $f : X \to Y$, then f is continuous at $x \in X$ if and only if for every net (x_α) converging to x, $(f(x_\alpha))$ converges to $f(x)$.*

Proof. If f is continuous at x and V is a neighborhood of $f(x)$, then $f^{-1}(V)$ is a neighborhood of x. Hence, if $x_\alpha \to x$, then (x_α) is eventually in $f^{-1}(V)$, so $(f(x_\alpha))$ is eventually in V, and thus $f(x_\alpha) \to f(x)$. On the other hand, if f is not continuous at x, there is a neighborhood V of $f(x)$ such that $f^{-1}(V)$ is not a neighborhood of x, that is, $x \notin \operatorname{Int} f^{-1}(V)$, or equivalently, $x \in \overline{f^{-1}(V^c)}$. By Proposition 1.7.2, there is a net (x_α) in $f^{-1}(V^c)$ that converges to x. But then $f(x_\alpha) \notin V$, so $f(x_\alpha)$ does not converge to $f(x)$. □

Proposition 1.7.4. *A net (x_α) in a product $X = \prod_s X_s$ converges to x if and only if for each s, $\pi_s(x_\alpha) \to \pi_s(x)$ in X_s.*

Proof. If $x_\alpha \to x$, then since each π_s is continuous, $\pi_s(x_\alpha) \to \pi_s(x)$ by the previous theorem, for each s.

Suppose on the other hand that $\pi_s(x_\alpha) \to \pi_s(x)$ for each s. Let $U = \bigcap_{i=1}^n \pi_{s_i}^{-1}(U_{s_i})$ be a basic neighborhod of x in the product space. Then for each $i = 1, \ldots, n$ there is a α_i such that whenever $\pi_{s_i}(x_\alpha) \in U_{s_i}$ for $\alpha \geq \alpha_i$. Thus if β is picked greater than all of $\alpha_1, \ldots, \alpha_n$, we have $\pi_{s_i}(x_\alpha) \in U$ for all $\alpha \geq \beta$. It follows that $x_\alpha \to x$ in the product space. □

A **subnet** of a net $(x_\alpha)_{\alpha \in A}$ is a net $(x_{\alpha_\beta})_{\beta \in B}$ together with a map $\beta \mapsto \alpha_\beta$ from B to A such that for every $\alpha_0 \in A$ there exists $\beta_0 \in B$ such that $\alpha_\beta \geq \alpha_0$ whenever $\beta \geq \beta_0$. Clearly if (x_α) converges to a point x, then so does any subnet (x_{α_β}).

Proposition 1.7.5. *If $(x_\alpha)_{\alpha \in A}$ is a net in a topological space X, then $x \in X$ is a cluster point of (x_α) if and only if (x_α) has a subnet that converges to x.*

Proof. If (x_{α_β}) is a subnet converging to x and U is a neighborhood of x, choose $\beta_1 \in B$ such that $x_{\alpha_\beta} \in U$ whenever $\beta \geq \beta_1$. Also, given $\alpha_0 \in A$, choose $\beta_2 \in B$ such that $\alpha_\beta \geq \alpha_0$ for $\beta \geq \beta_2$. Then there exists $\beta \in B$ with $\beta \geq \beta_1$ and $\beta \geq \beta_2$, and we have $\alpha_\beta \geq \alpha_0$ and $x_{\alpha_\beta} \in U$. Thus (x_α) is frequently in U, so x is a cluster point of (x_α).

Conversely, if x is a cluster point of (x_α), let $\mathcal{N}$ be the set of neighborhoods of x and make $\mathcal{N} \times A$ into a directed set by declaring that $(U, \alpha) \preceq (U', \alpha')$ iff $U \supseteq U'$ and $\alpha \preceq \alpha'$. For each $(U, \alpha) \in \mathcal{N} \times A$ we can choose $\alpha_{(U,\gamma)} \in A$ such that $\alpha_{(U,\gamma)} \succeq \gamma$ and $x_{\alpha_{(U,\gamma)}} \in U$. Then if $(U', \gamma') \succeq (U, \gamma)$ we have $\alpha_{(U',\gamma')} \succeq \gamma' \succeq \gamma$ and $x_{\alpha_{(U',\gamma')}} \in U' \subseteq U$, whence it follows that $(x_{\alpha_{(U,\gamma)}})$ is a subnet of (x_α) that converges to x. □

Definition 1.7.6. *A net (x_α) in a set X is an **ultranet** (universal net) if for each subset E of X, (x_α) is either eventually in E or eventually in E^c.*

It follows from this definition that if an ultranet is frequently in E then it is eventually in E. In particular, an ultranet in a topological space must converge to each of its cluster points.

For any directed set A, the map $P : A \to X$, defined by $P(\alpha) = x$ for all $\alpha \in A$, gives an ultranet on X, called the **trivial ultranet**. Nontrivial ultranets can be proved to exist but none has ever been explicitly constructed. Most facts about ultranets are best developed using filters and ultrafilters as a vehicle.

Proposition 1.7.7. *If (x_α) is an ultranet in X and $f : X \to Y$, then $(f(x_\alpha))$ is an ultranet in Y.*

Proof. If $A \subseteq Y$, then $f^{-1}(A) = f^{-1}(A^c)^c$, so (x_α) is eventually in either $f^{-1}(A)$ or $f^{-1}(A^c)$, from which it follows that $(f(x_\alpha))$ is eventually in either A or A^c. Thus, $(f(x_\alpha))$ is an ultranet. □

1.7.2 Filters

We have already seen that net provides an effective approach to the topology of a topological space X. In this part we introduce another tool to do this job, namely filters. Later we will see that these two concepts are equivalent.

Definition 1.7.8. *A **filter** $\mathfrak{F}$ on a set X is a nonempty collection of subsets of X with the properties:*

(F1) Every subset of X which contains a set of $\mathfrak{F}$ belongs to $\mathfrak{F}$.

(F2) Every finite intersection of sets of $\mathfrak{F}$ belongs to $\mathfrak{F}$.

(F3) The empty set is not in $\mathfrak{F}$.

A filter $\mathfrak{F}$ on X defines a structure on X, the axioms of which are (F1), (F2) and (F3); this structure is called a **structure of a filtered set**, and the set X endowed with this structure is called **a set filtered by** $\mathfrak{F}$.

Example 1.7.9 (Example of Filters).

(a) Let X be any set, $A \subseteq X$. Then $\{F \subseteq X : A \subseteq F\}$ is a filter on X with a particularly simple filter base, the collection consisting of the single set A.

(b) Let X be any topological space, $A \subseteq X$. Then $\{U \subseteq X : A \subseteq \operatorname{Int} U\}$ is a filter on X. In particular, the set $\mathfrak{U}(x)$ of all neighborhods of $x \in X$ is a filter on X, and any neighborhod base at x is a filterbase for $\mathfrak{U}(x)$. This filter will sometimes be called the **neighborhod filter** at x.

(c) If X is an infinite set, the complements of the finite subsets of X are the elements of a filter.This is called the **Fréchet filter on** X.

If $\mathfrak{F}_1$ and $\mathfrak{F}_2$ are filters on X, we say $\mathfrak{F}_1$ is **finer** than $\mathfrak{F}_2$ (or $\mathfrak{F}_2$ is **coarser** than $\mathfrak{F}_1$) if $\mathfrak{F}_1 \supseteq \mathfrak{F}_2$. Two filters are said to be comparable if one is finer than the other. The set of all filters on X is ordered by the relation "$\mathfrak{F}_1$ is coarser than $\mathfrak{F}_2$"; this relation is induced by the inclusion relation. The filter formed by the single set X is the smallest element of the ordered set of all filters on X. We shall see later that, if X has more than one element, the set of all filters on X has no greatest element.

Let $(\mathfrak{F}_i)_{i\in I}$ be any nonempty family of filters on a set X, then the set

$$\mathfrak{F} = \bigcap_{i\in I} \mathfrak{F}_i$$

is a filter on X, called the **intersection** of the family of filters $(\mathfrak{F}_i)_{i\in I}$ and is obviously the greatest lower bound of the set of the $\mathfrak{F}_i$, in the ordered set of all filters on X.

Given a set $\mathfrak{S}$ of subsets of a set X, let us consider whether there are any filters on X which contain $\mathfrak{S}$. If such a filter exists then by (F2) it contains also the set $\mathfrak{S}'$ of finite intersections of sets of $\mathfrak{S}$; hence a necessary condition for such a filter to exist is that the empty subset of X is not in $\mathfrak{S}'$. This condition is also sufficient, for by (F1) any filter which contains $\mathfrak{S}'$ also contains the set $\mathfrak{F}$ of subsets of X which contain a set of $\mathfrak{F}$. Now $\mathfrak{F}$ clearly satisfies (F1); it satisfies (F2) by reason of the definition of $\mathfrak{S}'$; and finally it satisfies (F3) because the empty set does not belong to $\mathfrak{S}$. Hence $\mathfrak{F}$ is the coarsest filter which contains $\mathfrak{S}$, and we have proved:

Proposition 1.7.10. *A necessary and sufficient condition that there should exist a filter on X containing a set $\mathfrak{S}$ of subsets of X is that no finite subset of $\mathfrak{S}$ has an empty intersection.*

The filter $\mathfrak{F}$ defined above is said to be **generated** by $\mathfrak{S}$, and $\mathfrak{S}$ is said to be a **subbase** of $\mathfrak{F}$.

Corollary 1.7.11. *Let $\mathfrak{F}$ be a filter on a set X, and A a subset of X. Then there is a filter $\mathfrak{G}$ which is finer than $\mathfrak{F}$ and such that $A \in \mathfrak{G}$, if and only if A meets all the sets of $\mathfrak{F}$.*

Corollary 1.7.12. *A set Φ of filters on a non-empty set X has a least upper bound in the set of all filters on X if and only if, for all finite sequences $(\mathfrak{F}_i)_{i=1}^n$ of elements of Φ and all $A_i \in \mathfrak{F}_i$, the intersection $A_1 \cap \cdots \cap A_n$ is not empty.*

Corollary 1.7.13. *The ordered set of all filters on a non-empty set X is inductive (every linearly ordered subset has a upper bound).*

Proof. For every linearly ordered set Φ of filters satisfies the condition of Corollary 1.7.12, since the sets A_i all belong to the same $\mathfrak{F}_j$ by hypothesis, and we can apply (F2). □

If $\mathfrak{S}$ is a subbase of a filter $\mathfrak{F}$ on X, then $\mathfrak{F}$ is not in general the set of subsets of X which contain a set of $\mathfrak{S}$; for $\mathfrak{S}$ to have this property it is necessary and sufficient that every finite intersection of sets of $\mathfrak{S}$ should contain a set of $\mathfrak{S}$. Hence the following proposition:

Proposition 1.7.14. *Let $\mathfrak{B}$ be a set of subsets of a set X. Then the set of subsets of X which contain a set of $\mathfrak{B}$ is a filter if and onlY if $\mathfrak{B}$ has the following two properties:*

(B1) The intersection of two sets of $\mathfrak{B}$ contains a set of $\mathfrak{B}$.

(B2) $\mathfrak{B}$ is not empty, and the empty set is not in $\mathfrak{B}$.

Definition 1.7.15. *A set $\mathfrak{B}$ of subsets of a set X which satisfies axioms (B1) and (B2) is said to be a* ***base*** *of the filter it generates. Two filter bases are said to be* ***equivalent*** *if they generate the same filter.*

If $\mathfrak{S}$ is a subbase of a filter $\mathfrak{F}$, then the set $\mathfrak{B}$ of finite intersections of sets of $\mathfrak{S}$ is a base of $\mathfrak{F}$.

Proposition 1.7.16. *A subset $\mathfrak{B}$ of a filter $\mathfrak{F}$ on X is a base of $\mathfrak{F}$ if and only if every set of $\mathfrak{F}$ contains a set of $\mathfrak{B}$.*

Proof. If $\mathfrak{B}$ is a base of $\mathfrak{F}$, then clearly every set of $\mathfrak{F}$ contains a set of $\mathfrak{B}$; conversely, if every set of $\mathfrak{F}$ contains a set of $\mathfrak{B}$, then the set of subsets of X containing a set of $\mathfrak{B}$ coincides with $\mathfrak{F}$ by reason of (F1). □

Corollary 1.7.17. *A filter $\mathfrak{F}'$ with base $\mathfrak{B}'$ is finer than a filter $\mathfrak{F}$ with base $\mathfrak{B}$ if and only if every set of $\mathfrak{B}$ contains a set of $\mathfrak{B}'$.*

Corollary 1.7.18. *Two filter bases $\mathfrak{B}$ and $\mathfrak{B}'$ on a set X are equivalent if and only if every set of $\mathfrak{B}$ contains a set of $\mathfrak{B}'$ and every set of $\mathfrak{B}'$ contains a set of $\mathfrak{B}$.*

Example 1.7.19 (Example of Filterbases).

(a) Let X be a topological space. Proposition 1.7.16 shows that the bases of the neighbourhood filter of a point $x \in X$ are precisely the fundamental systems of neighbourhoods of x.

(b) Let $(X, \preceq)$ be a non-empty directed set. For each $a \in X$, the set $S(a)$ of all $x \in X$ such that $a \preceq x$ will be called the section of X relative to the element a. Then the set $\mathfrak{B}$ of sections of X is a filter base, for it clearly satisfies (B2), and if a, b are any two elements of X, then there is by hypothesis an element $c \in X$ such that $a \preceq c$ and $b \preceq c$, and therefore $S(a) \cap S(b) \supseteq S(c) \neq \varnothing$, so that (B1) is satisfied. The filter generated by $\mathfrak{B}$ is called the **section filter** of the directed set X.

Finally, we introduce ultrafilters. An **ultrafilter** on a set X is a filter $\mathfrak{F}$ such that there is no filter on X which is strictly finer than $\mathfrak{F}$ (in other words, a maximal element in the ordered set of all filters on X). Since the ordered set of all filters on X is inductive, Zorn's lemma shows that:

Proposition 1.7.20. *If $\mathfrak{F}$ is any filter on a set X, there is an ultrafilter finer than $\mathfrak{F}$.*

Theorem 1.7.21. *Let $\mathfrak{F}$ be a filter on a set X. Then the following are equivalent:*

(i) *$\mathfrak{F}$ is an ultrafilter.*

(ii) *If $A \cup B \in \mathfrak{F}$, then either $A \in \mathfrak{F}$ or $B \in \mathfrak{F}$.*

(iii) *For every subset $A \subseteq X$, either $A \in \mathfrak{F}$ or $A^c \in \mathfrak{F}$.*

Proof. If there exist subsets A and B of X such that $A \notin \mathfrak{F}$ and $B \notin \mathfrak{F}$ but $A \cup B \in \mathfrak{F}$. Let $\mathfrak{G}$ be the set of subsets F of X such that $A \cup F \in \mathfrak{F}$. It is straightforward to check that $\mathfrak{G}$ is a filter on X, and $\mathfrak{G}$ is strictly finer than $\mathfrak{F}$, since $B \in \mathfrak{G}$; but this contradicts the hypothesis that $\mathfrak{F}$ is an ultrafilter. This proves $(i) \Rightarrow (ii)$.

Also, (ii) implies (iii), since we have $A \cup A^c = X \in \mathfrak{F}$ for any $A \subseteq X$. Finally, assume (iii), and let $A \in \mathfrak{G}$ where $\mathfrak{G}$ is a filter containing $\mathfrak{F}$. Then if $A \notin \mathfrak{F}$ we will have $A^c \in \mathfrak{F} \subseteq \mathfrak{G}$, which contradicts (F3). Thus $\mathfrak{F}$ is an ultrafilter. □

By induction, the following corollary is true.

Corollary 1.7.22. *If the union of a finite sequence $(A_i)_{i=1}^n$ of subsets of X belongs to an ultrafilter $\mathfrak{F}$, then at least one of the A_i belongs to $\mathfrak{F}$. In particular, if $(A_i)_{i=1}^n$ is a covering of X, then at least one of the A_i belongs to $\mathfrak{F}$.*

Example 1.7.23.

(a) A filter $\mathfrak{F}$ on X is a fixed ultrafilter if and only if $\mathfrak{F} = \mathfrak{U}(x)$ for some $x \in X$. By the criterion given in Theorem 1.7.21, each filter of this form is an ultrafilter. On the other hand, if $\mathfrak{F}$ is a fixed ultrafilter, say $\bigcap \mathfrak{F} = A \neq \varnothing$, then $\mathfrak{F}$ must be the filter of all sets containing A (since this is a filter containing $\mathfrak{F}$) and A must be a single point (since the filter of all sets containing $x \in A$ is finer than $\mathfrak{F}$). Such ultrafilters are called **trivial**.

(b) The Frechet filter $\mathfrak{F}$ on $\mathbb{R}$ is contained in some ultrafilter $\mathcal{G}$. Since $\mathfrak{F}$ is free, $\mathcal{G}$ must be also be free.

(c) The ultrafilter containing a given filter $\mathfrak{F}$ need not be unique. For if $\mathfrak{F}$ is the filter of all sets containing $A \subseteq X$, then for each $x \in A$, the filter of all sets containing x is an ultrafilter containing $\mathfrak{F}$. In fact, if a filter is contained in a unique ultrafilter, it is itself an ultrafilter.

Proposition 1.7.24. *Every filter $\mathfrak{F}$ on a set X is the intersection of the ultra filters finer than $\mathfrak{F}$.*

Proof. Clearly this intersection contains $\mathfrak{F}$. Conversely, let A be a subset of X which does not belong to $\mathfrak{F}$. Then A contains no set of $\mathfrak{F}$; hence every $F \in \mathfrak{F}$ meets A^c and there is a filter $\mathfrak{F}'$ which is finer than $\mathfrak{F}$ and contains A^c. If $\mathfrak{U}$ is an ultrafilter finer than $\mathfrak{F}'$ it follows that $A \notin \mathfrak{F}$. This completes the proof. □

1.7.3 Construction of filters

Proposition 1.7.25. *Let $\mathfrak{F}$ be a filter on a set X and A a subset of X. Then the trace $\mathfrak{F}_A$ of $\mathfrak{F}$ on A is a filter if and only if each set of $\mathfrak{F}$ meets A.*

Proof. Since $(F \cap G) \cap A = (F \cap A) \cap (G \cap A)$ we see that $\mathfrak{F}_A$ satisfies (F2); again, if $F \cap A \subseteq G \subseteq A$ then $G = (F \cup G) \cap A \in \mathfrak{F}_A$, whence $\mathfrak{F}_A$ satisfies (F1). Hence $\mathfrak{F}_A$ is a filter if and only if it satisfies (F3), i.e. if and only if each set of $\mathfrak{F}$ meets A. In particular, if $A \in \mathfrak{F}$ then $\mathfrak{F}_A$ is a filter on A, by (F1) and (F3). □

Definition 1.7.26. *Let A be a subset of a set X and $\mathfrak{F}$ a filter on X. If the trace of $\mathfrak{F}$ on A is a filter on A, this filter is said to be **induced** by $\mathfrak{F}$ on A.*

If a filter $\mathfrak{F}$ on X induces a filter on $A \subseteq X$, then the trace on A of a base of $\mathfrak{F}$ is a base of $\mathfrak{F}_A$, by Proposition 1.7.16.

Example 1.7.27. Let X be a topological space, A a subset of X, x a point of X. In order that the trace on A of the **neighbourhood filter** $\mathfrak{B}$ of x should be a filter on A, it is necessary and sufficient that every neighbourhood of x meets A, i.e. that x lies in the closure of A.

This example of an induced filter is of interest for two reasons: first because it plays an important role in the theory of limits and secondly because every filter can be defined in this way. Indeed, let $\mathfrak{F}$ be a filter on a set X and let X' be the set obtained by adjoining a new

element ω to X, X being identified with the complement of $\{\omega\}$ in X'; let $\mathfrak{F}'$ be the filter on X' consisting of the sets $F \cup \{\omega\}$, where F runs through $\mathfrak{F}$. For each point $x \neq \omega$ of X', let $\mathfrak{U}(x)$ be the set of all subsets of X' which contain x, and let $\mathfrak{U}(\omega)$ be $\mathfrak{F}'$; then the $\mathfrak{U}(x)$ for $x \in X'$ obviously satisfy the axioms in Proposition 1.1.18, and therefore define a topology on X' for which they are the neighbourhood filters of points. Finally ω lies in the closure of X in this topology, and $\mathfrak{F}$ is induced by $\mathfrak{F}' = \mathfrak{U}(\omega)$ on X. The topology thus defined on X' (resp. the set X' with this topology) is called the **topology** (resp. the topological space) **associated with** $\mathfrak{F}'$.

Proposition 1.7.28. *An ultrafilter $\mathfrak{U}$ on a set X induces a filter on a subset A of X if and only if $A \in \mathfrak{U}$ and if this condition is satisfied then $\mathfrak{U}_A$ is an ultrafilter on A.*

Proof. This follows from the characterization in Theorem 1.7.21. □

Let $\mathfrak{B}$ be a filter base on a set X, and let f be a mapping of X into a set Y; then $f(\mathfrak{B})$ is a filter base on Y, for the relation $A \neq \varnothing$ implies $f(A) \neq \varnothing$, and we have $f(A \cap B) \subseteq f(A) \cap f(B)$. If $\mathfrak{B}_1$ is a base of a filter which is finer than the filter of base $\mathfrak{B}$, then $f(\mathfrak{B}_1)$ is a base of a filter finer than the filter of base $f(\mathfrak{B})$, by Corollary 1.7.17.

Proposition 1.7.29. *If $\mathfrak{B}$ is an ultrafilter base on a set X and if f is a mapping of X into a set Y, than $f(\mathfrak{B})$ is an ultrafilter base on Y.*

Proof. Let N be a subset of Y. If $f^{-1}(N)$ contains a set M of $\mathfrak{B}$, then N contains $f(M)$; if not, then $f^{-1}(N)^c = f^{-1}(N^c)$ contains a set M of $\mathfrak{B}$ and therefore N^c contains $f(M)$. Hence the result follows from Theorem 1.7.21. □

Consider in particular the case where f is the canonical injection $A \hookrightarrow X$ of a subset A of a set X. If $\mathfrak{B}$ is a filter base on A then $f(\mathfrak{B})$ is a filter base on X. The filter $\mathfrak{F}$ on X generated by $f(\mathfrak{B})$ is called the **direct image** of $\mathfrak{B}$ under f. If $\mathfrak{B}$ is an ultrafilter hase on A it is also an ultrafilter base on X by reason of Corollary 1.7.17.

Let us next examine whether the **inverse image** of a filter base is a filter base. Let $\mathfrak{B}$ be a filter base on a set Y, and let f be a mapping of a set X into Y; then $f^{-1}(\mathfrak{B})$ is a filter base on X if and only if $f^{-1}(N) \neq \varnothing$ for each $N \in \mathfrak{B}$. This condition can also be expressed by saying that every set of $\mathfrak{B}$ meets $f(X)$. If this condition is satisfied, then $f(f^{-1}(\mathfrak{B}))$ is a base of a filter *finer* than the filter of base $\mathfrak{B}$ (by $N \supseteq f(f^{-1}(N))$ and Corollary 1.7.17).

If $\mathfrak{B}$ is a filter base on X it is clear that the above condition is satisfied by $\mathfrak{B}' = f(\mathfrak{B})$; $f^{-1}(f(\mathfrak{B}))$ is then a base of a filter *coarser* than the filter of base $\mathfrak{B}$ (by $f(f^{-1}(M)) \supseteq M$ and Corollary 1.7.17).

Let $(X_i)_{i\in I}$ be a family of sets, and for each $i \in I$ let $\mathfrak{B}_i$ be a filter base on X_i. Let $\mathfrak{B}$ be the set of subsets of the product set $X = \prod_{i\in I} X_i$ which are of the form $\prod_{i\in I} M_i$ where $M_i = X_i$ except for a finite number of indices and where $M_i \in \mathfrak{B}_i$ for each $i \in I$ such that $M_i \neq X_i$. The formula $(\prod_{i\in I} M_i) \cap (\prod_{i\in I} N_i) = \prod_{i\in I}(M_i \cap N_i)$ shows that $\mathfrak{B}$ is a filter base on X. Note that the filter of base $\mathfrak{B}$ is also generated by the sets $\pi_i^{-1}(M_i)$, where $M_i \in \mathfrak{B}_i$ and i runs through I, since

$$\pi_i^{-1}(M_i) = M_i \times \prod_{j\neq i} X_j.$$

The filter of base $\mathfrak{B}$ is the product filter of $\mathfrak{F}_i$, which we now define.

Definition 1.7.30. *Given a filter $\mathfrak{F}_i$ on each set X_i of a family of sets $(X_i)_{i\in I}$, the product of the filters $\mathfrak{F}_i$ is the filter on $X = \prod_{i\in I} X_i$, which has as a base the set of subsets of X of the form $\prod_{i\in I} M_i$, where $M_i \in \mathfrak{F}_i$ for each $i \in I$ and $M_i = X_i$ for all but a finite number of indices. The product filter is denoted $\prod_{i\in I} \mathfrak{F}_i$.*

Proposition 1.7.31. *The product of the filters $\mathfrak{F}_i$ is the coarsest filter $\mathfrak{G}$ on X such that $\pi_i(\mathfrak{G}) = \mathfrak{F}_i$ for each $i \in I$.*

Proof. By definition, $\prod_{i\in I} \mathfrak{F}_i$ has a base consists of sets of the form $\prod_{i\in I} M_i$, where $M_i \in \mathfrak{F}_i$ for each $i \in I$ and $M_i = X_i$ for all but a finite number of indices. These sets are mapped under π_j to $\mathfrak{F}_j$, for each index $j \in I$. Thus $\pi_j(\prod_{i\in I} \mathfrak{F}_i) = \mathfrak{F}_i$ for each j.

Conversely, let $\mathfrak{G}$ be a filter on X satisfying this condition. Then for each j and $M_j \in \mathfrak{F}_j$, $\pi_j(N) \subseteq M_j$ for some $N \subseteq X$. It then follows that $N \subseteq M_i \prod_{i\neq j} X_j$, whence $M_i \prod_{i\neq j} X_j \in \mathfrak{G}$. Since j is arbitrary, we see $\prod_{i\in I} \mathfrak{F}_i \subseteq \mathfrak{G}$. □

Corollary 1.7.32. *If $\mathfrak{B}_i$ is a base of $\mathfrak{F}_i$ for each $i \in I$, then $\mathfrak{B}$ is a base of the product filter $\prod_{i\in I} \mathfrak{F}_i$.*

Example 1.7.33. On a product $X = \prod_{i\in I} X_i$ of topological spaces, the neighbourhood filter of any point $x = (x_i)$ is the product of the neighbourhood filters of the x_i's.

1.7.4 Limit of filters

Now we define the convergence of a filter.

Definition 1.7.34. *A filter $\mathfrak{F}$ on a topological space X is said to **converge to $x \in X$** (written $\mathfrak{F} \to x$) if $\mathfrak{U}(x) \subseteq \mathfrak{F}$. That is, if $\mathfrak{F}$ is finer than the neighborhod filter at x. We say $\mathfrak{F}$ has x as a **cluster point** (or, $\mathfrak{F}$ **clusters at x**) if each $F \in \mathfrak{F}$ meets each $U \in \mathfrak{U}(x)$. It is clear that if $\mathfrak{F} \to x$, then $\mathfrak{F}$ clusters at x.*

It will be convenient to have the notions of convergence and clustering available for filter bases; they generalize easily and obviously. A filter base $\mathcal{B}$ **converges to x** if each $U \in \mathfrak{U}(x)$ contains some $B \in \mathcal{B}$ (iff the filter generated by $\mathcal{B}$ converges to x); $\mathcal{B}$ **clusters at x** if each $U \in \mathfrak{U}(x)$ meets each $B \in \mathcal{B}$ (iff the filter generated by $\mathcal{B}$ clusters at x).

Lemma 1.7.35. *Let $\mathfrak{F}$ be a filter on X. Then $\mathfrak{F}$ clusters to $x \in X$ if and only if $x \in \bigcap_{M\in\mathfrak{F}} \overline{F}$.*

Proof. Since $x \in \overline{F}$ if and only if F meets every element of $\mathfrak{U}(x)$, the claim is clear by definition. □

Example 1.7.36.

(a) Let X be a topological space, $A \subseteq X$. The cluster points of the filter $\mathfrak{F} = \{U \subseteq X : A \subseteq U\}$ include each point of $\overline{A}$.

(b) The Fréchet filter on $\mathbb{R}$ has no cluster points.

(c) Let $\mathfrak{F}$ be the filter on $\mathbb{R}$ generated by the filter base $\mathcal{B} = \{(0, \varepsilon) : \varepsilon > 0\}$. Then $\mathfrak{F} \to 0$ (although 0 does not belong to every element of $\mathfrak{F}$).

Proposition 1.7.37. *$\mathfrak{F}$ has x as a cluster point if and only if there is a filter $\mathcal{G}$ finer than $\mathfrak{F}$ which converges to x.*

Proof. If $\mathfrak{F}$ has x as a cluster point, the collection $\mathcal{B} = \{U \cap F : U \in \mathfrak{U}(x), F \in \mathfrak{F}\}$ is a filterbase for a filter $\mathcal{G}$ which is finer than $\mathcal{G}$ and converges to x (note that $X \in \mathfrak{F}$, so $\mathfrak{U}(x)$ is contained in $\mathcal{B}$, and hence $\mathcal{G}$).

Conversely, if $\mathfrak{F} \subseteq \mathcal{G} \to x$, then each $F \in \mathfrak{F}$ and each neighborhood U of x belong to $\mathcal{G}$ and hence meet, so $\mathfrak{F}$ clusters at x. □

According to the next propositions, filter convergence is adequate to the task of describing topological concepts.

Proposition 1.7.38. *A topological space X is Hausdorff if and only if the limit of every convergent filter is unique.*

Proof. If X is Hausdorff. let $x, y \in X$ be distinct and $\mathfrak{F}$ be a filter converges to x and y. Then since x and y have disjoint neighborhods, it follows that $\varnothing \in \mathfrak{F}$, which is impossible. Conversely, if X is not Hausdorff, then there exists $x, y \in X$, $x \neq y$ such that $U \cap V \neq \varnothing$ for any $U \in \mathfrak{U}(x), V \in \mathfrak{U}(y)$. Then $\mathcal{B} = \{U \cap V : U \in \mathfrak{U}(x), V \in \mathfrak{U}(y)\}$ is a filterbase, so it generates a filter $\mathfrak{F}$. It is clear that $\mathfrak{F}$ converges to both x and y. □

Proposition 1.7.39. *Let X be a topological space and $x \in X$. If $E \subseteq X$, then $x \in \overline{E}$ if and only if there is a filter $\mathfrak{F}$ such that $E \in \mathfrak{F}$ and $\mathfrak{F} \to x$.*

Proof. If $x \in \overline{E}$, then $\mathcal{B} = \{U \cap E : U \in \mathfrak{U}(x)\}$ is a filter base. The resulting filter contains E and converges to x. Conversely, if $E \in \mathfrak{F} \to x$, then x is a cluster point of $\mathfrak{F}$ and hence $x \in \overline{E}$. □

If $\mathfrak{F}$ is a filter on X and $f : X \to Y$, then $f(\mathfrak{F})$ is the filter on Y generated by $f(\mathfrak{F})$.

Proposition 1.7.40. *Let $f : X \to Y$ be a map between topological spaces. Then f is continuous at $x \in X$ if and only if whenever $\mathfrak{F} \to x$ in X then $f(\mathfrak{F}) \to f(x)$ in Y.*

Proof. Suppose f is continuous at x and $\mathfrak{F} \to x$. Let V be any neighborhod of $f(x)$ in Y. Then for some neighborhood U of x in X, $f(U) \subseteq V$. Then since $U \in \mathfrak{F}$, $V \in f(\mathfrak{F})$. Thus $f(\mathfrak{F}) \to f(x)$.

Conversely, suppose whenever $\mathfrak{F} \to x$ in X then $f(\mathfrak{F}) \to f(x)$ in Y. Let $\mathcal{U}(x)$ be the filter of all neighborhoods of x in X. Then since $f(\mathfrak{U}(x)) \to f(x)$, each neighborhood V of $f(x)$ belongs to $f(\mathfrak{U}(x))$, so for some neighborhood U of x, $f(U) \subseteq V$. Thus f is continuous at x. □

Proposition 1.7.41. *A filter $\mathfrak{F}$ converges to x in $X = \prod_s X_s$ if and only if $\pi_s(\mathfrak{F}) \to \pi_s(x)$ in X_s for each s.*

Proof. If $\mathfrak{F} \to x$ then $\pi_s(\mathfrak{F}) \to \pi(x)$ for each s by continuity. Conversely, suppose that $\pi_s(\mathfrak{F}) \to \pi_s(x)$ for each s. Let $U = \bigcap_{i=1}^n \pi_{s_i}^{-1}(U_{s_i})$ be a basic neighborhood of x in X. Then U_{s_i} is a neighborhood of $\pi_{s_i}(x)$ for each i, so $U_{s_i} \in \pi_{s_i}(\mathfrak{F})$ for each i, and hence $\pi_{s_i}(F_i) \subseteq U_{s_i}$ for some $F_i \in \mathfrak{F}$. Then $\bigcap_{i=1}^n F_i \in \mathfrak{F}$ and $\bigcap_{i=1}^n F_i \subseteq \bigcap_{i=1}^n \pi_{s_i}^{-1}(U_{s_i})$, so $\bigcap_{i=1}^n \pi_{s_i}^{-1}(U_{s_i}) \in \mathfrak{F}$. Thus $\mathfrak{F} \to x$. □

The similarities between net and filter convergence are manifest. Each describes the topology on a topological space with equal facility, "finer filters" provide a filter analog to "subnets". In addition, there is more than a casual relationship between the ideas behind the two approaches. Thus the fact that a formal bridge can be built between the two notions should come as no surprise.

Definition 1.7.42. *If (x_α) is a net in X, the filter generated by the filter base $\mathcal{B}$ consisting of the sets $B_{\alpha_0} = \{x_\alpha : \alpha \succeq \alpha_0\}$, $\alpha_0 \in A$, is called the* ***filter generated by x_α****.*

Definition 1.7.43. *If $\mathfrak{F}$ is a filter on X, let $A_{\mathfrak{F}} = \{(x, F) :\in F, F \in \mathfrak{F}\}$. Then $A_{\mathfrak{F}}$ is directed by the relation $(x_1, F_1) \preceq (x_2, F_2)$ iff $F_2 \subseteq F_1$, so the map $A_{\mathfrak{F}} \to X, (x, F) \mapsto x$ is a net in X. It is called the* ***net based on*** *$\mathfrak{F}$.*

Theorem 1.7.44. *Let X be a topological space.*

(a) A filter $\mathfrak{F}$ converges to x in X if and only if the net based on $\mathfrak{F}$ converges to x.

(b) A net (x_α) converges to x in X if and only if the filter generated by (x_α) converges to x.

Proof. Suppose $\mathfrak{F} \to x$. If U is a nhood of x, then $U \in \mathfrak{F}$. Pick $y_0 \in U$, then $(y_0, U) \in A_{\mathfrak{F}}$, and if $(y, F) \succeq (y_0, U)$ then $y \in F \subseteq U$. Thus the net based on $\mathfrak{F}$ converges to x.

Conversely, suppose the net based on $\mathfrak{F}$ converges to x. Let U be a nhood of x. Then for some $(y_0, F_0) \in A_{\mathfrak{F}}$ we have $(y, F) \succeq (y_0, F_0)$ implies $y \in U$. But then $F_0 \subseteq U$; otherwise, there is some $y \in F_0 \setminus U$, and then $(y, F_0) \succeq (y_0, F_0)$ but $y \notin U$. Hence $U \in \mathfrak{F}$, so $\mathfrak{F} \to x$.

The net (x_α) converges to x iff each nhood of x contains a tail of (x_α). Since the tails of (x_α) are a base for the filter generated by (x_α), the result follows. □

1.8 Compactness

Recall that an **open cover** of a space X is a collection $\mathcal{U}$ of open subsets of X whose union is X, and a **subcover** of $\mathcal{U}$ is a subcollection of elements of $\mathcal{U}$ that still covers X. A topological space X is said to be **compact** if every open cover of X has a finite subcover. Note that the empty set is compact.

As in the case of connectedness, to say that a subset of a topological space is compact is to say that it is a compact space when endowed with the subspace topology. In this situation, it is often useful to extend our terminology in the following way. If X is a topological space and $A \subseteq X$, a collection of subsets of X whose union contains A is also called a **cover of A**; if the subsets are open in X we sometimes call it an **open cover of A**. We try to make clear in each specific situation which kind of open cover of A is meant: a collection of open subsets of A whose union is A, or a collection of open subsets of X whose union contains A. The following lemma shows that either kind of open cover can be used to detect compactness of a subspace; it is an immediate consequence of the definitions of compactness and the subspace topology.

Example 1.8.1. The real line $\mathbb{R}$ is not compact, for the covering of $\mathbb{R}$ by open intervals $\{(n, n+2) : n \in \mathbb{Z}\}$ contains no finite subcollection that covers $\mathbb{R}$.

In general, it takes some effort to decide whether a given space is compact or not. First we shall prove some general theorems that show us how to construct new compact spaces out of existing ones.

Lemma 1.8.2 (Compactness Criterion for Subspaces). *If X is any topological space, a subset $A \subseteq X$ is compact (in the subspace topology) if and only if every cover of A by open subsets of X has a finite subcover.*

Proof. Assume that A is compact and let $\mathcal{U}$ be an open cover of A be open subsets of X. Then the intersection $A \cap \mathcal{U}$ is a open cover of A, hence there are finitely many sets $U_1, \ldots, U_k$ in $\mathcal{U}$ such that $A = \bigcup_{i=1}^k (U_i \cap A)$. This then implies $A \subseteq \bigcup_{i=1}^k U_i$, so $\mathcal{U}$ has a finite subcover.

Conversely, if every cover of A by open subsets of X has a finite subcover. Let $\mathcal{U}$ be an open cover of A consist of open subsets of A. Then by the definition of the subspace topology, each member of $\mathcal{U}$ is the intersection with A of an open subset of X, and we then obtain an open cover of A by open subsets of X. Since this cover has a finite subcover, it is easy to see that $\mathcal{U}$ also has a finite subcover, and hence A is compact. □

Proposition 1.8.3. *Suppose X is a topological space, and (x_i) is a sequence of points in X converging to $x \in X$. Then the set $A = \{x_i : i \in \mathbb{N}\} \cup \{x\}$ is compact in the subspace topology.*

Proof. Suppose $\mathcal{U}$ is a cover of A by open subsets of X. There is some set $U \in \mathcal{U}$ containing x, and U must contain x_i for all but finitely many i. Choosing one set in $\mathcal{U}$ for each of those finitely many elements, we obtain a finite subcover of A. □

The most important fact about compactness is that continuous images of compact spaces are compact.

Proposition 1.8.4. *Let X and Y be topological spaces, and let $f : X \to Y$ be a continuous map. If X is compact, then $f(X)$ is compact.*

Proof. Let $\mathcal{U}$ be a cover of $f(X)$ by open subsets of Y. For each $U \in \mathcal{U}$, $f^{-1}(U)$ is an open subset of X. Since $\mathcal{U}$ covers $f(X)$, every point of X is in some set $f^{-1}(U)$, so the collection $\{f^{-1}(U) : U \in \mathcal{U}\}$ is an open cover of X. By compactness of X, some finite number of these, say $f^{-1}(U_1), \ldots, f^{-1}(U_k)$, cover X. Then it follows that $U_1, \ldots, U_k$ cover $f(X)$. □

Proposition 1.8.5. *Every closed subspace of a compact space is compact.*

Proof. Let A be a closed subspace of the compact space X. Given a covering $\mathcal{U}$ of A by sets open in X, let us form an open covering $\mathcal{V}$ of X by adjoining to $\mathcal{U}$ the single open set A^c. Some finite subcollection of $\mathcal{V}$ covers X. If this subcollection contains the set A^c, discard A^c; otherwise, leave the subcollection alone. The resulting collection is a finite subcollection of $\mathcal{U}$ that covers A. □

Proposition 1.8.6 (Separation of Compact Subsets). *If X is a Hausdorff space and $A, B \subseteq X$ are disjoint compact subsets, there exist disjoint open subsets $U, V \subseteq X$ such that $A \subseteq U$ and $B \subseteq V$. In particular, compact subset of X are closed.*

Proof. First consider the case in which $B = \{y\}$ is a singleton. For each $x \in A$, there exist disjoint open subsets U_x containing x and V_x containing y by the Hausdorff property. The collection $\{U_x : x \in A\}$ is an open cover of A, so it has a finite subcover: call it $\{U_{x_1}, \ldots, U_{x_k}\}$. Let $U = \bigcup_{i=1}^k U_{x_i}$ and $V = \bigcap_{i=1}^k V_{x_k}$. Then U and V are disjoint open subsets with $A \subseteq U$ and $\{y\} \subseteq V$, so this case is proved.

Next consider the case of a general compact subset B. The argument above shows that for each $y \in B$ there exist disjoint open subsets $U_y, V_y \subseteq X$ such that $A \subseteq U_y$ and $y \in V_y$. By compactness of B, finitely many of these, say $V_{y_1}, \ldots, V_{y_k}$, cover B. Then setting $U = \bigcap_{i=1}^k U_{y_k}$ and $V = \bigcup_{i=1}^k V_{y_k}$ proves the result. □

Example 1.8.7. One needs the Hausdorff condition in the hypothesis of Proposition 1.8.6. Consider, for example, the finite complement topology on the real line. The only proper subsets of $\mathbb{R}$ that are closed in this topology are the finite sets. But every subset of $\mathbb{R}$ is compact in this topology.

One important use of the preceding results is as a tool for verifying that a continuous map is closed:

Theorem 1.8.8. *Suppose $f : X \to Y$ is a continuous map from a compact space to a Hausdorff space, then it is closed.*

Proof. Let F be a closed subset of X, then it is compact, so the image $f(F)$ is also compact. By Proposition 1.8.6, $f(F)$ is closed. □

Lemma 1.8.9 (The tube lemma). *Let X and Y be topological spaces and consider the product space $X \times Y$. Let A be a compact subset of X and B be a compact subset of Y. If N is an open set containing $A \times B$, then N contains a neighborhood of $A \times B$ of the form $U \times V$, where U is open in X and V is open in Y.*

Proof. By the definition of the product topology, for each $(a, b) \in A \times B$, there are open sets $U_{(a,b)} \subseteq X$ and $V_{(a,b)} \subseteq Y$ such that $(a, b) \in U_{(a,b)} \times V_{(a,b)} \subseteq N$. For any fixed $a \in A$, the collection $\{V_{(a,b)} : b \in B\}$ is an open cover of B, and thus has a finite subcover; namely, there exists a finite subset B_a of B such that $V_a := \bigcup_{b \in B_a} V_{(a,b)}$ contains B. For each $a \in A$, let $U_a = \bigcap_{b \in B_a} U_{(a,b)}$, which is a neighborhood of a in X since B_a is finite. Moreover, the construction of U_a and V_a implies that $\{a\} \times B \subseteq U_a \times V_a \subseteq N$. We now essentially repeat the argument to drop the dependence on a: By the compactness of A, there exists a finite subset $A_0 \subseteq A$ such that $U = \bigcup_{a \in A_0} U_a$ contains A. Set $V = \bigcap_{a \in A_0} V_a$, it then follows by the above reasoning that $A \times B \subseteq U \times V \subseteq N$, which completes the proof. □

Example 1.8.10. The tube lemma is certainly not true if Y is not compact. For example, let Y be the y-axis in $\mathbb{R}^2$, and let

$$N = \{(x, y) : |x| < (y^2 + 1)^{-1}\}.$$

Then N is an open set containing the set $\{0\} \times \mathbb{R}$, but it contains no tube about $\{0\} \times \mathbb{R}$

Theorem 1.8.11. *The product of finitely many compact spaces is compact.*

Proof. Let X and Y be compact spaces. Let $\mathcal{A}$ be an open covering of $X \times Y$. Given $x_0 \in X$, the slice $x_0 \times Y$ is compact and may therefore be covered by finitely many elements $A_1, \ldots, A_m$ of A. Their union $N = A_1 \cup \cdots \cup A_m$ is an open set containing $x_0 \times Y$; by tube lemma, the open set N contains a tube $W \times Y$ about $x_0 \times Y$, where W is open in X. Then $W \times Y$ is covered by finitely many elements $A_1, \ldots, A_m$ of A. Now since X is compact, $X \times Y$ is covered by finitely many such tubes, which implies $X \times Y$ is covered by finitely many elements of $\mathcal{A}$, thus is compact. □

1.8.1 Limit point compactness and sequencially compactness

A space X is said to be **limit point compact** if every infinite subset of X has a limit point in X, and **sequentially compact** if every sequence of points in X has a subsequence that converges to a point in X.

Proposition 1.8.12. *Compactness implies limit point compactness, but not the converse.*

Proof. Suppose X is compact, and let $S \subseteq X$ be an infinite subset. If S has no limit point in X, then it is closed, hence compact, and every point $x \in X$ has a neighborhood U such that $U \cap S$ is either empty or $\{x\}$. Finitely many of these neighborhoods cover X. But since each

such neighborhood contains at most one point of S, this implies that S is finite, which is a contradiction. □

Example 1.8.13. Let Y consist of two points; give Y the topology consisting of Y and the empty set. Then the space $X = \mathbb{Z}_+ \times Y$ is limit point compact, for every nonempty subset of X has a limit point. It is not compact, for the covering of X by the open sets $U_n = \{n\} \times Y$ has no finite subcollection covering X.

Example 1.8.14. Consider the first uncountable ordinal S_Ω, in the order topology. The space S_Ω is not compact, since it has no largest element. However, it is limit point compact: Let A be an infinite subset of S_Ω. Choose a subset B of A that is countably infinite. Being countable, the set B has an upper bound b in S_Ω; then B is a subset of the interval $[a_0, b]$ of S_Ω, where a_0 is the smallest element of S_Ω. Since S_Ω has the least upper bound property, the interval $[a_0, b]$ is compact. By the preceding theorem, B has a limit point x in $[a_0, b]$. The point x is also a limit point of A. Thus S_Ω is limit point compact.

Proposition 1.8.15. *Sequentially compactness implies limit point compactness, and for first countable Hausdorff spaces they are equivalent.*

Proof. Suppose that X is sequentially compact and let $A \subseteq X$ be an infinite subset. Let $\{x_n\} \subseteq A$ be a sequence such that x_n's are distinct. Then $\{x_n\}$ has a subsequence $\{x_{n_k}\}$ converging to a point $x \in X$. Then by Proposition 1.7.2, x is a limit point of A. Thus X is limit point compact.

Suppose X is first countable Hausdorff and limit point compact, and let (x_n) be any sequence of points in X. If the sequence takes on only finitely many values, then it has a constant subsequence, which is certainly convergent. So we may suppose it takes on infinitely many values. By hypothesis the set of values $\{x_n\}$ has a limit point $x \in X$. If x is actually equal to x_n for infinitely many values of n, again there is a constant subsequence and we are done; so by discarding finitely many terms at the beginning of the sequence if necessary we may assume $x_n \neq x$ for all n. Because X is first countable, there is a nested neighborhood base at x, say $\{V_n\}$. For such a neighborhood base, it is easy to see that any subsequence $\{x_{n_i}\}$ such that $x_{n_i} \subseteq V_i$ converges to x.

Since x is a limit point, we can choose n_1 such that $x_{n_1} \subseteq V_1$. Suppose by induction that we have chosen $n_1 < n_2 < \cdots < n_k$ with $x_{n_i} \in V_i$. Since X is Hausdorff, the sequence takes on infinitely many values in V_{k+1}, so we can choose some $n_{k+1} > n_k$ such that $x_{n_{k+1}} \in V_{k+1}$. This completes the induction, and proves that there is a subsequence x_{n_k} converging to x. □

We now show that these different versions of compactness coincide for certain spaces; for this purpose, we need the following lemma. compactness.

Lemma 1.8.16 (The Lebesgue number lemma). *Let $\mathcal{U}$ be an open covering of the metric space (X, d). If X is sequencially compact, there is a $\delta > 0$ such that for each subset of X having diameter less than δ, there exists an element of $\mathcal{U}$ containing it. The number δ is called a* ***Lebesgue number*** *for the covering $\mathcal{U}$.*

Proof. Let $\mathcal{U}$ be an open covering of X. We assume that there is no $\delta > 0$ such that each set of diameter less than δ has an element of $\mathcal{U}$ containing it, and derive a contradiction.

Our assumption implies in particular that for each positive integer n, there exists a set C_n of diameter less than $1/n$ that is not contained in any element of $\mathcal{U}$. Choose a point $x_n \in C_n$ for

each n. By hypothesis, some subsequence (x_{n_i}) of the sequence (x_n) converges, say to the point x. Now x belongs to some element U of the collection $\mathcal{U}$, and because U is open, there is an $\varepsilon > 0$ such that $B_\varepsilon(x) \subseteq U$. If we choose i so large that $1/n_i < \varepsilon/2$ and $d(x_{n_i}, x) < \varepsilon/2$, then C_{n_i} lies in the ε-neighborhood of x. But this means that $C_{n_i} \subseteq U$, contrary to the hypothesis. □

Proposition 1.8.17. *For metric spaces and second countable topological spaces, sequentially compactness implies compactness.*

Proof. Suppose first that X is second countable and sequentially compact, and let $\mathcal{U}$ be an open cover of X. Since X is also lindelöf, $\mathcal{U}$ has a countable subcover $\{U_i\}$. Assume no finite subcollection of U_i's covers X. Then for each i there exists $x_i \in X$ such that $x_i \notin U_1 \cup \cdots \cup U_i$. By hypothesis, the sequence x_i has a convergent subsequence $x_{n_i} \to x$. Now, $x \in U_m$ for some m because the U_i's cover X, and then convergence of the subsequence means that $x_{n_k} \in U_m$ for all but finitely many values of k. But by construction, $x_{n_k} \notin U_m$ as soon as $n_k \geq m$, which is a contradiction. This proves that second countable sequentially compact spaces are compact.

Second, let M be a sequentially compact metric space. We show that given $\varepsilon > 0$, there exists a finite covering of X by open ε-balls. Assume that there exists an $\varepsilon > 0$ such that X cannot be covered by finitely many ε-balls. Construct a sequence of points x_n of X as follows: First, choose x_1 to be any point of X. Noting that the ball $B_\varepsilon(x_1)$ is not all of X (otherwise X could be covered by a single ε-ball), choose x_2 to be a point of X not in $B_\varepsilon(x_)$. In general, given $x_1, \ldots, x_n$, choose x_{n+1} to be a point not in the union

$$B_\varepsilon(x_1) \cup \cdots \cup B_\varepsilon(x_n)$$

using the fact that these balls do not cover X. Note that by construction $d(x_{n+1}, x_i) \geq \varepsilon$ for $1 \leq i \leq n$. Therefore, the sequence (x_n) can have no convergent subsequence; in fact, any ball of radius $\varepsilon/2$ can contain x_n for at most one value of n.

Let $\mathcal{A}$ be an open covering of X. Because X is sequentially compact, the open covering $\mathcal{A}$ has a Lebesgue number δ. Let $\varepsilon = \delta/3$; use sequentially compactness of X to find a finite covering of X by open ε-balls. Each of these balls has diameter at most $2\delta/3$, so it lies in an element of $\mathcal{U}$. Choosing one such element of $\mathcal{U}$ for each of these ε-balls, we obtain a finite subcollection of $\mathcal{U}$ that covers X. □

Combining the results above, we have the following theorem.

Theorem 1.8.18. *Let X be a metrizable space. Then the following are equivalent:*

(i) X is compact.

(ii) X is limit point compact.

(iii) X is sequentially compact.

Example 1.8.19. Recall that $\bar{S}_\Omega$ denotes the first uncountable ordinal S_Ω with the point Ω adjoined. It is easy to see that the space $\bar{S}_\Omega$ is not metrizable, for it does not satisfy the sequence lemma: The point Ω is a limit point of S_Ω, but it is not the limit of a sequence of points of S_Ω, for any sequence of points of S_Ω has an upper bound in S_Ω. The space S_Ω, on the other hand, does satisfy the sequence lemma. Nevertheless, S_Ω is not metrizable, for it is limit point compact but not compact.

1.8.2 General characterization of compactness

We now show that a version of the Balzano-Weierstrass property holds for compact topological spaces. As one might suspect, it is merely necessary to replace sequences by nets.

Theorem 1.8.20. *If X is a topological space, the following are equivalent:*

(a) X is compact.

(b) Every net in X has a cluster point .

(c) Every net in X has a convergent subnet.

Proof. The equivalence of (b) and (c) follows from Proposition 1.7.5. If X is compact and (x_α) is a net in X, let $E_\alpha = \{x_\beta : \beta \succeq \alpha\}$. Since for any $\alpha, \beta \in A$ there exists $\gamma \in A$ with $\alpha \preceq \gamma$ and $\beta \preceq \gamma$, the family $\{E_\alpha\}_{\alpha \in A}$ has the finite intersection property. If (x_α) has no cluster point , then E_α is closed for each α, so by compactness, $\bigcap_{\alpha \in A} E_\alpha \neq \varnothing$. If $x \in \bigcap_\alpha E_\alpha$, and U is a neighborhood of x, then U intersects each E_α, which means that (x_α) is frequently in U, so x is a cluster point of (x_α). This is a contradiction.

On the other hand, if X is not compact, let $\{U_\beta\}_{\beta \in B}$ be an open cover of X with no finite subcover. Let $\mathcal{A}$ be the collection of finite subsets of B, directed by inclusion, and for each $A \in \mathcal{A}$ let x_A be a point in $(\bigcup_{\beta \in A} U_\beta)^c$. Then $(x_A)_{A \in \mathcal{A}}$ is a net with no cluster point . Indeed, if $x \in X$, choose $\beta \in B$ with $x \in U_\beta$. If $A \in \mathcal{A}$ and $A \succeq \{\beta\}$, then $x_A \notin U_\beta$, so (x_α) is not frequently in U_β, and thus x is not a cluster point of (x_A). □

Using the above characterization of compactness, we prove the following important theorem about compactness of product spaces. To prepare for it, we introduce some notation. Recall that an element x of $X = \prod_{\alpha \in A} X_\alpha$ is, strictly speaking, a mapping from A into $\bigcup_{\alpha \in A} X_\alpha$; namely, $x(\alpha) \in X_\alpha$ is the α-th coordinate of x, which we generally denote by $\pi_\alpha(x)$. If $B \subseteq A$, there is a natural map $\pi_B : X \to \prod_{\alpha \in B} X_\alpha$; namely, $\pi_B(x)$ is the restriction of the map x to B. (In particular, $\pi_{\{\alpha\}}$ is essentially identical to π_α, and we shall not distinguish between them.) If $p \in \prod_{\alpha \in B} X_\alpha$ and $q \in \prod_{\alpha \in B} X_\alpha$, we shall say that q is an **extension** of p if q extends p as a mapping, that is, if $B \subseteq C$ and $p(\alpha) = q(\alpha)$ for $\alpha \in B$.

Theorem 1.8.21 (Tychonoff's Theorem). *If $\{X_\alpha\}_{\alpha \in A}$ is any family of compact topological spaces, the $\prod_{\alpha \in A} X_\alpha$ is compact with the product topology.*

Proof. By Theorem 1.8.20, it is enough to show that any net $(x_i)_{i \in I}$ in X has a cluster point. We shall do this by examining cluster points of the nets $(\pi_B(x_i))$ in the subproducts of X. To wit, let

$$\mathcal{P} = \bigcup_{B \subseteq A} \{p \in \prod_{\alpha \in B} X_\alpha : p \text{ is a cluster point of the net } (\pi_B(x_i))\}.$$

It is clear that $\mathcal{P}$ is nonempty, because each X_α is compact and so $(\pi_B(x_i))$ has cluster points when $B = \{\alpha\}$. Moreover, $\mathcal{P}$ is partially ordered by extension; that is, $p \leq q$ if q is an extension of p as defined above.

Suppose that $\{p_\lambda : \lambda \in \Lambda\}$ is a linearly ordered subset of $\mathcal{P}$, where $p_\lambda \in \prod_{\alpha \in B_\lambda} X_\alpha$. Let $\widetilde{B} = \bigcup_\lambda B_\lambda$ and $\widetilde{p}$ be the unique element of $\prod_{\alpha \in \widetilde{B}} X_\alpha$ that extends every p_λ. We claim that $\widetilde{p} \in \mathcal{P}$. Indeed, from the definition of the product topology, any neighborhood of $\widetilde{p}$ contains a set of the form $\prod_{\alpha \in \widetilde{B}} U_\alpha$, where each U_α is open in X_α and $U_\alpha = X_\alpha$ for all but finitely many

α, say $\alpha_1, \ldots, \alpha_n$. Each of these α_j's belongs to some B_λ, so by linearity of the ordering they all belong to a single B_λ. But then $\prod_{\alpha \in B_\lambda} U_\alpha$ is a neighborhood of p_λ, so $(\pi_{B_\lambda}(x_i))$ is frequently in $\prod_{\alpha \in B_\lambda} U_\alpha$; hence $(\pi_{\widetilde{B}}(x_i))$ is frequently in $\prod_{\alpha \in \widetilde{B}} U_\alpha$, and $\widetilde{p}$ is a cluster point of $(\pi_{\widetilde{B}}(x_i))$. This implies $\{p_\lambda\}$ has a upper bound $\widetilde{p}$ in $\mathcal{P}$.

By Zorn's lemma, then, $\mathcal{P}$ has a maximal element $p_0 \in \prod_{\alpha \in B_0} X_\alpha$. We claim that $B_0 = A$. If not, pick $\gamma \in A \backslash B_0$. By Proposition 1.7.5 there is a subnet $(\pi_{B_0}(x_{i_j}))_{j \in J}$ of $(\pi_{B_0}(x_i))$ that converges to p_0, and since X_γ is compact, there is a subnet $(\pi_\gamma(x_{i_{j(k)}}))_{k \in K}$ of $(\pi_{B_0}(x_{i_j}))$ that converges to some $p_\gamma \in X_\gamma$. Let q be the unique element of $\prod_{\alpha \in B_0 \cup \{\gamma\}} X_\alpha$ that extends both p_0 and p_γ, then the net $(\pi_{B_0 \cup \{\gamma\}}(x_{i_{j(k)}}))_{k \in K}$ converges to q and hence q is a cluster point of $(\pi_{B_0 \cup \{\gamma\}}(x_i))$, contradicting the maximality of p_0. Therefore p_0 is a cluster point of (x_i), and we are done. □

For interest, we give a proof about the equivalence of Tychonoff's theorem and the axiom of choice. We already know that the latter is equivalent to Zorn's lemma, so we only need to use Tychonoff's theorem to deduce the axiom of choice.

Proposition 1.8.22. *Tychonoff's theorem implies the axiom of choice.*

Proof. Suppose that $\{X_\alpha\}_{\alpha \in A}$ is a nonempty collection of nonempty sets. Pick a point ω that is not an element of any X_α, define $X_\alpha^* = X_\alpha \cup \{\omega\}$, and define a topology on X_α^* by declaring the open sets to be $\varnothing, X_\alpha, \{\omega\}$, and X_α^*. Evidently each X_α^* is compact, so Tychonoff's theorem implies that $X^* = \prod_{\alpha \in A} X_\alpha^*$ is compact. Let $F_\alpha = \pi_\alpha^{-1}(X_\alpha)$. The sets F_α are closed (X_α is closed and π_α is continuous), and by the axiom of choice for finite collections of sets which is provable from the other standard axioms of set theory, they have the finite intersection property. Indeed, given a finite set $B \subseteq A$, pick $x_\beta \in X_\beta$ for $\beta \in B$; then $\bigcap_{\beta \in B} F_\beta$ contains the point $x \in X$ such that $\pi_\beta(x) = x_\beta$ for $\beta \in B$ and $\pi_\alpha(x) = \omega$ for $\alpha \notin B$. By the compatness, $\bigcap_{\alpha \in A} F_\alpha$, which is precisely $\prod_{\alpha \in A} X_\alpha$, is nonempty. □

1.8.3 Inverse limit of compact spaces

Proposition 1.8.23. *Let $(X_\alpha, f_{\alpha\beta})$ be an inverse system of compact Hausdorff spaces indexed by a directed set I such that $f_{\alpha\alpha}$ is the identity mapping for each $\alpha \in I$. Let $X = \varprojlim X_\alpha$ be the inverse limit and $f_\alpha : X \to X_\alpha$ the canonical mapping. Then*

(a) X is compact Huasdorff and for each $\alpha \in I$ we have

$$f_\alpha(X) = \bigcap_{\beta \geq \alpha} f_{\alpha\beta}(X_\beta). \tag{8.3.1}$$

(b) If the X_α are all non-empty then X is non-empty.

Proof. The sapce X is a closed subspace of $\prod_\alpha X_\alpha$, which is compact and Hausdorff. For $\beta \geq \alpha$ we define

$$L_\beta = \{y \in \prod X_\gamma : f_{\gamma\beta}(y_\beta) = y_\gamma \text{ for } \gamma \preceq \beta\}.$$

Since each component of $\prod X_\gamma$ is Hausdorff, we can see that each L_β is closed in the product space by showing that every point in the complement is an interior point by using the continuity of the $f_{\alpha\beta}$'s. Thus each L_β is compact. Furthermore, by construction, we have $\bigcap_{\beta \in I} L_\beta \subseteq X$. Thus we only need to show $\bigcap_\beta L_\beta \neq \varnothing$, and this follows from the observation that any finite

intersection of the L_β's is nonempty. This proves (b) and the first part of (a). Now, for $x_\alpha \in X_\alpha$, if we set

$$L_\beta(x_\alpha) = \{y \in \prod X_\gamma : \pi_\alpha(y) = x_\alpha \text{ and } f_{\gamma\beta}(y_\beta) = y_\gamma \text{ for } \gamma \preceq \beta\}$$

then we have

$$f_\alpha(X) = \{x_\alpha \in X_\alpha : \bigcap_{\beta \preceq \alpha} L_\beta(x_\alpha) \neq \varnothing\}$$

whence $f_\alpha(X) \subseteq \bigcap_{\beta \succeq \alpha} f_{\alpha\beta}(X_\beta)$. Conversely, if $x_\alpha \in \bigcap_{\beta \succeq \alpha} f_{\alpha\beta}(X_\beta)$ then $L_\beta(x_\alpha) \neq \varnothing$ for all $\beta \succeq \alpha$, whence $\bigcap L_\beta(x_\alpha) \neq \varnothing$ by compactness. This finishes the proof. □

Corollary 1.8.24. *Let $(X_\alpha, f_{\alpha\beta})$ be an inverse system of topological spaces indexed by a directed set, such that for each pair of indices α, β for which $\alpha \preceq \beta$ and for each $x_\alpha \in X_\alpha$, $f_{\alpha\beta}^{-1}(x_\alpha)$ is compact. Then equation (8.3.1) is valid and $f_\alpha^{-1}(x_\alpha)$ is compact for each index α and each $x_\alpha \in X_\alpha$.*

Proof. For each $x_\alpha \in \bigcap_{\beta \succeq \alpha} f_{\alpha\beta}(X_\beta)$ and each $\alpha \in I$, let L_β denote $f_{\alpha\beta}^{-1}(x_\alpha)$. If $\alpha \preceq \beta \preceq \gamma$ then we have $f_{\beta\gamma}(L_\gamma) \subseteq L_\beta$ and the set of all indices $\beta \preceq \alpha$ is cofinal in the index set. It follows immediately that the $(L_\beta, f_{\beta\gamma})$ form an inverse system of topological spaces whose inverse limit L is homeomorphic to $f_\alpha^{-1}(x_\alpha)$. Since by hypothesis the L_β are compact and not empty, the corollary follows from Proposition 1.8.23. □

Corollary 1.8.25. *Let $(X_\alpha, f_{\alpha\beta})$ and $(Y_\alpha, g_{\alpha\beta})$ be two inverse systems of topological spaces indexed by the same directed set I, and let (u_α) be an inverse system of mappings $u_\alpha : X_\alpha \to Y_\alpha$. Let $X = \varprojlim X_\alpha$, $Y = \varprojlim Y_\alpha$ and $u = \varprojlim u_\alpha$. Then:*

(a) If $y = (y_\alpha) \in Y$ is such that $u_\alpha^{-1}(y_\alpha)$ is compact and non-empty for each $\alpha \in I$, then $u^{-1}(y)$ is compact and non-empty.

(b) If the X_α are compact Hausdorff, the Y_α are Hausdorff and the u_α surjective and continuous, then u is surjective.

Proof. Let L_α denote $u^{-1}(y_\alpha)$; then clearly the L_α form an inverse system of topological spaces and $L = u^{-1}(y)$ is the inverse limit of the L_α. Assertion (a) therefore follows from Proposition 1.8.23 and (b) is an immediate consequence of (a). □

1.8.4 Aezelá-Ascoli theorem

We now turn to the Arzelá-Ascoli theorem, which has to do with compactness in spaces of continuous mappings. There are several variants of this result; the theorems below are two of the most useful ones.

If X is a topological space and $\mathscr{F} \subseteq \mathbb{K}^X$ is a subset, $\mathscr{F}$ is called **equicontinuous at $x \in X$** if for every $\varepsilon > 0$ there is a neighborhood U of x such that $|f(y) - f(x)| < \varepsilon$ for all $y \in U$ and all $f \in \mathscr{F}$; $\mathscr{F}$ is called **equicontinuous** if it is equicontinuous at each $x \in X$. Also, $\mathscr{F}$ is said to be **pointwise bounded** if $\mathscr{F}(x) = \{f(x) : f \in \mathscr{F}\}$ is bounded for each $x \in X$.

Lemma 1.8.26. *Let X be a topological space. The same topology is induced on equicontinuous subsets $\mathscr{F}$ of $C(X)$ by the point-open topology $\mathcal{T}_p$ and the compact-open topology $\mathcal{T}_c$.*

Proof. Let $\mathscr{F} \subseteq C(X)$ be equicontinuous. Generally, $\mathcal{T}_p \subseteq \mathcal{T}_c$, so we need only show that $\mathcal{T}_c \cap \mathscr{F} \subseteq \mathcal{T}_p \cap \mathscr{F}$. To this end, let $f_0 \in \mathscr{F}$. A $\mathcal{T}_c \cap \mathscr{F}$-subbasic neighborhood of x_0 is of the form

$$U_c = \{f \in \mathscr{F} : \|f - f_0\|_K < r\}$$

where $r > 0$ and K is a compact subset of X. We now find $r' > 0$ and $x_1, \dots, x_n \in X$ such that the $\mathcal{T}_p \cap \mathscr{F}$-neighborhood

$$U_p = \{f \in \mathscr{F} : \|f - f_0\|_{\{x_1,\dots,x_n\}} < r'\} \subseteq U_c.$$

To this end, let K and $r > 0$ be given. Since $\mathscr{F}$ is equicontinuous, there exist neighborhoods V_x of x for each $x \in X$ such that $|f(x)-f(y)| < r/4$ for each $y \in V_x$ and each $f \in \mathscr{F}$. A finite number $V_{x_1}, \dots, V_{x_n}$ cover the compact set K. Now consider $f \in \mathscr{F}$ such that $\|f - f_0\|_{\{x_1,\dots,x_n\}} < r/2$. For $x \in K$, there is an i such that $x \in V_{x_i}$. Thus

$$|f(x) - f_0(x)| \leq |f(x) - f(x_i)| + |f(x_i) - f_0(x_i)| + |f_0(x_i) - f_0(x)| < r/4 + r/2 + r/4 = r.$$

Since $x \in K$ is arbitrary, it follows that $f \in U_c$. □

Lemma 1.8.27. *Let X be a topological space and $\mathscr{F}$ be an equicontinuous subset of $\mathbb{K}^X$. Then the pointwise closure $\mathrm{cl}_p\mathscr{F}$ of $\mathscr{F}$ in $\mathbb{K}^X$ is an equicontinuous subset of $C(X)$.*

Proof. Let $\mathscr{F} \subseteq \mathbb{K}^X$ be equicontinuous. Given $r > 0$ and $x \in X$, there is an eighborhood V of x such that

$$|f(x) - f(y)| < r \tag{8.4.1}$$

for $y \in V$ and $f \in \mathscr{F}$. We show that (8.4.1) holds for each $g \in \mathrm{cl}_p\mathscr{F}$ as well. To this end let $g \in \mathrm{cl}_p\mathscr{F}$ and let $y \in V$. Since $g \in \mathrm{cl}_p\mathscr{F}$, given $r' > 0$, there is an $f \in \mathscr{F}$ such that $\|f - g\|_{\{x,y\}} < r'$. Hence

$$|g(x) - g(y)| \leq |g(x) - f(x)| + |f(x) - f(y)| + |f(y) - g(y)| < r' + r + r'.$$

It follows that $\mathrm{cl}_p\mathscr{F}$ is equicontinuous as well. □

As an immediate consequence of Lemmas 1.8.26 and 1.8.27, the $\mathcal{T}_c$-closure of an equicontinuous subset of $\mathbb{K}^X$ is equicontinuous in $C(X, \mathbb{K}, c)$. In our next result we obtain some results connecting pointwise boundedness of equicontinuous sets and compactness.

Theorem 1.8.28 (Arzelá-Ascoli). *Let X be a topological space. If $\mathscr{F}$ is an equicontinuous subset of $C(X, \mathbb{K}, c)$ and is pointwise bounded, then $\mathscr{F}$ is precompact in $C(X, \mathbb{K}, c)$. Conversely, if X is locally compact and $\mathscr{F}$ is precompact in $C(X, \mathbb{K}, c)$ then $\mathscr{F}$ is equicontinuous and pointwise bounded.*

Proof. Suppose first that $\mathscr{F}$ is equicontinuous and pointwise bounded. As such, eaeh $\mathscr{F}(x)$ is precompact by the Heine-Borel theorem. Let $\mathrm{cl}_p\mathscr{F}$ and $\mathrm{cl}_c\mathscr{F}$ denote the $\mathcal{T}_p$- and $\mathcal{T}_c$-closures of $\mathscr{F}$ in $C(X)$, respectively. By Lemma 1.8.27, the pointwise closure $\mathrm{cl}_p\mathscr{F}$ of $\mathscr{F}$ computed in $\mathbb{K}^X$ is an equicontinuous subset of $C(X)$. Consider the homeomorphism

$$\iota : C(X, \mathbb{K}, p) \to \mathbb{K}^X, \quad f \mapsto (f(x))_{x \in X}.$$

To see that $\mathrm{cl}_p\iota(\mathscr{F})$ is compact in $\mathbb{K}^X$, note

$$\mathrm{cl}_p\iota(\mathscr{F}) = \iota(\mathrm{cl}_p\mathscr{F}) = \{(f(x))_{x\in X} : f \in \mathrm{cl}_p\mathscr{F}\} = \prod_{x\in X}(\mathrm{cl}_p\mathscr{F})(x) \subseteq \prod_{x\in X}\mathrm{cl}_{\mathbb{K}}\mathscr{F}(x).$$

It follows from Tychonoff theorem that $\mathrm{cl}_p\iota(\mathscr{F})$ is compact and therefore $\mathrm{cl}_p\mathscr{F}$ is $\mathcal{T}_p$-compact. Since $\mathscr{F}$ is equicontinuous, $\mathrm{cl}_p\mathscr{F} = \mathrm{cl}_c\mathscr{F}$ by Lemma 1.8.26 and $\mathrm{cl}_c\mathscr{F}$ is $\mathcal{T}_c$-compact.

Conversely, suppose that X is locally compact and that $\mathscr{F} \subseteq C(X, \mathbb{K}, c)$ is relatively compact. For any $x \in X$, it is easy to see the evaluation map δ_x is continuous on $C(X, \mathbb{K}, c)$, hence each $\delta_x(\mathrm{cl}_p\mathscr{F})$ is compact. It follows that $\delta_x(\mathscr{F})$ is precompact—hence bounded—for any $x \in X$.

To show equicontinuity of $\mathscr{F}$, consider $x \in X$ and $r > 0$. Since X is locally compact, we may choose a compact neighborhood K of x. Let $B_{p_K} = \{f \in C(X, \mathbb{K}, c) : \|f\|_K < 1\}$. Since $\mathscr{F}$ is relatively $\mathcal{T}_c$-compact, there exists $n \in \mathbb{N}$ and $f_i \in \mathrm{cl}_c\mathscr{F}$ with $i = 1, \dots, n$ such that $\{f_i + (r/3)B_{p_K}\}$ cover $\mathscr{F}$. Thus for each $y \in K$ and $f \in \mathscr{F}$, there is some f_i such that $|f(y) - f_i(y)| < r/3$. Since each f_i is continuous, there exist neighborhoods V_i of x such that

$$|f_i(x) - f_i(y)| < r/3 \quad \text{for} \quad y \in V_i.$$

Now for any $f \in \mathscr{F}$, any $y \in K \cap V_1 \cap \cdots \cap V_n$, we have, for some i whose choice depends on f,

$$|f(x) - f(y)| \le |f(x) - f_i(x)| + |f_i(x) - f_i(y)| + |f_i(y) - f(y)| < r.$$

Hence the equicontinuity of $\mathscr{F}$ is established. □

Theorem 1.8.29 (Arzelá-Ascoli). *Let X be a compact Hausdorff space and endow $C(X)$ with the uniform topology. Then a subspace $\mathscr{F}$ in $C(X)$ is totally bounded if and only if $\mathscr{F}$ is equicontinuous and pointwise bounded.*

Proof. If X is compact Hausdorff then $\mathcal{T}_c = \mathcal{T}_u$ and they can be metrized by the supremum norm. Moreover, $C(X, \|\cdot\|_\infty)$ is complete. Since totally boundedness is equivalent to precompactness in complete metric spaces. The claim follows. □

Corollary 1.8.30. *Let X be a compact Hausdorff space and endow $C(X)$ with the uniform topology. Then a subspace $\mathscr{F}$ in $C(X)$ is compact if and only if it is closed, pointwise bounded and equicontinuous.*

Proposition 1.8.31. *Let X be a σ-compact locally compact Hausdorff space. If $\{f_n\}$ is an equicontinuous, pointwise bounded sequence in $C(X)$, there exist $f \in C(X)$ and a subsequence of $\{f_n\}$ that converges to f uniformly on compact sets.*

Proof. Let $\{K_j\}$ be a exhaustion of X by compact sets (Proposition 1.13.5). By Theorem 1.8.29, applied to $C(K_1)$, there is a subsequence $\{f_i^1\}$ of $\{f_n\}$ that is uniformly Cauchy on K_1. Proceeding inductively, for $j \in \mathbb{N}$ we obtain a subsequence $\{f_i^j\}_{i=1}^\infty$ of $\{f_i^{j-1}\}_{i=1}^\infty$ that is uniformly Cauchy on K_j. Let $g_i = f_i^i$; then $\{g_i\}$ is a subsequence of $\{f_n\}$ which is (except for the first $j-1$ terms) a subsequence of $\{f_i^j\}$ and hence is uniformly Cauchy on each K_j. Let $f = \lim g_i$. Then $f \in C(X)$ and $g_i \to f$ uniformly on compact sets by Propositions 1.9.7 and 1.9.8. □

1.8.5 Compactification

A **compactification** of a topological space X is a pair (Y, ι) where Y is a compact Hausdorff space and ι is a homeomorphism from X onto a dense subset of Y. Since Hausdorff compact spaces satisfy many properties which are hereditary, compactification is not available for all topological spaces. In this part, we consider completely regular spaces and show that their compactifications correspond to subalgebras of the continuous functions.

Let X be a topological space and $BC(X)$ be the space of bounded continuous functions on X. Without further referring, we endow $BC(X)$ with the supremum norm, which makes it a Banach space. Recall that a subalgebra $\mathcal{F}$ of $C(X, I)$ is said to **separate points and closed sets** if for every closed $E \subseteq X$ and every $x \in E^c$ there exists $f \in \mathcal{F}$ such that $f(x) = 0$ and $f(E) = \{1\}$. It follows that a T_1 space X admits a family $\mathcal{F}$ that separates points and closed sets iff X is completely regular.

Let X be a completely regular space. A subalgebra $\mathcal{A}$ of $BC(X)$ is called **completely regular** if

(a) it is closed in $BC(X)$ and contains constant functions;

(b) $\mathcal{A} \cap C(X, I)$ separates points and closed sets.

Due to the remark above, completely regular subalgebra always exists in $BC(X)$. An important example is provided by the following proposition.

Proposition 1.8.32. *Let (Y, ι) be a compactification of X, then $\mathcal{A}_Y = \{f \circ \iota : f \in C(Y)\}$ is a completely regular subalgebra of $BC(X)$.*

Proof. Clearly $\mathcal{A}_Y$ contains constant functions, and it is easy to see $\mathcal{A}_Y \cap C(X, [0, 1])$ saparates points and closed sets of X, since Y is completely regular. Now let f_α be a net in $C(Y)$ such that $f_\alpha \circ \iota \to f$ in $BC(X)$ for some $f \in BC(X)$. We now prove that f_α is Cauchy in $C(Y)$, so that it has a limit $\tilde{f} \in C(Y)$. With this, we immediate see $\tilde{f} \circ \iota = f$, so the proposition is proved.

Now, by definition, for any fixed $\varepsilon > 0$ there exists an index γ such that

$$|f_\alpha(\iota(x)) - f_\beta(\iota(x))| < \varepsilon/3, \quad \forall x \in X, \forall \alpha, \beta \preceq \gamma.$$

Now fix $\alpha, \beta \preceq \gamma$. Since $\iota(X)$ is dense in Y and f_α, f_β are continuous, for any $y \in Y$ there exists $x_0 \in X$ such that

$$|f_\alpha(\iota(x)) - f_\alpha(y)| < \varepsilon/3, \quad |f_\beta(\iota(x)) - f_\beta(y)| < \varepsilon/3,$$

whence

$$|f_\alpha(y) - f_\beta(y)| \leq |f_\alpha(y) - f_\alpha(\iota(x))| + |f_\alpha(\iota(x)) - f_\beta(\iota(x))| + |f_\beta(\iota(x)) - f_\beta(y)| < \varepsilon.$$

Since this is true for all $y \in Y$, we see (f_α) is Cauchy so the claim follows. □

Note that for a compact Hausdorff Y, Y can be embedded into the dual space $C(Y)^*$ (with the weak* topology) by the evaluation map δ defined by

$$\delta : Y \to C(Y)^*, \quad y \mapsto \delta_y.$$

With this observation, we now consider two compactifications (Y_1, ι_1) and (Y_2, ι_2) of X. Via the map δ, the spaces Y_1 and Y_2 can be embedded into $C(Y_1)^*$ and $C(Y_2)^*$, respectively. One may wonder in what condition does there exist a continuous map from (Y_1, ι_1) to (Y_2, ι_2). Instead of thinking Y_1 and Y_2, let's try to define a map Ψ from $C(Y_1)^*$ to $C(Y_2)^*$. Let $p \in C(Y_1)^*$, we then need to determine how it acts on a function $g \in C(Y_2)$. For this, consider the restriction $g \circ \iota_2 \in \mathcal{A}_{Y_2}$. If we have $g \circ \iota_2 \in \mathcal{A}_1$, then there will be a unique function $\tilde{g} \in C(Y_1)$ such that $\tilde{g} \circ \iota_1 = g \circ \iota_2$, and we can then define

$$p(g) := p(\tilde{g}).$$

In this way, we see if $\mathcal{A}_{Y_2} \subseteq \mathcal{A}_{Y_1}$ then there is a map $\Psi : C(Y_1)^* \to C(Y_2)^*$. A crucial fact is that the map Ψ is continuous with respect to the weak* topology and this construction is functorial.

Proposition 1.8.33. *Let (Y_1, ι_1), (Y_2, ι_2), (Y_3, ι_3) be compactifications of X.*

(a) If $\mathcal{A}_{Y_2} \subseteq \mathcal{A}_{Y_1}$ then there is a continuous map $\Psi : C(Y_1)^* \to C(Y_2)^*$ which restricts to a continuous map $\psi : Y_1 \to Y_2$ such that the following diagram commutes:

$$\begin{tikzcd}
X \arrow[r, "\iota_1"] \arrow[d, equal] & Y_1 \arrow[r, hook, "\delta"] \arrow[d, "\psi"] & C(Y_1)^* \arrow[d, "\Psi"] \\
X \arrow[r, "\iota_2"] & Y_2 \arrow[r, hook, "\delta"] & C(Y_2)^*
\end{tikzcd}$$

If $\Psi' : C(Y_1)^* \to C(Y_2)^*$ is another map with this property, then $\Psi'|_{Y_1} = \psi$.

(b) If $\mathcal{A}_{Y_3} \subseteq \mathcal{A}_{Y_2} \subseteq \mathcal{A}_{Y_1}$ then the following diagram commutes:

$$\begin{tikzcd}
X \arrow[r, "\iota_1"] \arrow[d, equal] & Y_1 \arrow[r, hook, "\delta"] \arrow[d, "\psi"] & C(Y_1)^* \arrow[d, "\Psi"] \\
X \arrow[r, "\iota_2"] \arrow[d, equal] & Y_2 \arrow[r, hook, "\delta"] \arrow[d, "\phi"] & C(Y_2)^* \arrow[d, "\Phi"] \\
X \arrow[r, "\iota_3"] & Y_3 \arrow[r, hook, "\delta"] & C(Y_3)^*
\end{tikzcd}$$

where Ψ and Φ are the maps in (a).

Proof. Let p_α be a net in $C(Y_1)^*$ which converges weakly to $p \in C(Y_1)^*$. Then for any $g \in C(Y_2)$, we see

$$\Psi(p_\alpha)(g) = p_\alpha(\tilde{g}) \to p(\tilde{g}) = \Psi(p)(g),$$

which shows $\Psi(p_\alpha) \to \Psi(p)$ weakly, so Ψ is continuous. Moreover, let $x \in X$, then

$$\Psi(\delta_{\iota_1(x)})(g) = \tilde{g}(\iota_1(x)) = g(\iota_2(x)) = \delta_{\iota_2(x)}(g).$$

Therefore $\Psi \circ \delta \circ \iota_1 = \delta \circ \iota_2$. In particular, since $\iota_1(X)$ is dense in Y_1, we have

$$\Psi(\delta(Y_1)) = \Psi(\overline{\delta(\iota_1(X))}) \subseteq \overline{\delta(\iota_2(X))} = \delta(Y_2),$$

so Ψ restricts to a map $\psi : Y_1 \to Y_2$, which is continuous since δ is an embedding for both Y_1 and Y_2. Finally, if Ψ' is another map making the diagram commutes, then it must coincide with

Ψ on $\delta(\iota_1(X))$, hence we have $\Psi'|_{Y_1} = \psi$. This completes the proof of (a), and the validity of (b) follows from the definition of Φ and Ψ. □

Corollary 1.8.34. *Let (Y_1, ι_1) and (Y_2, ι_2) be compactifications of X with $\mathcal{A}_{Y_1} = \mathcal{A}_{Y_2}$. Then the map $\Psi : C(Y_1)^* \to C(Y_2)^*$ induces a homeomorphism of (Y_1, ι_1) and (Y_2, ι_2).*

Now we consider the converse process. With full generality, each nonempty subset $\mathcal{F} \subseteq C(X, I)$ canonically induces a map $\iota : X \to I^{\mathcal{F}}$ by the formula $\iota(x) = (f(x))_{f \in \mathcal{F}}$. We call ι the map from X into the cube $I^{\mathcal{F}}$ **associated to** $\mathcal{F}$.

Proposition 1.8.35. *Let X be a topological space, $\mathcal{F} \subseteq C(X, I)$, and $\iota : X \to I^{\mathcal{F}}$ be the map associated to $\mathcal{F}$. Then*

(a) The map ι is continuous.

(b) If $\mathcal{F}$ separates points, then ι is injective.

(c) If X is T_1 and $\mathcal{F}$ separates points and closed sets, then ι is an embedding.

Proof. Part (a) and (b) are obvious. Next, observe that if $\mathcal{F}$ separates points and closed sets and X is T_1, then ι is injective. To prove the continuity of the inverse, suppose that U is open in X. If $x \in U$, choose $f \in \mathcal{F}$ with $f(x) = 0$ and $f(U^c) = \{1\}$, and let $V = \pi_f^{-1}([0, 1))$. Then V is open in $I^{\mathcal{F}}$ and $\iota(x) \in V \cap \iota(X) \subseteq \iota(U)$. Thus $\iota(U)$ is a neighborhood of $\iota(x)$ in $\iota(X)$, so $\iota(U)$ is open in $\iota(X)$. It follows that ι^{-1} is continuous. □

Corollary 1.8.36. *Every compact Hausdorff space is homeomorphic to a closed subset of a cube.*

Now let $\mathcal{A}$ be a completely regular subalgebra of $BC(X)$ and let $\mathcal{F} = \mathcal{A} \cap C(X, I)$. Then by Proposition 1.8.35, we have a compactification (Y, ι) associated with $\mathcal{F}$. We now consider the relation between $\mathcal{A}$ and $\mathcal{A}_Y$.

Proposition 1.8.37. *Suppose that $\mathcal{F} \subseteq C(X, I)$ separates points and closed sets. Let (Y, ι) be the compactification of X associated to $\mathcal{F}$. Then $\mathcal{A}_Y$ is the smallest closed subalgebra of $BC(X)$ that contains $\mathcal{F}$ and constant functions.*

Proof. Let $\mathcal{A}$ be the smallest closed subalgebra of $BC(X)$ that contains $\mathcal{F}$. Let $f \in \mathcal{F}$, then f can be extended to Y by

$$f(p) := \pi_f(p), \quad \forall p \in I^{\mathcal{F}},$$

If $p_\alpha \to p$ in $I^{\mathcal{F}}$, then we have $f(p_\alpha) = \pi_f(p_\alpha) \to \pi_f(p) = f(p)$, therefore this extension is continuous. This shows $\mathcal{F} \subseteq \mathcal{A}_Y$, and therefore $\mathcal{F} \subseteq \mathcal{A} \subseteq \mathcal{A}_Y$.

Let π_f be the coordinate map on $I^{\mathcal{F}}$, then by Stone-Weierstrass theorem, the algebra generated by the coordinate projections $\{\pi_f : f \in \mathcal{F}\}$ and the constant functions is dense in $C(I^{\mathcal{F}})$. Moreover, $\pi_f \circ \iota = f$ for each $f \in \mathcal{F}$. Since $\mathcal{A}$ is closed and contains constant functions, it follows that $\mathcal{A} \supseteq \mathcal{A}_Y$, so the claim follows. □

Theorem 1.8.38. *Let X be a completely regular space. The compactifications of X are in one-to-one correspondence with the completely regular subalgebras of $BC(X)$.*

Proof. If $\mathcal{A}$ is a completely regular subalgebra, we denote by $(Y_{\mathcal{A}}, \iota)$ the compactification of X associated with $\mathcal{F} := \mathcal{A} \cap C(X, I)$. By the definition of completely regularity and Proposition 1.8.37, We have $\mathcal{A}_{Y_{\mathcal{A}}} = \mathcal{A}$.

Conversely, for each compactification (Y, ι), we consider the map $(Y, \iota) \mapsto \mathcal{A}_Y$. We have already seen that $\mathcal{A}_Y$ is completely regular. Moreover, if $Y_{\mathcal{A}_Y}$ is the compactification associated with $\mathcal{A}_Y$, then we have $\mathcal{A}_{Y_{\mathcal{A}_Y}} = \mathcal{A}_Y$ by Proposition 1.8.37, which implies Y are homeomorphic to $Y_{\mathcal{A}_Y}$, by Corollary 1.8.34. These together prove the theorem. □

1.9 Local compactness

A topological space X is said to be **locally compact** if for every $p \in X$ there is a compact subset of X containing a neighborhood of p. In this generality, the definition is not particularly useful, and does not seem parallel to other definitions of what it means for a topological space to possess a property "locally", which usually entails the existence of a base of open subsets with a particular property. But when combined with the Hausdorff property, local compactness is much more useful. A subset A of a topological space X is said to be **precompact** (or sometimes **relatively compact**) in X if $\overline{A}$ is compact.

Proposition 1.9.1. *Let X be a Hausdorff space. The following are equivalent.*

(a) X is locally compact.

(b) Each point of X has a precompact neighborhood.

(c) X has a base of precompact open subsets.

Proof. Clearly $(c) \Rightarrow (b) \Rightarrow (a)$, so all we have to prove is $(a) \Rightarrow (c)$. It suffices to show that if X is a locally compact Hausdorff space, then each point $x \in X$ has a neighborhood base of precompact open subsets. Let $K \subseteq X$ be a compact set containing a neighborhood U of x. The collection $\mathcal{V}$ of all neighborhoods of x contained in U is clearly a neighborhood base at x.

Because X is Hausdorff, K is closed in X. If $V \in \mathcal{V}$, then $\overline{V} \subseteq K$ (because $V \subseteq U \subseteq K$ and K is closed), and therefore $\overline{V}$ is compact (because a closed subset of a compact set is compact). Thus $\mathcal{V}$ is the required neighborhood base. □

Lemma 1.9.2. *Let X be a locally compact Hausdorff space. If $x \in X$ and U is any neighborhood of x, there exists a precompact neighborhood V of x such that $\overline{V} \subseteq U$.*

Proof. Suppose U is a neighborhood of x. By Proposition 1.9.1 there is a precompact neighborhood W of x. Then $\overline{W} \setminus U$ is closed in $\overline{W}$ and therefore compact. Because compact subsets can be separated by open subsets in a Hausdorff space, there are disjoint open subsets Y containing x and Y' containing $\overline{W} \setminus U$. Let $V = Y \cap W$. Because $\overline{V} \subseteq \overline{W}$, it is compact.

Because $V \subseteq Y \subseteq (Y')^c$, we have $\overline{V} \subseteq \overline{(Y')^c} = (Y')^c$. Since $\overline{W} \setminus U$ is contained in Y', this then implies $\overline{V} \cap (\overline{W} \setminus U) = \varnothing$, and therefore $\overline{V} \subseteq \overline{W} \cap U \subseteq U$. □

Proposition 1.9.3. *Let X be a locally compact Hausdorff space, let K be a compact subset of X, and let U be an neighborhood of K. Then there is a precompact neighborhood V of K such that $\overline{V} \subseteq U$.*

Proof. Lemma 1.9.2 implies that each point in K has a precompact neighborhood whose closure is included in U. Since K is compact, some finite collection of these neighborhoods covers K. Let V be the union of the sets in such a finite collection; then V is the required set. □

Proposition 1.9.4. *Any open or closed subset of a locally compact Hausdorff space is a locally compact Hausdorff space.*

Proof. Let X be a locally compact Hausdorff space. Note that every subspace of X is Hausdorff, so only local compactness needs to be checked. If $Y \subseteq X$ is open, Lemma 1.9.2 says that any point in Y has a neighborhood whose closure is compact and contained in Y, so Y is locally compact. Suppose $Z \subseteq X$ is closed. Any $x \in Z$ has a precompact neighborhood U in X. Since $\overline{U \cap Z}$ is a closed subset of the compact set $\overline{U}$, it is compact. Since $\overline{U \cap Z} \subseteq \overline{Z} = Z$, it follows that $U \cap Z$ is a precompact neighborhood of x in Z. Thus Z is locally compact. □

A subset of a topological space X is a $\boldsymbol{G_\delta}$ if it is the intersection of a sequence of open subsets of X and is an $\boldsymbol{F_\sigma}$ if it is the union of a sequence of closed subsets of X.

Proposition 1.9.5. *Let X be a second countable locally compact Hausdorff space. Then each open subset of X is an F_σ and is in fact the union of a sequence of compact sets. Likewise, each closed subset of X is a G_δ.*

Proof. Suppose that $\mathcal{U}$ is a countable base for the topology of X. Let U be an open subset of X, and let $\mathcal{U}_U$ be the collection of those sets V in $\mathcal{U}$ for which V is precompact and included in U. Lemma 1.9.2 implies that U is the union of the closures of the sets in $\mathcal{U}_U$. Thus U is the union of a countable collection of sets that are closed and, in fact, compact.

Now suppose that C is a closed subset of X. Then C^c is open and so is the union of a sequence $\{F_n\}$ of closed sets. Consequently C is the intersection of the open sets $\{F_n^c\}$. □

Recall that a topological space (or a subset thereof) is σ-compact if it is the union of a countable collection of compact sets.

Corollary 1.9.6. *Every second countable locally compact Hausdorff space is σ-compact.*

Proof. Since a topological space is an open subset of itself, this is an immediate corollary of Proposition 1.9.5. □

1.9.1 Continuous functions

If X is a topological space, the space $\mathbb{R}^X$ of all real-valued functions on X can be topologized in various ways. One way, of course, is the product topology, that is, the topology of pointwise convergence. Another is the **topology of uniform convergence**, which is generated by the sets

$$\{g \in \mathbb{R}^X : \sup_{x \in X} |g(x) - f(x)| < 1/n\}$$

for $f \in \mathbb{R}^X$. Intermediate between these two topologies is the topology of uniform convergence on compact sets, which is generated by the sets

$$\{g \in \mathbb{R}^X : \sup_{x \in K} |g(x) - f(x)| < 1/n\}$$

where $f \in \mathbb{R}^X$ and $K \subseteq X$ is compact. We shall now examine this topology in the case where X is a locally compact Hausdorff space.

Proposition 1.9.7. *If X is a locally compact Hausdorff space, then $C(X)$ is a closed subspace of $\mathbb{R}^X$ in the topology of uniform convergence on compact sets.*

Proof. If f is in the closure of $C(X)$, then f is a uniform limit of continuous functions on each compact $K \subseteq X$, so $f|_K$ is continuous. If $E \subseteq \mathbb{R}$ is closed, then $f^{-1}(E) \cap K = (f|_K)^{-1}(E)$ is closed for each compact K, so $f^{-1}(E)$ is closed (X is compactly generated), whence f is continuous. □

Proposition 1.9.8. *Let X be a σ-compact locally compact Hausdorff space and $\{K_n\}$ be a exhaustion of X by compact subsets, then for each $f \in \mathbb{R}^X$ the sets*

$$\{g \in \mathbb{R}^X : \sup_{x \in K_n} |f(x) - g(x)| < 1/m\}$$

form a neighborhood base for f in the topology of uniform convergence on compact sets. Hence this topology is first countable, and $f_n \to f$ uniformly on compact sets if and only if $f_n \to f$ uniformly on each K_n.

Proof. These assertions follow easily from the observation that if $K \subseteq X$ is compact, then $\{\operatorname{Int} K_n\}$ is an open cover of K and hence $K \subseteq K_n$ for some n. □

One may wonder if there are enough continuous functions on a locally compact Hausdorff space. The following results answer this question.

Proposition 1.9.9 (Urysohn's Lemma, Locally Compact Version). *Let X be a locally compact Hausdorff space. If K is a compact subset of X and U is a neighborhood of K, then there is a continuous function $f : X \to [0,1]$ such that $f \equiv 1$ on K and $f \equiv 0$ outside a compact subset of U.*

Proof. By Proposition 1.9.3, there exists a precompact neighborhood V of K such that $\overline{V} \subseteq U$. Then V is normal, so by Urysohn's lemma there exists a continuous function $f : \overline{V} \to [0,1]$ such that $f \equiv 1$ on K and $f \equiv 0$ on ∂V. We extend f to X by setting $f = 0$ on V.

Now we show that f is a continuous function on X. Suppose that $E \subseteq [0,1]$ is closed. If $0 \notin E$, then we have $f^{-1}(E) = (f|_{\overline{V}})^{-1}(E)$, and if $0 \in E$ we have $f^{-1}(E) = (f|_{\overline{V}})^{-1}(E) \cup (\overline{V})^c = (f|_{\overline{V}})^{-1}(E) \cup (V)^c$ (note that ∂V is contained in $(f|_{\overline{V}})^{-1}(E)$). In either case, $f^{-1}(E)$ is closed, so f is continuous. □

Proposition 1.9.10 (Tietze Extension Theorem, Locally Compact Version). *Let X be a locally compact Hausdorff space and K is a compact subset.*

(a) Any continuous map of K into a closed interval $[a, b]$ may be extended to a continuous map of all of X into $[a, b]$.

(b) Any continuous map of K into $\mathbb{R}$ may be extended to a continuous map of all of X into $\mathbb{R}$.

Moreover, the extension may be taken to vanish outside a compact set.

Proof. We prove (a), and (b) follows as in tietze extension theorem. Let $f : K \to [a, b]$ be a continuous function. Let V be a precompact neighborhood of K. Then $\overline{V}$ is normal, so by Tietze extension theorem there exists a continuous function $F : \overline{V} \to [a, b]$ such that $F|_K = f$. Since V is a neighborhood of K, by 1.9.9 there is a continuous function $\varphi : X \to [0, 1]$ such that $\varphi \equiv 1$ on K and $\varphi \equiv 0$ on a compact subset of V. Define $\widetilde{F}(x) = F(x)\varphi(x)$. By the choice of φ, it is easy to see $\widetilde{F}$ is continuous and $\widetilde{F}|_K = f$. Therefore $\widetilde{F}$ is the required function. □

The preceding results show that locally compact Huasdorff spaces have a rich supply of continuous functions that vanish outside compact sets. Let us recall some terminology: If X is a topological space and $f \in C(X)$, the support of f, denoted by $\operatorname{supp}(f)$, is the smallest closed set outside of which f vanishes, that is, the closure of $\{x : f(x) \neq 0\}$. If $\operatorname{supp}(f)$ is compact, we say that f is **compactly supported**, and we define

$$C_c(X) = \{f \in C(X) : \operatorname{supp}(f) \text{ is compact}\}$$

to be the set of continuous functions on X with compact support. Moreover, if $f \in C(X)$, we say that f **vanishes at infinity** if for every $\varepsilon > 0$ the set $\{x : |f(x)| \geq \varepsilon\}$ is compact, and we define

$$C_0(X) = \{f \in C(X) : f \text{ vanishes at infinity}\}.$$

Clearly $C_c(X) \subseteq C_0(X)$. Moreover, $C_0(X) \subseteq BC(X)$, because for $f \in C_0(X)$ the image of the set $\{x : |f(x)| \geq \varepsilon\}$ is compact, and $|f| < \varepsilon$ on its complement.

Proposition 1.9.11. *If X is a locally compact Hausdorff space, then $C_0(X)$ is the closure of $C_c(X)$ in the uniform metric.*

Proof. If $\{f_n\}$ is a sequence in $C_c(X)$ that converges uniformly to $f \in C(X)$, for each $\varepsilon > 0$ there exists $n \in \mathbb{N}$ such that $\|f - f_n\| < \varepsilon$. Then $|f(x)| < \varepsilon$ for $x \notin \operatorname{supp}(f_n)$, so $f \in C_0(X)$.

Conversely, if $f \in C_0(X)$, for $n \in \mathbb{N}$ let $K_n = \{x : |f(x)| \geq 1/n\}$. Then K_n is compact, so by Proposition 1.9.9 there exists $\varphi_n \in C_c(X)$ with $0 \leq \varphi_n \leq 1$ and $\varphi_n \equiv 1$ on K_n. Let $f_n = \varphi_n f$. Then $f_n \in C_c(X)$ and $\|f_n - f\|_\infty \leq 1/n$, so f_n converges to f uniformly. □

Now we derive some consequences of Proposition 1.9.9 which will be used later. Let us begin with the following lemma.

Lemma 1.9.12. *Let X be a Hausdorff space, let K be a compact subset of X, and let U_1 and U_2 be open subsets of X such that $K \subseteq U_1 \cup U_2$. Then there are compact sets K_1 and K_2 such that $K = K_1 \cup K_2$, $K_1 \subseteq U_1$ and $K_2 \subseteq U_2$.*

Proof. Let $L_1 = K \setminus U_1$ and $L_2 = K \setminus U_2$. Then L_1 and L_2 are disjoint and compact, and so according to Proposition 1.8.6 they can be separated by disjoint open sets, say by V_1 and V_2. If we define K_1 and K_2 by $K_1 = K \setminus V_1$ and $K_2 = K \setminus V_2$, then K_1 and K_2 are compact, are included in U_1 and U_2, respectively, and have K as their union. □

Proposition 1.9.13. *Let X be a locally compact Hausdorff space, let f belong to $C_c(X)$, and let $U_1, \dots, U_n$ be open subsets of X such that* $\operatorname{supp}(f) \subseteq U = \bigcup_{i=1}^n U_i$. *Then there are functions $f_1, \dots, f_n$ in $C_c(X)$ such that $f = f_1 + \cdots + f_n$ and such that for each i the support of f_i is contained in U_i. Furthermore, if the function f is nonnegative, then the functions $f_1, \dots, f_n$ can be chosen so that all are nonnegative.*

Proof. In case $n = 1$ we need only let f_1 be f. So we can begin by supposing that $n = 2$. Use Lemma 1.9.12 to construct compact sets K_1 and K_2 such that $K_1 \subseteq U_1$ and $K_2 \subseteq U_2$, and $\operatorname{supp}(f) = K_1 \cup K_2$, and then use Proposition 1.9.9 to construct functions h_1 and h_2 that belong to $C_c(X)$ and satisfy $\chi_{K_i} \le h_i \le \chi_{U_i}$ and $\operatorname{supp}(h_i) \subseteq U_i$ for $i = 1, 2$. Define functions g_1 and g_2 by $g_1 = h_1$ and $g_2 = h_2 - (h_1 \wedge h_2)$. Then g_1 and g_2 are non-negative, their supports are included in U_1 and U_2, respectively, and they satisfy

$$g_1 + g_2 = h_1 + h_2 - (h_1 \wedge h_2) = h_1 \vee h_2 = 1.$$

at each x in $\operatorname{supp}(f)$. We can complete the proof in the case where $n = 2$ by defining f_1 and f_2 to be fg_1 and fg_2, and the general case follows by induction. □

Proposition 1.9.14. *Let X be a locally compact Hausdorff space, let $K_1, \dots, K_n$ be disjoint compact subsets of X, and let $\alpha_1, \dots, \alpha_n$ be real (or complex) numbers. Then there is a function f that belongs to $C_c(X)$ and satisfies*

(a) $f(x) = \alpha_i$ *if* $x \in K_i$, *for* $i = 1, \dots, n$.

(b) $\|f\|_\infty = \max\{|a_1|, \dots, |a_n|\}$.

Proof. We begin by constructing disjoint open sets $U_1, \dots, U_n$ such that $K_i \subseteq U_i$ holds for each i. If $n = 2$, such sets are provided by Proposition 1.8.6. The general case follows by induction. Next we use Proposition 1.9.9 to choose functions $f_1, \dots, f_n$ that belong to $C_c(X)$ and satisfy $\chi_{K_i} \le f_i \le \chi_{U_i}$ for $i = 1, \dots, n$. The required function f is now given by $f = \sum_{i=1}^n \alpha_i f_i$. □

1.9.2 One-point compactification

If X is a noncompact locally compact Hausdorff space, it is possible to make X into a compact space by adding a single point "at infinity" in such a way that the functions in $C_0(X)$ are precisely those continuous functions f such that $f(x) \to 0$ as x approaches the point at infinity. Here is the precise definition of this space.

Proposition 1.9.15. *Let X be a topological space. Then X is locally compact Hausdorff if and only if there exists a space X^* satisfying the following conditions:*

(a) *X is a subspace of X^*.*

(b) *$X^* \setminus X$ consists of a single point.*

(c) X^* is a compact Huasdorff space.

If X_1 and X_2 are two spaces satisfying these conditions, then there is a homeomorphism of X_1 with X_2 that equals the identity map on X.

Proof. We first verify uniqueness. Let X_1 and X_2 be two spaces satisfying these conditions. Define $h : X_1 \to X_2$ by letting h map the single point p of $X_1 \setminus X$ to the point q of $X_2 \setminus X$, and letting h equal the identity on X. We show that if U is open in X_2, then $h(U)$ is open in X_2. Symmetry then implies that h is a homeomorphism.

First, consider the case where U does not contain p. Then $h(U) = U$. Since U is open in X_1 and is contained in X, it is open in X. Because X is open in X_2, the set U is also open in X_2, as desired. Second, suppose that U contains p. Since $C = X_1 \setminus U$ is closed in X_1, it is compact as a subspace of X_1. Because C is contained in X, it is a compact subspace of X. Then because X is a subspace of X_2, the space C is also a compact subspace of X_2, and hence is closed in X_2. So $h(U) = X_2 \setminus C$ is open, as desired.

Now we suppose X is locally compact Hausdorff and construct the space X^*. Let us take some object that is not a point of X, denote it by the symbol ∞ for convenience, and adjoin it to X, forming the set $X^* = X \cup \{\infty\}$. Topologize X^* by defining the collection of open sets of X^* to consist of (1) all sets U that are open in X, and (2) all sets of the form $X^* \setminus C$, where C is a compact subspace of X. We need to check that this collection is in fact a topology on X^*. The empty set is a set of type (1), and the space X^* is a set of type (2). Checking that the intersection of two open sets is open involves two cases:

$$(X^* \setminus C_1) \cap (X^* \setminus C_2) = X^* \setminus (C_1 \cup C_2), \quad U_1 \cap (X^* \setminus C_1) = U_1 \cap (X \setminus C_1).$$

Similarly, checking that arbitrary union open sets is open involves two cases:

$$\bigcup_\alpha (X^* \setminus C_\alpha) = X^* \setminus \bigcap_\alpha C_\alpha, \quad \Big(\bigcup_\alpha U_\alpha\Big) \cup \bigcup_\beta (X^* \setminus C_\beta) = U \cup (X^* \setminus C) = X^* \setminus (C \setminus U).$$

Therefore we have defined a topology on X^*.

Now we show that X is a subspace of X^*. Given any open set of X^*, we show its intersection with X is open in X. If U is of type (1), then $U \cap X = U$; if $U = X^* \setminus C$ is of type (2), then $U \cap X = X \setminus C$; both of these sets are open in X. Conversely, any set open in X is a set of type (1) and therefore open in X^* by definition.

To show that X^* is compact, let $\mathcal{U}$ be an open covering of X^*. The collection $\mathcal{U}$ must contain an open set of type (2), say $X^* \setminus C$, since none of the open sets of type (1) contain the point ∞. Take all the members of $\mathcal{U}$ different from $X^* \setminus C$ and intersect them with X; they form a collection of open sets of X covering C. Because C is compact, finitely many of them over C; the corresponding finite collection of elements of $\mathcal{U}$ will, along with the element $X^* \setminus C$, cover all of X^*. Therefore X^* is compact.

To show that X^* is Hausdorff, let x and y be two distinct points of X^*. If both of them lie in X, there are disjoint sets U and V open in X containing them, respectively, since X is Huasdorff. On the other hand, if $x \in X$ and $y = \infty$, we can choose a compact set C in X containing a neighborhood U of x. Then U and $X^* \setminus C$ are disjoint neighborhoods of x and ∞, respectively, in X^*.

Finally, we prove the converse. Suppose a space X^* satisfying conditions (a)—(c) exists. Then X is Hausdorff because it is a subspace of the Hausdorff space X^*. Given $x \in X$, we show X is locally compact at x. Choose disjoint open sets U and V of X^* containing x and the single point of $X^* \setminus X$, respectively. Then the set $C = X^* \setminus V$ is closed in X^*, so it is a compact subspace of X^*. Since C lies in X, it is also compact as a subspace of X; it contains the neighborhood U of x. □

If X itself should happen to be compact, then the space X^* of the preceding theorem is not very interesting, for it is obtained from X by adjoining a single isolated point. However, if X is not compact, then the point of $X^* \setminus X$ is a limit point of X, so that $\overline{X} = X^*$.

Definition 1.9.16. *If Y is a compact Hausdorff space and X is a proper subspace of Y whose closure equals Y, then Y is said to be a compactification of X. If $Y \setminus X$ equals a single point, then Y is called the* ***one-point compactification*** *of X.*

Example 1.9.17. The one-point compactification of the real line $\mathbb{R}$ is homeomorphic with the circle, as you may readily check. Similarly, the one-point compactification of $\mathbb{R}^2$ is homeomorphic to the sphere S^2. If $\mathbb{R}^2$ is looked at as the space $\mathbb{C}$ of complex numbers, then $\mathbb{C} \cup \{\infty\}$ is called the **Riemann sphere**, or the **extended complex plane**.

Proposition 1.9.18. *Let X be a locally compact Hausdorff space and X^* be its one-point compactification. Let $f \in C(X)$, then f extends continuously to X^* if and only if f has a limit at the point infinity. That is, if and only if $f = g + a$ where $g \in C_0(X)$ and a is a constant, in which case the continuous extension is given by $f(\infty) = a$.*

Proof. Let f be the form stated above. We extend f to X^* by defining $f(\infty) = a$. We only need to check that f is continuous at ∞, since f is in $C(X)$ and every open set of X is open in X^*. Let $\varepsilon > 0$ be arbitrary, then the set $C_\varepsilon = \{x : |g(x)| \geq \varepsilon\}$ is compact in X, and hence $X^* \setminus C_\varepsilon$ is a neighborhood of ∞ in X^*. By definition, this then implies $|f(x) - a| < \varepsilon$ for $x \in X^* \setminus C_\varepsilon$. Therefore f is continuous at ∞, and so $f \in C(X^*)$.

Conversely, assume that $f \in C(X)$ has an extension $\widetilde{f}$ on X^*. Define $a = \widetilde{f}(\infty)$ and $g(x) = f(x) - a$. We need to show that $g \in C_0(X)$. Let $\varepsilon > 0$, then there exists a neighborhood U of ∞ in X^* such that $f(U) \subseteq (a - \varepsilon, a + \varepsilon)$. By the topology of X^*, since $\infty \in U$, $X \setminus U$ is then compact in X. Since $\{x : |g(x)| \geq \varepsilon\} = \{x : |f(x) - a| \geq \varepsilon\}$ is contained in $X \setminus U$, it is also compact, as desired. □

1.9.3 Stone-Weierstrass theorem

In this part we prove a far-reaching generalization of the well-known theorem of Weierstrass to the effect that any continuous function on a compact interval $[a, b]$ is the uniform limit of polynomials on $[a, b]$. In what follows, X will denote a compact Hausdorff space, and we equip the space $C(X)$ with the uniform metric.

A subset $\mathscr{A}$ of $C(X, \mathbb{R})$ or $C(X, \mathbb{C})$ is said to be **separating** if for every $x, y \in X$ with $x \neq y$ there exists $f \in \mathscr{A}$ such that $f(x) \neq f(y)$. $\mathscr{A}$ is called an **algebra** if it is a real (resp. complex) vector subspace of $C(X, \mathbb{R})$ (resp. $C(X, \mathbb{C})$) such that $fg \in \mathscr{A}$ whenever $f, g \in \mathscr{A}$. If $\mathscr{A} \subseteq C(X, \mathbb{R})$, $\mathscr{A}$ is called a **lattice** if $\max(f, g)$ and $\min(f, g)$ are in $\mathscr{A}$ whenever $f, g \in \mathscr{A}$. Since the algebra and lattice operations are continuous, one easily sees that if $\mathscr{A}$ is an algebra or a lattice, so is its closure $\mathscr{A}$ in the uniform metric.

Theorem 1.9.19 (Stone-Weierstrass Theorem). *Let X be a compact Hausdorff space. If $\mathscr{A}$ is a separating closed subalgebra of $C(X,\mathbb{R})$, then either $A = C(X,\mathbb{R})$ or $A = \{f \in C(X,\mathbb{R}) : f(x_0) = 0\}$ for some $x_0 \in X$. The first alternative holds iff $\mathscr{A}$ contains the constant functions.*

The proof will require several lemmas. The first one, in effect, proves the theorem when X consists of two points, and the second one is a special case of the classical Weierstrass theorem for $X = [-1,1]$. After these two we return to the general case.

Lemma 1.9.20. *Consider $\mathbb{R}^2$ as an algebra under coordinatewise addition and multiplication. Then the only subalgebras of $\mathbb{R}^2$ are $\mathbb{R}^2$, $\{(0,0)\}$, and the linear span of $(1,0)$, $(0,1)$, or $(1,1)$.*

Proof. The subspaces of $\mathbb{R}^2$ listed above are evidently subalgebras. If $\mathscr{A} \subseteq \mathbb{R}^2$ is a nonzero algebra and $(0,0) \neq (a,b) \in \mathscr{A}$, then $(a^2,b^2) \in \mathscr{A}$. If a,b are nonzero and distinct then (a,b) and (a^2,b^2) are linearly independent, so $A = \mathbb{R}^2$. The other possibilities give the other three subalgebras. □

Lemma 1.9.21. *For any $\varepsilon > 0$ there is a polynomial P on $\mathbb{R}$ such that $P(0) = 0$ and $||x| - P(x)| < \varepsilon$ for $x \in [-1,1]$.*

Proof. Consider the Maclaurin series for $(1-t)^{1/2}$:

$$(1-t)^{1/2} = 1 - \sum_n c_n t^n.$$

By the ratio test, this series converges for $|t| < 1$. Moreover, by the monotone convergence theorem (applied to counting measure on $\mathbb{N}$),

$$\sum_n c_n = \lim_{t\to 1^-} \sum_n c_n t^n = 1 - \lim_{t\to 1-} (1-t)^{1/2} = 1.$$

It follows from the finiteness of $\sum_n c_n$ that the series $1 - \sum_n c_n t^n$ converges absolutely and uniformly on $[-1,1]$, and its sum is $(1-t)^{1/2}$ there. Therefore, given $\varepsilon > 0$, by taking a suitable partial sum of this series we obtain a polynomial Q such that $|(1-t)^{1/2} - Q(t)| < \varepsilon/2$ for $t \in [-1,1]$. Set $t = 1-x^2$ and $R(x) = Q(1-x^2)$, we obtain a polynomial R such that $||x|-R(x)| < \varepsilon/2$ for $x \in [-1,1]$. In particular, $|R(0)| < \varepsilon/2$. If we set $P(x)-R(x)-R(0)$, we then get the claim. □

Lemma 1.9.22. *If $\mathscr{A}$ is a closed subalgebra of $C(X,\mathbb{R})$, then $|f| \in \mathscr{A}$ whenever $f \in \mathscr{A}$; hence $\mathscr{A}$ is a lattice.*

Proof. If $f \in \mathscr{A}$ and $f \neq 0$, let $h = f/\|f\|_\infty$. Then h maps X into $[-1,1]$, so if $\varepsilon > 0$ and P is as in Lemma 1.9.21, we have $||h| - P \circ h| < \varepsilon$. Since $P(0) = 0$, P has no constant term, so $P \circ h \in \mathscr{A}$ since $\mathscr{A}$ is an algebra. Since $\mathscr{A}$ is closed and ε is arbitrary, we have $|h| \in \mathscr{A}$ and hence $|f| \in \mathscr{A}$. This proves the first assertion, and the second one follows because $\max(f,g)$ and $\min(f,g)$ can be represented by f, g, and $|f-g|$. □

Lemma 1.9.23. *Suppose $\mathscr{A}$ is a closed lattice in $C(X,\mathbb{R})$ and $f \in C(X,\mathbb{R})$. If for every $x,y \in X$ there exists $h_{xy} \in \mathscr{A}$ such that $h_{xy}(x) = f(x)$ and $h_{xy}(y) = f(y)$, then $f \in \mathscr{A}$.*

Proof. Given $\varepsilon > 0$, for each $x,y \in X$ let

$$U_{xy} = \{z \in X : f(z) < h_{xy}(z) + \varepsilon\}, \quad V_{xy} = \{z \in X : f(z) > h_{xy}(z) - \varepsilon\}.$$

These sets are open and contain x and y. Fix y, then $\{U_{xy} : x \in X\}$ covers X, so there is a finite subcover $\{U_{x_j y}\}$. Let $h_y = \max(h_{x_1 y}, \dots, h_{x_n y})$, then $f < h_y + \varepsilon$ on X and $f > h_y - \varepsilon$ on $V_y = \bigcup_{i=1}^n V_{x_i y}$, which is open and contains y. Thus $\{V_y : y \in X\}$ is another open cover of X, so there is a finite subcover $\{V_{y_j}\}$. Let $h = \min(h_{y_1}, \dots, h_{y_m})$, then $\|f - h\| < \varepsilon$. Since $\mathscr{A}$ is a lattice, $h \in \mathscr{A}$, and since $\mathscr{A}$ is closed and ε is arbitrary, $f \in \mathscr{A}$. □

Proof of Theorem 1.9.19. Given $x \neq y \in X$, let $\mathscr{A}_{xy} = \{(f(x), f(y)) : f \in \mathscr{A}\}$. Then $\mathscr{A}_{xy}$ is a subalgebra of $\mathbb{R}^2$ as in Lemma 1.9.20 because $f \mapsto (f(x), f(y))$ is an algebra homomorphism. If $\mathscr{A}_{x,y} = \mathbb{R}^2$ for all x, y, then Lemmas 1.9.22 and 1.9.23 imply that $\mathscr{A} = C(X, \mathbb{R})$. Otherwise, there exist x, y for which $\mathscr{A}_{xy}$ is a proper subalgebra of $\mathbb{R}^2$. It cannot be $\{(0,0)\}$ or the linear span of $(1,1)$ because $\mathscr{A}$ separates points, so by Lemma 1.9.20 $\mathscr{A}_{xy}$ is the linear span of $(1,0)$ or $(0,1)$. In either case there exists $x_0 \in X$ such that $f(x_0) = 0$ for all $f \in \mathscr{A}$. There is only one such x_0 since A separates points, so if neither x nor y is x_0, we have $\mathscr{A}_{xy} = \mathbb{R}^2$. Lemmas 1.9.22 and 1.9.23 now imply that $\mathscr{A} = \{f \in C(X, \mathbb{R}) : f(x_0) = 0\}$. Finally, if $\mathscr{A}$ contains constant functions, there is no x_0 such that $f(x_0) = 0$ for all $f \in \mathscr{A}$, so $\mathscr{A}$ must equal $C(X, \mathbb{R})$. □

We have stated the Stone-Weierstrass theorem in the form that is most natural for the proof. However, in applications one is typically dealing with a subalgebra $\mathscr{B}$ of $C(X, \mathbb{R})$ that is not closed, and one applies the theorem to $\mathscr{A} = \overline{\mathscr{B}}$. The resulting restatement of the theorem is as follows:

Corollary 1.9.24. *Suppose $\mathscr{B}$ is a separating subalgebra of $C(X, \mathbb{R})$. If there exists $x_0 \in X$ such that $f(x_0) = 0$ for all $f \in \mathscr{B}$, then $\mathscr{B}$ is dense in $\{f \in C(X, \mathbb{R}) : f(x_0) = 0\}$. Otherwise, $\mathscr{B}$ is dense in $C(X, \mathbb{R})$.*

The classical Weierstrass approximation theorem is the special case where X is a compact subset of $\mathbb{R}^n$ and $\mathscr{B}$ is the algebra of polynomials on $\mathbb{R}^n$ (restricted to X); here $\mathscr{B}$ contains the constant functions, so the conclusion is that it is dense in $C(X, \mathbb{R})$.

The Stone-Weierstrass theorem, as it stands, is false for complex-valued functions. For example, the algebra of polynomials in one complex variable is not dense in $C(K)$ for most compact subsets K of $\mathbb{C}$. (In particular, if $\operatorname{Int} K \neq \varnothing$, any uniform limit of polynomials on K must be holomorphic on $\operatorname{Int} K$.) Here we shall give a simple proof that the function $f(z) = \bar{z}$ cannot be approximated uniformly by polynomials on the unit circle. If $P(z) = \sum_j a_j z^j$, then

$$\int_0^{2\pi} \overline{f(e^{it})} P(e^{it})\, dt = \sum_{j=0}^n a_j \int_0^{2\pi} e^{i(j+1)t}\, dt = 0.$$

Since $|f| = 1$ on the unit circle we have

$$2\pi = \int_0^{2\pi} \bar{f} f\, dt \Big| \leq \Big| \int_0^{2\pi} \bar{f}(f - P)\, dt \Big| + \Big| \int_0^{2\pi} \bar{f} P\, dt \Big| \leq \int_0^{2\pi} |f - P|\, dt \leq 2\pi \|f - P\|_\infty.$$

Therefore, $\|f - P\|_\infty \geq 1$ for any polynomial P.

There is, however, a complex version of the Stone-Weierstrass theorem.

Theorem 1.9.25 (Complex Stone-Weierstrass Theorem). *Let X be a compact Hausdorff space. If $\mathscr{A}$ is a separating closed complex subalgebra of $C(X, \mathbb{C})$ that separates points and is closed under complex conjugation, then either $A = C(X, \mathbb{C})$ or $A = \{f \in C(X, \mathbb{C}) : f(x_0) = 0\}$ for some $x_0 \in X$.*

Proof. Since $\mathrm{Re}(f) = (f + \bar{f})/2$ and $\mathrm{Im}(f) = (f - \bar{f})/2i$, the set $\mathscr{A}_{\mathbb{R}}$ of real and imaginary parts of functions in $\mathscr{A}$ is a subalgebra of $C(X, \mathbb{R})$ to which the Stone-Weierstrass theorem applies. Since $\mathscr{A} = \mathscr{A}_{\mathbb{R}} + i\mathscr{A}_{\mathbb{R}}$, the desired result follows. □

There is also a version of the Stone-Weierstrass theorem for locally compact Hausdorff spaces.

Theorem 1.9.26. *Let X be a locally compact Hausdorff space. If $\mathscr{A}$ is a separating closed subalgebra of $C_0(X, \mathbb{R})$, then either $\mathscr{A} = C_0(X, \mathbb{R})$ or $\mathscr{A} = \{f \in C_0(X, \mathbb{R}) : f(x_0) = 0\}$ for some $x_0 \in X$.*

Proof. If there exists $x_0 \in X$ such that $f(x_0) = 0$ for all $f \in \mathscr{A}$, let Y be the one-point compactification of $X \setminus \{x_0\}$. Then by Proposition 1.9.18 we can write $\mathscr{A} \subseteq \{f \in C(Y, \mathbb{R}) : f(+\infty) = 0\}$. Since $\mathscr{A}$ separates points on $X \setminus \{x_0\}$, there is no $y \in X \setminus \{x_0\}$ such that $f(y) = 0$ for all $f \in \mathscr{A}$; it follows that $\mathscr{A}$ separates points in Y, and by the Stone-Weierstrass theorem we get $\mathscr{A} = \{f \in C(Y, \mathbb{R}) : f(+\infty) = 0\} = \{f \in C_0(X, \mathbb{R}) : f(x_0) = 0\}$.

If there is no $x_0 \in X$ such that $f(x_0) = 0$ for all $f \in \mathscr{A}$, let Y be the one-point compactification of X. By the same proof we see $\mathscr{A} = C_0(X, \mathbb{R})$. □

By the same proof as Theorem 1.9.25, we also have the following complex version.

Theorem 1.9.27. *Let X be a locally compact Hausdorff space. If $\mathscr{A}$ is a separating closed complex subalgebra of $C_0(X, \mathbb{C})$ that separates points and is closed under complex conjugation, then either $A = C(X, \mathbb{C})$ or $A = \{f \in C(X, \mathbb{C}) : f(x_0) = 0\}$ for some $x_0 \in X$.*

1.9.4 Metrizability

Now we consider metrizability of locally compact spaces.

Proposition 1.9.28. *A compact Hausdorff space is metrizable if and only if it is second countable.*

Proof. First suppose that X is compact and metrizable. Then X is separable and so is second countable.

Now suppose that X is a compact Hausdorff space that is second countable and let $\mathcal{U}$ be a countable base. The space X is normal, and so for each pair of sets U, V that belong to $\mathcal{U}$ and satisfy $U \cap V = \varnothing$ there is, by Urysohn's lemma, a continuous function $f : X \to [0, 1]$ that vanishes on $\overline{U}$ and has value 1 everywhere on $\overline{V}$. Form a sequence $\{f_n\}$ by choosing one such function for each such pair of sets. Our next step is to check that this sequence of functions separates the points of X, and for this it is enough to show that for each pair x, y of distinct points in X there are sets U and V that belong to $\mathcal{U}$, have disjoint closures, and contain x and y, respectively. To construct such sets, choose disjoint open neighborhoods W_1 and W_2 of x and y, and use Lemma 1.9.2 to choose open sets U and V such that $x \in U \subseteq \overline{U} \subseteq W_1$ and $y \in V \subseteq \overline{V} \subseteq W_2$. By making U and V a bit smaller, if necessary, we can assume that they belong to $\mathcal{U}$. Thus the required sets U and V exist, and the sequence $\{f_n\}$ separates the points of X.

Define a function $d : X \times X \to \mathbb{R}$ by setting

$$d(x, y) = \sum_{n=1}^{\infty} \frac{1}{2^n} |f_n(x) - f_n(y)|.$$

It is easy to use the fact that the functions $\{f_n\}$ separate the points of X to check that d is a metric on the set X and to use the fact that the functions $\{f_n\}$ are continuous (with respect to the original topology on X) to check that the topology induced by d is weaker than the original topology. Since the original topology makes X a compact space, while the topology induced by d is weaker and Hausdorff, the two topologies must be the same (id is a continuous bijection from a compact space to a Huasdorff space). Thus the original topology on X is metrizable and in fact is metrized by d. □

Our next task is to prove that each second countable locally compact Hausdorff space is metrizable. For this we need the following lemma.

Lemma 1.9.29. *Let X be a locally compact Hausdorff space. If X is second countable, then the one-point compactification of X is also second countable.*

Proof. Let $\mathcal{U}$ be a countable base for the topology of X, and let $\mathcal{U}_0$ be the collection of those sets V in $\mathcal{U}$ for which V is precompact. Arrange the sets in $\mathcal{U}_0$ in a sequence, say $\{V_k\}$. Then $X = \bigcup_k V_k$, since X is locally compact, and so for each compact subset K of X there is a positive integer n such that $K \subseteq \bigcup_{k=1}^n V_k$. Thus if U is an open neighborhood in X^* of the point at infinity and if $K = X^* \setminus U$, then there is a positive integer n such that $K \subseteq \bigcup_{k=1}^n V_k$ and hence such that $X^* \setminus \overline{\bigcup_{k=1}^n V_k} \subseteq U$. It follows that the sets in U, together with the sets $X^* \setminus \overline{\bigcup_{k=1}^n V_k}$, form a countable base for the topology of X. □

Proposition 1.9.30. *Each secound countable locally compact Hausdorff space is metrizable.*

Proof. Let X be a secound countable locally compact Hausdorff space. Proposition 1.9.28 and Lemma 1.9.29 imply that the one-point compactification X^* of X is metrizable. Then X, as a subspace of the metrizable space X^*, is metrizable. □

1.10 Proper maps

1.10.1 Proper maps

If f and g are closed continuous maps, it does not follow that $f \times g$ is closed, even if f is the identity map. An example is given below.

Example 1.10.1. Every constant mapping into a Hausdorff space is closed. But it f is the constant mapping $\mathbb{Q} \to \{0\}$, then $f \times \mathrm{id}_{\mathbb{Q}}$ is the mapping $(x, y) \mapsto (0, y)$ of $\mathbb{Q}^2$ into $\mathbb{Q}^2$, so it is the second projection and is not closed.

Definition 1.10.2. *A map $f : X \to Y$ is said to be **proper** if f is continuous and if the mapping $f \times \mathrm{id}_Z : X \times Z \to Y \times Z$ is closed, for every topological space Z.*

If in the definition we take the space Z to consist of a single point, then we see that any proper map is closed. A partial converse holds when the map f is injective:

Proposition 1.10.3. *Let $f : X \to Y$ be a continuous injection. Then the following three statements are equivalent.*

(i) f is proper.

(ii) *f is closed.*

(iii) *f is a homeomorphism of X onto a closed subset of Y.*

Proof. We have just seen that (i) implies (ii). Since the equivalence relation $f(x) = f(y)$ is the equality relation, the quotient space of X with respect to this relation can be identified with X; hence (ii) implies (iii) by Proposition 1.3.5. Finally, if (iii) is satisfied then $f \times \mathrm{id}_Z$ is a homeomorphism of $X \times Z$ onto a closed subspace of $Y \times Z$ and is therefore a closed mapping; hence (iii) implies (i). □

Proposition 1.10.4. *Let $f : X \to Y$ be a continuous map. If B is any subset of Y, let f_B denote the restriction of f on $f^{-1}(B)$.*

(a) *If f is proper, so is f_B.*

(b) *Let $(B_i)_{i\in I}$ be a family of subsets of Y whose interiors cover Y, or which is a locally finite closed covering of Y; then if each of the mappings f_B is proper, so is f.*

Proof. Let Z be a topological space. If B is any subset of Y, we have

$$f_B \times \mathrm{id}_Z = (f \times \mathrm{id}_Z)_{B\times Z}.$$

If f is proper, then $f \times \mathrm{id}_Z$ is closed, hence so is $(f \times \mathrm{id}_Z)_{B\times Z}$ (**??**), whence (a) is proved. If now $(B_i)_{i\in I}$ satisfies one of the two conditions stated in (b), then the covering $(B_i \times Z)_{i\in I}$ of $Y \times Z$ has the same property; if the f_{B_i} are proper then the mappings $(f \times \mathrm{id}_Z)_{B\times Z}$ are closed, whence $f \times \mathrm{id}_Z$ is closed (**??**). This completes the proof. □

Proposition 1.10.5. *Let $f : X \to Y$ and $g : Y \to Z$ be two continuous mappings.*

(a) *If f and g are proper, then $g \circ f$ is proper.*

(b) *If $g \circ f$ is proper and f is surjective, then g is proper.*

(c) *If $g \circ f$ is proper and g is injective, then f is proper.*

(d) *If $g \circ f$ is proper and Y is Hausdorff, then f is proper*

Proof. □

1.10.2 Proper maps

If X and Y are topological spaces, a map $f : X \to Y$ (continuous or not) is said to be **proper** if the preimage of each compact subset of Y is compact. For example, every exhaustion function $f : X \to \mathbb{R}$ is a proper map.

In order to visualize the behavior of proper maps, it is useful to introduce the following definition: if X is a topological space, a sequence (x_i) in X is said to **diverge to infinity** if for every compact set $K \subseteq X$ there are at most finitely many values of i for which $x_i \in K$.

Lemma 1.10.6. *Suppose X is a first countable Hausdorff space. A sequence in X diverges to infinity if and only if it has no convergent subsequence.*

Proof. Assume first that (x_i) is a sequence in X that diverges to infinity. If there is a subsequence (x_{i_j}) that converges to $x \in X$, then the set $K = \{x\} \cup \{x_{i_j}\}$ is compact and contains infinitely many terms of the sequence, which is a contradiction. (This implication does not require the hypothesis that X is first countable and Hausdorff.)

Conversely, assume that (x_i) has no convergent subsequence. If $K \subseteq X$ is any compact set that contains x_i for infinitely many i, then there is a subsequence (x_{i_j}) such that $x_{i_j} \in K$ for all j. Because a compact, first countable Hausdorff space is sequentially compact, this subsequence in turn has a convergent subsequence, which is a contradiction. □

Proposition 1.10.7. *Suppose X and Y are topological spaces and $f : X \to Y$ is a proper map. Then f takes every sequence diverging to infinity in X to a sequence diverging to infinity in Y.*

Proof. Suppose (x_i) is a sequence in X that diverges to infinity. If $\big(f(x_i)\big)$ does not diverge to infinity, then there is a compact subset $K \subseteq Y$ that contains $f(x_i)$ for infinitely many values of i. It follows that x_i lies in the compact set $f^{-1}(K)$ for these values of i, which contradicts the assumption that (x_i) diverges to infinity. □

Because the definition of properness is sometimes tricky to check directly, it is useful to have other sufficient conditions for a map to be proper. The next proposition gives several such conditions.

Proposition 1.10.8. *Suppose X and Y are topological spaces, and $f : X \to Y$ is a continuous map.*

(a) If X is compact and Y is Hausdorff, then f is proper.

(b) If X is a second countable Hausdorff space and f takes sequences diverging to infinity in X to sequences diverging to infinity in Y, then f is proper.

(c) If f is a closed map with compact fibers, then f is proper.

(d) If f is a topological embedding with closed image, then f is proper.

(e) If Y is Hausdorff and f has a continuous left inverse, then f is proper.

(f) If f is proper and $A \subseteq X$ is any subset that is saturated with respect to f, then $f|_A : A \to f(A)$ is proper.

Proof. Suppose X is compact and Y is Hausdorff. If $K \subseteq Y$ is compact, then it is closed in Y because Y is Hausdorff. By continuity, $f^{-1}(K)$ is closed in X and therefore compact.

Assume X is a second countable Hausdorff space, and suppose $f : X \to Y$ takes sequences diverging to infinity to sequences diverging to infinity. Let $K \subseteq Y$ be any compact set, and let $L = f^{-1}(K) \subseteq X$. Because of our hypothesis on X, to show that L is compact, it suffices to show that it is sequentially compact. Suppose on the contrary that (x_i) is a sequence in L with no convergent subsequence. It diverges infinity by Lemma 1.10.6, so our assumption about f implies that $\big(f(x_i)\big)$ diverges to infinity. But this is impossible because $f(x_i)$ lies in the compact set K for all i.

Assume f is a closed map with compact fibers. Let $K \subseteq Y$ be compact, and let $\mathcal{U}$ be a cover of $f^{-1}(K)$ by open subsets of X. If $y \in K$ is arbitrary, the fiber $f^{-1}(y)$ is covered by finitely many of the sets in $\mathcal{U}$, say $U_1, \ldots, U_k$. The set $A_y = X - \bigcup_{i=1}^{k} U_i$ is closed in X and disjoint

from $f^{-1}(y)$, so $V_y = Y - f(A_y)$ is open in Y and contains y. It follows from ourconstruction that

$$f^{-1}(V_y) = f^{-1}(Y - f(A_y)) \subseteq X - A_y = U_1 \cap \cdots \cap U_k.$$

Because K is compact, it is covered by finitely many of the sets V_y. Thus $f^{-1}(K)$ is covered by finitely many sets of the form $f^{-1}(V_y)$, each of which is covered by finitely many of the sets in $\mathcal{U}$, so it follows that $f^{-1}(K)$ is compact.

Now (d) follows from (c), because a topological embedding with closed image is a closed map, and its fibers are singletons, which are certainly compact.

Assume that Y is Hausdorff and $g : Y \to X$ is a continuous left inverse for f, and suppose K is a compact subset of Y. Then we observe that

$$x \in f^{-1}(K) \Rightarrow x = g(f(x)) \in g(K)$$

Since K is closed in Y (because Y is Hausdorff), itfollows that $f^{-1}(K)$ is a closed subset of the compact set $G(K)$, so it is compact.

Finally, to prove (f), suppose $f :\to Y$ is proper and $A \subseteq X$ is saturated. Let $K \subseteq f(A)$ be compact. The fact that A is saturated means that $(f|_A)^{-1}(K) = f(K)$, which is compact because f is proper. □

A topological space X is said to be **compactly generated** if it has the following property:

$$A \text{ is closed in } X \iff A \cap K \text{ is closed in } X \text{ for any compact subset } K$$

It is easy to see that an equivalent definition is obtained by substituting open for closed.

Lemma 1.10.9. *First countable spaces and locally compact spaces are compactly generated.*

Proof. Let X be a space satisfying either of the two hypotheses, and let $A \subseteq X$ be a subset whose intersection with each compact set $K \subseteq X$ is closed in K.

First assume that X is first countable, and let $x \in \overline{A}$. By the sequence lemma, there is a sequence (a_i) of points in A converging to x. The set $K = \{x\} \cup \{a_i : i \in \mathbb{N}\}$ is compact, so $A \cap K$ is closed in K by hypothesis. Since x is the limit of a sequence of points in $A \cap K$, it must also be in $A \cap K \subseteq A$. Thus A is closed.

Now assume X is locally compact. Let $x \in A^c$, we want to find a neighborhood of x disjoint from A. Now let K be a compact subset of X containing a neighborhood U of x. If $U \cap A = \varnothing$, then we are done. Otherwise let $\widetilde{U} = U \setminus (A \cap K)$. Since $A \cap K$ is closed, $\widetilde{U}$ is open in X. This is the desired neighborhood of x. □

Theorem 1.10.10. *Suppose X is any topological space, Y is a compactly generated Hausdorff space and $F : X \to Y$ is a proper continuous map. Then F is a closed map.*

Proof. Let $A \subseteq X$ be a closed subset. We show that $F(A)$ is closed in Y by showing that its intersection with each compact subset is closed. If $K \subseteq Y$ is compact, then $F^{-1}(K)$ is compact since F is proper, and so is $A \cap F^{-1}(K)$ because it is a closed subset of a compact set. By the main theorem on compactness, $F\big(A \cap F^{-1}(K)\big)$ is compact as well. This set is equal to $F(A) \cap K$. Because K is Hausdorff, $F(A) \cap K$ is closed in K. □

Corollary 1.10.11. *If X is a topological space and Y is a compactly generated Hausdorff space, an embedding $F : X \to Y$ is proper if and only if it has closed image.*

Proof. If F is proper, then by Theorem 1.10.10 F is closed, so $F(X)$ is closed. Conversely, if $F(X)$ is closed, then by Proposition 1.10.8(d) we know F is proper. □

Corollary 1.10.12. *Suppose F is a proper continuous map from a topological space to a compactly generated Hausdorff space.*

(a) If F is surjective, it is a quotient map.

(b) If F is injective, it is a topological embedding.

(c) If F is bijective, it is a homeomorphism.

1.11 Baire Spaces

1.11.1 Nowhere dense sets and meager sets

We develop the elementary properties of nowhere dense sets here.

Definition 1.11.1. *A subset A of a topological space X is called **nowhere dense** if its closure has empty interior.*

Before giving some examples, we consider some elementary properties of nowhere dense sets.

Proposition 1.11.2. *In a topological space X:*

(a) $A \subseteq X$ is nowhere dense iff $(\overline{A})^c$ is dense.

(b) $A \subseteq X$ is nowhere dense iff every nonempty open subset U of X contains a nonempty open subset that is disjoint from A.

Proof. Assume that A is nowhere dense. If $A = \varnothing$, the result is clear so suppose that $A \neq \varnothing$. Then any nonempty open subset U of X meets the dense subset $(\overline{A})^c$ and the nonempty open set $U \cap (\overline{A})^c$ is disjoint from A. Conversely, the condition says that any nonempty open set meets $(\overline{A})^c$ which means that $(\overline{A})^c$ is dense and so A is nowhere dense by (a). □

We point out that when we speak of a set $A \subseteq X$ as being nowhere dense, we mean with respect to X's topology, not the topology it induces on X—a nonempty set X is never a nowhere dense subset of itself, because $\mathrm{cl}_A A = A$.

Example 1.11.3.

(a) Any subset of a nowhere dense set is nowhere dense. The empty set is nowhere dense; so are singletons in any Hausdorff space as long as the point is not isolated. The only nowhere dense subset of a discrete space is $\varnothing$.

(b) The rationals $\mathbb{Q}$ are not nowhere dense in $\mathbb{R}$, but the integers $\mathbb{Z}$ are.

(c) The set $\{1/n : n \in \mathbb{N}\} \cup \{0\}$ is nowhere dense in $\mathbb{R}$.

(d) The boundary ∂A of a set A is the set $\overline{A} \cap \overline{(A^c)}$. If A is open, then $\partial A \subseteq A^c$ while a neighborhood of any point in ∂A must meet A and A^c. Thus ∂A has no interior. By the same reasoning, if A is closed, $\partial A \subseteq A$ and $\operatorname{Int} \partial A = \varnothing$. Two things follow: a closed set is nowhere dense iff it coincides with its boundary; and boundaries of open or closed sets are nowhere dense.

(e) A linear subspace M of a topological vector space X is nowhere dense or dense. Note that the closure of a subspace is again a subspace. If M is not nowhere dense then $\operatorname{Int} \overline{M} \neq \varnothing$. By translation, it follows immediately that 0 is an interior point of $\overline{M}$. Thus $\overline{M}$ is a neighborhood of 0 and is therefore equal to X.

(f) In a Hausdorff topological vector space, finite-dimensional subspaces are closed. Thus, by (e), proper finite-dimensional subspaces are nowhere dense.

Now we present some elementary properties of nowhere dense sets.

Proposition 1.11.4. *Let X be a topological space.*

(a) Subsets of nowhere dense ses are nowhere dense.

(b) Finite unions of nowhere dense sets are nowhere dense.

(c) Suppose that $A \subseteq S \subseteq X$. If A is nowhere dense in S, then A is nowhere dense in X. Conversely, if S is open in X and A is nowhere dense in X, then A is nowhere dense in S.

Proof. If A is nowhere dense then so is any $B \subseteq A$ since $\overline{B} \subseteq \overline{A}$. The key fact is that finite intersections of dense open sets are dense. To prove this, suppose that A and B are dense open sets. Thus, if U is a nonempty open set, $U \cap A \neq \varnothing$. As $U \cap A$ is a nonempty open set, it meets B nontrivially. Thus $A \cap B$ is dense.

Suppose that $A \subseteq S \subseteq X$ and that A is not nowhere dense in X. Then there is a nonempty open set U in X that does not meet $(\overline{A})^c$, i.e., such that $U \subseteq \overline{A}$ and $U \cap S \subseteq \overline{A} \cap S = \operatorname{cl}_S A$. Since $U \cap A \subseteq U \cap S$ and $U \cap A \neq \varnothing$ because $U \subseteq \overline{A}$, this shows that $\operatorname{cl}_S A$ has nonempty interior, i.e., that A is not nowhere dense in S.

For the converse, suppose that A is nowhere dense in X, S is open and U is a nonempty open subset of S. Since S is open in X, so is U. Since A is nowhere dense in X, U must contain a nonempty open subset V of X—hence also of S—that does not meet A. It follows from Proposition 1.11.2 that A is nowhere dense in S. □

Corollary 1.11.5. *Let A be a nowhere dense subset in X and $U \subseteq X$ be open. Then $U \cap A$ is nowhere dense in U.*

Definition 1.11.6. *A subset of a topological space X is called **meager in X** if it can be written as a countable union of nowhere dense sets of X, or, equivalently, is a subset of such a union. Otherwise, E is called **nonmeager in X**. A topological space is called **meager** if it is a meager subset of itself.*

Example 1.11.7 (Examples of Meager and Nonmeager Sets).

(a) As we can write the rationals $\mathbb{Q}$ as a countable union of singletons, $\mathbb{Q}$ is a meager subset of $\mathbb{R}$. Indeed, any countable Hausdorff space without isolated points is meager.

(b) Any topological space which contains an isolated point x is nonmeager, as no set to which x belongs can be nowhere dense. Thus discrete spaces are never meager.

(c) Singletons are always nonmeager subspaces. A singleton is a nonmeager subset of a topological space iff the point is isolated.

(d) View $\mathbb{Q}\times\mathbb{Q}$ together with the x-axis as a subspace of $\mathbb{R}^2$. As the x-axis is a nowhere dense subset of $\mathbb{R}^2$ and we can enumerate $\mathbb{Q}\times\mathbb{Q}$, $(\mathbb{Q}\times\mathbb{Q})\cup(\mathbb{R}\times\{0\})$ is a meager subset of $\mathbb{R}^2$. However, as we will see, $\mathbb{R}\times\{0\}$ it self is a nonmeager subspace. The point is that the presence of a nonmeager subspace does not imply that the space itself is nonmeager.

An important property of meager sets is that any open subset of a meager set is again meager.

Proposition 1.11.8. *Let $U \subseteq X$ be a open subset. If X is meager, then so is U.*

Proof. If there are nowhere dense subsets $\{E_n\}$ of X such that $X = \bigcup_n E_n$, then $U = \bigcup_n (E_n \cap U)$. As U is open in X, each $E_n \cap U$ is nowhere dense in U by Corollary 1.11.5 and therefore U is meager. □

It is then interesting that whether any open subsets of a nonmeager space is nonmeager. For this, we recall that empty set is meager, so we may concentrate on nonempty open subsets. It turns out that this property is equivalent to some other conditions, and is not true in general. The Baire spaces that we will define are exactly nonmeager spaces satisfying these conditions.

Theorem 1.11.9. *The following conditions on a topological space X are equivalent:*

(i) The union of countably many closed nowhere dense sets have empty interior.

(ii) The intersection of countably many dense open sets is dense.

(iii) Each nonempty open subset is nonmeager.

(iv) Each meager subsets has dense complement.

*A **Baire space** is one which satisfies either of the conditions above.*

Proof. It is clear that $(i) \Leftrightarrow (ii)$. Assume (ii) and let $U \subseteq X$ be a meager open set so that there are nowhere dense subset $\{E_n\}$ such that $U = \bigcup_n E_n \subseteq \bigcup_n \overline{E}_n$. Then $U^c \supseteq \bigcap_n (\overline{E}_n)^c$ and since each $(\overline{E}_n)^c$ is dense and open, $\bigcap_n (\overline{E}_n)^c$ must be dense by hypothesis. Since U^c is closed, it follows that $U^c = X$ or $U = \varnothing$.

Suppose that nonempty open subsets are nonmeager in X. Let $A \subseteq X$ be meager, then $\operatorname{Int} A$ must be meager, too. By hypothesis $\operatorname{Int} A = \varnothing$ and therefore A^c is dense. This proves $(iii) \Rightarrow (iv)$.

Finally, assume (iv). Let $\{E_n\}$ be a sequence of closed nowhere dense sets and let $E = \bigcup_n E_n$. Since E is meager, E^c is dense by hypothesis. Therefore $\operatorname{Int} E = \varnothing$. □

It is clear that every open subset of a Baire space is Baire. Thus a Baire space is **locally Baire**. It turns out that the converse is also ture.

Proposition 1.11.10. *If each point in a topologiral space X has a neighborhood which is a Baire space, then X is a Baire space.*

Proof. Let $U \subseteq X$ be a nonempty open subset and let $x \in U$. By hypothesis, x has an open neighborhood V which is a Baire space. If U were meager in X, $U \cap V$ would be meager in V and open in V, contradicting the Baireness of V. □

Example 1.11.11. Obviously, Baire spaces are nonmeager. To see that nonmeager spaces need not be Baire, consider the metric space $\mathbb{Q} \cup (0,1)$. Since it contains the open nonmeager subspace $(0,1)$, it is nonmeager. Since it has meager open sets such as $\{x \in \mathbb{Q} : x > 1\}$, it is not a Baire space. Note also that this is an incomplete metric space which is nonmeager.

Some interesting properties for Baire spaces are given below.

Proposition 1.11.12. *Let X be a Baire space and $\{f_s : s \in S\}$ a family of lower semicontinuous real-valued functions on X that is pointwise bounded from above on X. Then each nonempty open subset of X contains a nonempty open subset on which $\{f_s : s \in S\}$ is bounded from above.*

Proof. It suffices to prove the claim for X. The map $f = \sup_s f_s$ is lower semicontinuous. Decompose X into the union of the closed sets $F_n = f^{-1}([-n, n])$. Since X is nonmeager, some F_n has a nonempty interior. The theorem now follows. □

Note that Proposition 1.11.12 remain valid for complex-valued functions, and even for functions $\{f_s : s \in S\}$ with values in a normed space by considering the functions $\|f_s\|$.

Proposition 1.11.13. *Let X be a space; let (Y, d) be a metric space. Let $f_n : X \to Y$ be a sequence of continuous functions such that $f_n(x) \to f(x)$ for all $x \in X$, where $f : X \to Y$. If X is a Baire space, the set of points at which f is continuous is dense in X.*

Proof. Given a positive integer N and given $\varepsilon > 0$, define

$$E_N(\varepsilon) = \{x \in X : d(f_n(x), f_m(x)) \leq \varepsilon \text{ for } n, m \geq N\}.$$

Note that $E_N(\varepsilon)$ is closed in X. For the set of those x for which $d(f_n(x), f_m(x)) \leq \varepsilon$ is closed in X, by continuity of f_n and f_m, and $E_N(\varepsilon)$ is the intersection of these sets for all $n, m \geq N$. For fixed ε, since $f_n \to f$, we have $\bigcup_N E_N(\varepsilon) = X$. Now let

$$U(\varepsilon) = \bigcup_{N=1}^{\infty} \operatorname{Int} E_N(\varepsilon).$$

We claim that $U(\varepsilon)$ is open and dense. To show this, it suffices to show that for any nonempty open set V of X, there is an N such that the set $V \cap \operatorname{Int} E_N(\varepsilon)$ is nonempty. For this purpose, we note first that for each N, the set $V \cap E_N(\varepsilon)$ is closed in V. Because V is a Baire space, at least one of these sets, say $V \cap E_M(\varepsilon)$, must contain a nonempty open set W of V. Because V is open in X, the set W is open in X; therefore, it is contained in $\operatorname{Int} E_M(\varepsilon)$.

Now we show that f_n converges to f uniformly on the set $C = \bigcap_n U_n(1/n)$, which is dense since X is a Baire space. To this end, let $\varepsilon > 0$ be fixed. Choose $N \in \mathbb{N}$ such that $1/N < \varepsilon$. Then since $C \subseteq U_N(1/N)$, we have $d(f_n(x), f_m(x)) < \varepsilon$ for $n, m \geq N$ and $x \in C$. Let $m \to +\infty$, this implies $d(f_n(x), f(x)) < \varepsilon$ for $n \geq N$, thus the claim follows. □

1.11.2 Baire category theorem

Proposition 1.11.14 (Criterion for Baireness). *A topological space $(X, \mathcal{T})$ is a Baire space if there exists a relation $\preceq$ among the collection $\mathcal{T}^*$ of nonempty open subsets of X such that for $A, B, C, D \in \mathcal{T}^*$,*

(a) if $A \preceq B$, then $A \subseteq B$;

(b) for every $B \in \mathcal{T}^*$, there is an $A \in \mathcal{T}^*$ such that $A \preceq B$;

(c) if $A \subseteq B \preceq C \subseteq D$, then $A \preceq D$;

(d) if $\{A_n\}$ is a sequence of nonempty open sets such that $A_n \succeq A_{n+1}$ for each $n \in \mathbb{N}$, then $\bigcap_n A_n \neq \varnothing$.

Proof. Suppose that the relation $\preceq$ satisfies (a)–(d) is defined on the nonempty open sets $\mathcal{T}^*$ of the topological space $(X, \mathcal{T})$. If X is not a Baire space, it must contain a nonempty meager open set U. Consequently, there must be a sequence $\{E_n\}$ of closed nowhere dense sets whose union contains U. We now construct a sequence $\{U_n\}$ of open subsets of U such that $U_n \succeq U_{n+1}$ and $U_n \cap (E_1 \cup \cdots \cup E_n) = \varnothing$ for each $n \in \mathbb{N}$. With this, we see

$$\bigcap_{n=1}^{\infty} U_n = U \cap \bigcap_{n=1}^{\infty} U_n \subseteq \bigcap_{n=1}^{\infty} U_n \cap \bigcup_{n=1}^{\infty} E_n = \varnothing,$$

which contradicts condition (d).

Now we construct $\{U_n\}$. Since $\operatorname{Int} E_1 = \varnothing$, certainly $U \nsubseteq E_1$. Hence $U \cap E_1^c$ is a nonempty open subset of U which does not meet E_1. By (b), there is a nonempty open set U_1 such that $U_1 \preceq U \cap E_1^c$. By (c) we have $U_1 \preceq U$, so $U_1 \subseteq U$ and $U_1 \cap E_1 = \varnothing$. Since U_1 is a nonempty open set, $U_1 \nsubseteq (E_1 \cup E_2)$ and there must be a nonempty open set U_2 such that $U_2 \preceq U_1$ and $U_2 \cap (E_1 \cup E_2) = 0$. By induction, the sequence $\{U_n\}$ mentioned above is now seen to exist. □

We show next that a complete pseudometric space or locally compact Hausdorff space is a Baire space by showing that a relation such as the one of Proposition 1.11.14 may be defined on the nonempty open sets.

Theorem 1.11.15 (Baire Category Theorem). *Any locally compact Hausdorff space or complete pseudometric space is Baire.*

Proof. We first consider locally compact Hausdorff spaces. For nonempty open sets A and B of a locally compact Hausdorff space X, define $A \preceq B$ if A is precompact and $\overline{A} \subseteq B$. In view of Lemma 1.9.2, properties (a)–(c) of Proposition 1.11.14 are easy to verify. As for (d), suppose that $\{U_n\}$ is a sequence of nonempty open sets such that $U_n \succeq U_{n+1}$. The sets $\{\overline{U}_n : n > 2\}$ are nested in the compact space $\overline{U}_2$, so they have nonempty intersection. It then follows that

$$\varnothing \neq \bigcap_{n=3}^{\infty} \overline{U}_n \subseteq \bigcap_{n=2}^{\infty} U_n \subseteq \bigcap_{n=1}^{\infty} U_n.$$

Thus X is Baire by Proposition 1.11.14.

Now we turn to complete pseudometric spaces. For any subset A of a complete pseudometric space (X, d), let

$$d(A) = \operatorname{diam}(A), \quad d^*(A) = \min\{1, d(A)\}$$

and note that $A \subseteq B$ implies $d^*(A) \leq d^*(B)$. For $A, B \in \mathcal{T}^*$, we define $A \preceq B$ iff $\overline{A} \subseteq B$ and $d(A) \leq (1/2)d^*(B)$. We show that $\preceq$ satisfies conditions of Proposition 1.11.14. That $A \preceq B$ implies $A \subseteq B$ is clear. Moreover, for any $A \in \mathcal{T}^*$, let $x \in A \in \mathcal{T}^*$ and choose $0 < r < 1$ such that $B_r(x) \subseteq A$. With $r' = d(B_r(x)) \leq r < 1$ and $U = B_{r'/4}(x)$, we have $U \preceq A$. As for (c), if $A \subseteq B \preceq C \subseteq D$, then $\overline{A} \subseteq C \subseteq D$; since $d(A) \leq (1/2)d^*(C) \leq (1/2)d^*(D)$, it follows that $A \preceq D$.

We now use the completeness of X to show that (d) is satisfied. For this purpose, let $\{U_n\}$ be a sequence of nonempty open sets, decreasing with respect to $\preceq$. Since $d^*(U_1) \leq 1$, we have $d(U_n) \leq 2^{-n+1}$ for each $n \in \mathbb{N}$. Hence, choosing $x_n \in U_n$ for each $n \in \mathbb{N}$ yields a d-Cauchy sequence. Since X is complete, $\{x_n\}$ has a limit $x \in X$. Since $x_m \in U_n$ for $m \geq n$, we have $x \in \overline{U}_n$ for each n, and thus $x \in \bigcap_n U_n$. □

Corollary 1.11.16. *In a locally compact Hausdorff space or a complete metric space, every nonempty countable closed subset contains at least one isolated point.*

Proof. Assume X is such a space. Let $A \subseteq X$ be a nonempty countable closed subset, and assume that A has no isolated points. The fact that A is closed in X means that A itself is either a locally compact Hausdorff space or a complete metric space. For each $a \in A$, the singleton $\{a\}$ is nowhere dense in A: it is closed in A because A is Hausdorff, and it contains no nonempty open subset because A has no isolated points. Since A is a countable union of singletons, A is meager in A, which is a contradiction. □

Proposition 1.11.17. *Let $\{U_n\}$ be a sequence of open dense subsets of a locally compact Hausdorff space or a complete metric space X with no isolated points and $U := \bigcap_n U_n$. Then U is dense in X and uncountable. In particular, no countable dense subset of X can be obtained as the intersection of a countable family of open sets, i.e., is not G_δ.*

Proof. Since X is Baire, we know U is dense. If $U = \{x_n\}$ then, since each $\{x_n\}$ is closed and nowhere dense in X, it follows that

$$U \cap \bigcap_n \{x_n\}^c = U \cap U^c = \varnothing$$

is open dense, which is a contradiction. □

Corollary 1.11.18. *There is no function from $\mathbb{R}$ to $\mathbb{R}$ which is continuous at each rational point and discontinuous at each irrational point.*

Proof. The points of continuity of f form a G_δ set. But $\mathbb{Q}$ is not G_δ by Proposition 1.11.17. □

1.12 Topological manifolds

1.12.1 Definition of manifolds

A topological space M is said to be **locally Euclidean** of dimension n if every point of M has a neighborhood in M that is homeomorphic to an open subset of $\mathbb{R}^n$.

Lemma 1.12.1. *A topological space M is locally Euclidean of dimension n if and only if either of the following properties holds:*

(a) Every point of M has a neighborhood homeomorphic to an open ball in $\mathbb{R}^n$.

(b) Every point of M has a neighborhood homeomorphic to $\mathbb{R}^n$.

In addition, $\mathbb{R}^n$ is homeomorphic to an open ball in $\mathbb{R}^n$.

Proof. It is immediate that any space with property (a) or (b) is locally Euclidean of dimension n. Conversely, suppose M is locally Euclidean of dimension n. Because any open ball in $\mathbb{R}^n$ is homeomorphic to $\mathbb{R}^n$ itself, properties (a) and (b) are equivalent, so we need only prove (a).

Given a point $p \in M$, let U be a neighborhood of p that admits a homeomorphism $\varphi : U \to V$, where V is an open subset of $\mathbb{R}^n$. The fact that V is open in $\mathbb{R}^n$ means that there is some open ball B around $\varphi(p)$ that is contained in V, and then $\varphi^{-1}(B)$ is a neighborhood of p homeomorphic to B. □

Suppose M is locally Euclidean of dimension n. If $U \subseteq M$ is an open subset that is homeomorphic to an open subset of $\mathbb{R}^n$, then U is called a **coordinate domain**, and any homeomorphism φ from U to an open subset of $\mathbb{R}^n$ is called a **coordinate map**. The pair (U, φ) is called a **coordinate chart** (or just a chart) for M. A **coordinate domain** that is homeomorphic to a ball in $\mathbb{R}^n$ is called a **coordinate ball**. The preceding lemma shows that every point in a locally Euclidean space is contained in a coordinate ball.

The definition of locally Euclidean spaces makes sense even when $n = 0$. Because $\mathbb{R}^0$ is a single point, Lemma 1.12.1(b) implies that a space is locally Euclidean of dimension 0 if and only if each point has a neighborhood homeomorphic to a one-point space, or in other words if and only if the space is discrete.

Definition 1.12.2 (topological manifold). *An n-dimensional **topological manifold** is a second countable Hausdorff space that is locally Euclidean of dimension n.*

The most obvious example of an n-manifold is $\mathbb{R}^n$ itself. More generally, any open subset of $\mathbb{R}^n$—or in fact of any n-manifold—is again an n-manifold, as the next proposition shows.

Proposition 1.12.3. *Every open subset of an n-manifold is an n-manifold.*

Proof. Let M be an n-manifold, and let V be an open subset of M. Any $p \in V$ has a neighborhood (in M) that is homeomorphic to an open subset of $\mathbb{R}^n$; the intersection of that neighborhood with V is still open, still homeomorphic to an open subset of $\mathbb{R}^n$, and is contained in V, so V is locally Euclidean of dimension n. Since any open subset of a Hausdorff space is Hausdorff and any open subset of a second countable space is second countable, we see that V is an n-manifold. □

Theorem 1.12.4. *A separable metric space that is locally Euclidean of dimension n is an n-manifold. And the converse is also true.*

Proof. Every metric space is Hausdorff, and Theorem 1.6.2 shows that a separable metric space is second countable. For the converse, separability follows from Theorem 1.6.1, and metrizability follows from Urysohn metrization theorem. □

Proposition 1.12.5. *Suppose P is a second countable space and M is a quotient space of P. If M is locally Euclidean, then it is second countable. Thus if M is locally Euclidean and Hausdorff, it is a manifold.*

Proof. Let $q : P \to M$ denote the quotient map, and let $\mathcal{U}$ be a cover of M by coordinate balls. The collection $q^{-1}(\mathcal{U}) = \{q^{-1}(U) : U \in \mathcal{U}\}$ is an open cover of P, which has a countable subcover since P is Lindelöf. If we let $\mathcal{U}' \subseteq \mathcal{U}$ denote a countable subset of $\mathcal{U}$ such that $q^{-1}(\mathcal{U}')$ covers P, then $\mathcal{U}'$ is a countable cover of M by coordinate balls. Each such ball is second countable, so M is also second countable. □

1.12.2 Manifolds with boundary

In many cases we will encounter spaces that would be manifolds except that they have a boundary. The following definition deals with this problem.

The closed n dimensional upper half-space $\mathbb{H}^n \subseteq \mathbb{R}^n$ is defined by

$$\mathbb{H}^n := \{(x_1, \dots, x_n) \in \mathbb{R}^n : x_n \geq 0\}$$

Definition 1.12.6 (Manifolds with Boundary). *An n-dimensional manifold with boundary is a second countable Hausdorff space in which every point has a neighborhood homeomorphic either to an open subset of $\mathbb{R}^n$, or to an open subset of $\mathbb{H}^n$.*

Note that, despite the terminology, a manifold with boundary is not necessarily a manifold. When it is important to make the distinction, we say (U, φ) is an **interior chart** if (U, φ_0) is an open subset of $\mathbb{R}^n$, and a **boundary chart** if (U, φ) is an open subset of $\mathbb{H}^n$ with $\varphi(U) \cap \partial\mathbb{H}^n \neq \varnothing$.

If M is an n-manifold with boundary, we define a coordinate chart for M to be a pair (U, φ), where $U \subseteq M$ is open and φ is a homeomorphism from U to an open subset of either $\mathbb{R}^n$ or $\mathbb{H}^n$. Just as in the case of manifolds, the set U is called a **coordinate domain**, and φ is called a coordinate map. We use the notation $\partial\mathbb{H}^n$ to denote the boundary of $\mathbb{H}^n$, and $\operatorname{Int}\mathbb{H}^n$ to denote its interior, considering $\mathbb{H}^n$ as a subset of $\mathbb{R}^n$. For $n > 0$, this means

$$\partial\mathbb{H}^n = \{(x_1, \dots, x_n) : x_n = 0\}, \quad \operatorname{Int}\mathbb{H}^n = \{(x_1, \dots, x_n) : x_n > 0\}.$$

When $n = 0$, we have $\mathbb{H}^0 = \mathbb{R}^0 = \{0\}$, so $\operatorname{Int}\mathbb{H}^0 = \mathbb{H}^0$ and $\partial\mathbb{H}^0 = \varnothing$. It follows that 0-dimensional manifolds with boundary are no different from 0-manifolds.

Example 1.12.7. The upper half-spaceHn itself is an nmanifold with boundary, with the identity map as a global coordinate map. Similarly, any closed or half-open interval in $\mathbb{R}$ is a 1-manifold with boundary, for which charts are easy to construct. Another important example is the closed unit ball $\overline{B}^n$ with the Euclidean topology. It is not hard to see intuitively that $\overline{B}^n$ is an n-manifold with boundary

If M is an n-manifold with boundary, a point $p \in M$ is called an **interior point** of M if it is in the domain of an interior chart; and it is called a **boundary point** of M if it is in the domain of a boundary chart that takes p to $\partial\mathbb{H}^n$. The **boundary of M**, denoted by ∂M, is the set of all its boundary points, and its **interior**, denoted by $\operatorname{Int} M$, is the set of all its interior points.

Note that these are new meanings for the terms boundary and interior, distinct from their use earlier in reference to subsets of topological spaces. If M is a manifold with boundary, it

might have nonempty boundary in this new sense, irrespective of whether it has any boundary points as a subset of some other topological space. Usually the distinction is clear from the context, but if necessary we can always distinguish the two meanings by referring to the **topological boundary** (for the original meaning) or the **manifold boundary** (for this new meaning) as appropriate.

Theorem 1.12.8. *If M is an n-dimensional manifold with boundary, then* $\mathrm{Int}M$ *is an open subset of M, which is itself an n-dimensional manifold without boundary. And ∂M is an $(n-1)$-manifold without boundary.*

There is a subtlety about these definitions that might not be immediately evident. Although the interior and boundary of M are well-defined subsets whose union is M, and it might seem intuitively rather obvious that they are disjoint from each other, we have no way of proving at this stage that a point $p \in M$ cannot be simultaneously a boundary point and an interior point, meaning that there is one interior chart whose domain contains p, and another boundary chart that sends p to $\partial\mathbb{H}^n$. After we have developed some more machinery, you will be able to prove the following theorem.

Theorem 1.12.9 (Invariance of the Boundary). *If M is a manifold with boundary, then a point of M cannot be both a boundary point and an interior point. Thus ∂M and* $\mathrm{Int}M$ *are disjoint subsets whose union is M.*

Corollary 1.12.10. *If M is a nonempty n-dimensional manifold with boundary, then ∂M is closed in M, and M is an n-manifold if and only if $\partial M = \varnothing$.*

Proof. Because $\mathrm{Int}\, M$ is an open subset of M by Theorem 1.12.8, it follows from Theorem 1.12.9 that $\partial M = M \setminus \mathrm{Int}\, M$ is closed. If M is a manifold, then every point is in the domain of an interior chart, so $M = \mathrm{Int}\, M$, and it follows from Theorem 1.12.9 that $\partial M = \varnothing$. Conversely, if $\partial M = \varnothing$, then $M = \mathrm{Int}\, M$, which is a manifold by Theorem 1.12.8. □

Corollary 1.12.11. *Let M be a smooth manifold with boundary, let (U, φ) be a boundary chart on M, and let p be a point in $\partial M \cap U$. Then $\varphi(p)$ is in $\partial\mathbb{H}^n$. Thus, a coordinate map sends boundary points to boundary points.*

Proof. If p is a boundary point, then $\varphi(p)$ is also a boundary point in $\mathbb{H}^n$. Thus by Theorem 1.12.9 we know $\varphi(p) \in \partial\mathbb{H}^n$. □

More generally, we have the following result.

Theorem 1.12.12. *If M and N are smooth manifolds with boundary and $F : M \to N$ is a homeomorphism, then $F(\partial M) = \partial N$, hence $F(\mathrm{Int}\, M) = F(\mathrm{Int}\, N)$.*

Proof. Since F is a homeomorphism, every boundary point of M is mapped to boundary of N, and vise versa. Thus we have $F(\partial M) = \partial N$, and since M is the disjoint union of its interior and boundary, we also have $F(\mathrm{Int}\, M) = \mathrm{Int}\, N$. □

Example 1.12.13. If $U \subseteq \mathbb{R}^n$ is an open subset and $f : U \to \mathbb{R}^k$ is any continuous map, the graph of f is the subset $\Gamma(f) \subseteq \mathbb{R}^{n+k}$ defined by

$$\Gamma(f) := \{(x, y) \in \mathbb{R}^{n+k} : x \in U \text{ and } y = f(x)\}$$

with the subspace topology inherited from $\mathbb{R}^{n+k}$. Let $\Phi_f : U \to \mathbb{R}^{n+k}$ be the continuous injective map

$$\Phi_f(x) = \big(x, f(x)\big)$$

the the restriction to $\Gamma(f)$ of the projection $\pi : \mathbb{R}^{n+k} \to \mathbb{R}^n$ is a continuous inverse for Φ_f. Hence $\Gamma(f)$ is homeomorphic to U and is a manifold.

Example 1.12.14. Define $\mathbb{RP}^n$ to be the set of 1-dimensional linear subspaces (lines through the origin) in $\mathbb{R}^{n+1}$, and $\mathbb{CP}^n$ be the set of all 1-dimensional complex subspaces of $\mathbb{C}^{n+1}$, called n-dimensional complex projective space. Topologize them as thequotient $(\mathbb{R}^{n+1} \setminus \{0\})/\mathbb{R}^*$ and $(\mathbb{C}^{n+1} \setminus \{0\})/\mathbb{C}^*$. Then $\mathbb{RP}^n$ is an n-manifold, $\mathbb{CP}^n$ is a $2n$-manifold.

Example 1.12.15. Let X be the subset $(\mathbb{R} \times \{0\} \cup (\mathbb{R} \times \{1\} \subseteq \mathbb{R}^2$. Define an equivalence relation on X by declaring $(x, 0) \sim (x, 1)$ if $x \neq 0$. Show that the quotient space $X/\sim$ is locally Euclidean and second countable, but not Hausdorff. (This space is called the **line with two origins**)

Example 1.12.16. Consider the product $\mathbb{R}^d \times \mathbb{R}$, where $\mathbb{R}^d$ means $\mathbb{R}$ with discrete topology. This space is Huasdorff and Locally Euclidean, but not second countable.

1.12.3 Adjunction spaces

Definition 1.12.17. *Suppose X and Y are topological spaces, A is a closed subspace of Y , and $f : A \to X$ is a continuous map. Let $\sim$ bethe equivalence relation on the disjoint union $X \amalg Y$ generated by $a \sim f(a)$ for all $a \in A$, and denote the resulting quotient space by*

$$X \cup_f Y := (X \amalg Y)/\sim$$

*Any such quotient space is called an **adjunction space**, and is said to be formed by attaching Y to X along f. The map f is called the attaching map. Note that the equivalence relation identifies each point $x \in X$ with all of the points (if any) in $f^{-1}(x) \in A$. If $A = \varnothing$, then $X \cup_f Y$ is just the disjoint union space $X \amalg Y$.*

Theorem 1.12.18. *Let $X \cup_f Y$ be an adjunction space, and let $q : X \amalg Y \to X \cup_f Y$ be the associated quotient map.*

(a) The restriction of q to X is a topological embedding, whose image set $q(X)$ is a closed subspace of $X \cup_f Y$.

(b) The restriction of q to $Y \setminus A$ is a topological embedding, whose image set $q(Y \setminus A)$ is an open subspace of $X \cup_f Y$.

(c) $X \cup_f Y$ is the disjoint union of $q(X)$ and $q(Y \setminus A)$.

Proof. We begin by showing that $q|_X$ is a closed map. Suppose that B is a closed subset of X. To show that $q(B)$ is closed in the quotient space, we need to show that $q^{-1}(q(B))$ is closed in $X \amalg Y$, which is equivalent to showing that its intersections with X and Y are closed in X and Y, respectively. From the form of the equivalence relation, it follows that $q^{-1}(q(B)) \cap X = B$, which is closed in X by assumption; and $q^{-1}(q(B)) = f^{-1}(B)$, which is closed in A by the continuity of f, and thus is closed in Y because A is closed in Y. It follows, in particular, that $q(X)$ is closed in $X \cup_f Y$.

Now $q|_X$ is clearly injective because the equivalence relation does not identify any points in X with each other. Because it is also closed, it is a topological embedding. This proves (a).

To prove (b), we just note that $Y \setminus A$ is a saturated open subset of $X \amalg Y$, so the restriction $q|_{Y\setminus A}$ is a quotient map, and since it is bijective it is a homeomorphism. Its image is open in $X \cup_f Y$ by definition of the quotient topology. Finally, part (c) is an easy consequence of the definition of the equivalence relation. □

Because of the preceding proposition, one typically identifies X with $q(X)$ and $Y \setminus A$ with $q(X \setminus A)$, considering each as a subspace of the adjunction space.

Example 1.12.19 (Adjunction Spaces).

(a) Suppose X and Y are topological spaces with chosen base points $x \in X$ and $y \in Y$. Let $A = \{y\} \subseteq Y$, and define $f : A \to X$ by $f(y) = x$. Then the adjunction space $X \cup_f Y$ is just the wedge sum $X \wedge Y$.

(b) Let $A = S^1 \subseteq \overline{B}^2$, and let $f : A \to \overline{B}^2$ be the inclusion map. Then the adjunction space is homeomorphic to S^2.

Suppose M and N are n-dimensional manifolds with nonempty boundaries, such that ∂M and ∂N are homeomorphic. Let $h : \partial N \to \partial M$ be a homeomorphism. Assuming the theorem on the invariance of the boundary, we conclude that ∂N is a closed subset of N, so we can define the adjunction space $M \cup_h N$ (considering h as a map into M). This space is said to be formed by **attaching M and N together along their boundaries**.

Theorem 1.12.20. *With M, N, and h as above, $M \cup_h N$ is an n-manifold (without boundary). There are topological embeddings $e : M \to M \cup_h N$ and $f : N \to M \cup_h N$ whose images are closed subsets of $M \cup_h N$ satisfying*

$$e(M) \cup f(N) = M \cup_h N, \quad e(M) \cap f(N) = e(\partial M) = f(\partial N).$$

Proof. First we need to show that $M \cup_h N$ is locally Euclidean of dimension n. Let $q : M \amalg N \to M \cup_h N$ denote the quotient map, and write $S = q(\partial M \cup \partial N)$. Note that $\operatorname{Int} M \amalg \operatorname{Int} N$ is a saturated open subset of $M \amalg N$, and therefore q restricts to a quotient map from $\operatorname{Int} M \amalg \operatorname{Int} N$ onto $(M \cup_h N) \setminus S$. Because this restriction is injective, it is a homeomorphism, and thus $(M \cup_h N) \setminus S$ is locally Euclidean of dimension n. Thus we need only consider points in S.

Suppose $s \in S$, and let $y \in \partial N$ and $x = h(y) \in \partial M$ be the two points in the fiber $q^{-1}(s)$. We can choose coordinate charts (U, φ) for M and (V, ψ) for N such that $x \in U$ and $y \in V$, and let $\widehat{U} = \varphi(U)$, $\widehat{V} = \psi(V)$. It is useful in this proof to identify $\mathbb{H}^n$ with $\mathbb{R}^{n-1} \times [0, +\infty)$ and $\mathbb{R}^n$ with $\mathbb{R}^{n-1} \times \mathbb{R}$. By shrinking U and V if necessary, we may assume that $h(V \cap \partial N) = U \cap \partial M$, and that $\widehat{U} = U_0 \times [0, \varepsilon)$ and $\widehat{V} = V_0 \times [0, \varepsilon)$ for some $\varepsilon > 0$ and some open subsets $U_0, V_0 \subseteq \mathbb{R}^{n-1}$. Then we can write the coordinate maps as

$$\varphi(x) = (\varphi_0(x), \varphi_1(x)), \quad \psi(y) = (\psi_0(y), \psi_1(y))$$

for some continuous maps $\varphi_0 : U \to U_0$, $\varphi_1 : U \to [0, \varepsilon)$, $\psi_0 : V \to V_0$ and $\psi_1 : V \to [0, \varepsilon)$. Our assumption that x and y are boundary points means that $\varphi_1(x) = \psi_1(y) = 0$.

Figure 12.3.1: Attaching along boundaries.

We wish to assemble these two charts into a map whose image is an open subset of $\mathbb{R}^n$, by matching them up along corresponding points in ∂M and ∂N. As they stand, however, the maps φ and might not take corresponding boundary points to the same image point, so we need to adjust for that. Both of the restrictions

$$\varphi_0|_{U\cap\partial M} : U \cap \partial M \to U_0, \quad \psi_0|_{V\cap\partial N} : V \cap \partial N \to V_0$$

are homeomorphisms. Define a homeomorphism $\tau : V_0 \to U_0$ by

$$\tau = (\varphi_0|_{U\cap\partial M}) \circ h \circ (\psi_0|_{V\cap\partial N})^{-1},$$

and let $B : \widehat{V} \to \mathbb{R}^n$ be the map

$$B(x_1, \ldots, x_n) = (\tau(x_1, \ldots, x_{n-1}), -x_n).$$

Geometrically, B rearranges the boundary points according to the map τ, and then "flips" each vertical line segment above a boundary point to a line segment below the image point. Our construction ensures that for $y \in \partial N$,

$$B \circ \psi(y) = (\tau \circ \psi(y), 0) = (\varphi_0 \circ h(y), 0) = \varphi \circ h(y). \tag{12.3.1}$$

Now define $\widetilde{\Phi} : U \amalg V \to \mathbb{R}^n$ by

$$\widetilde{\Phi} = \begin{cases} \varphi(y), & y \in U; \\ B \circ \psi(y), & y \in V. \end{cases}$$

Because $U \amalg V$ is a saturated open subset of $M \amalg N$, the restriction of q to it is a quotient map onto the neighborhood $q(U \amalg V)$ of s, and (12.3.1) shows that $\widetilde{\Phi}$ passes to the quotient and defines an injective continuous map $\Phi : q(U \amalg V) \to \mathbb{R}^n$. Since φ, ψ, and B are homeomorphisms onto their images, we can define an inverse for Φ as follows:

$$\Phi^{-1}(y) = \begin{cases} q \circ \varphi^{-1}(y), & y^n \geq 0; \\ q \circ \psi^{-1} \circ B^{-1}(y) & y^n \leq 0. \end{cases}$$

These two definitions agree where they overlap, so the resulting map is continuous by the gluing lemma. Thus Φ is a homeomorphism. Note that the image of Φ is exactly $U_0 \times (-\varepsilon, \varepsilon)$, which is open in $\mathbb{R}^n$. Therefore $M \cup_h N$ is locally Euclidean of dimension n.

The quotient space $M \cup_h N$ is second countable by Proposition 1.12.5. To prove that it is Hausdorff, we need to show that the fibers of q can be separated by saturated open subsets. It is straightforward to check on a case-by-case base that the preimages of sufficiently small coordinate balls will do.

It follows immediately from Theorem 1.12.18(a) that the quotient map q restricts to a topological embedding of M into $M \cup_h N$ with closed image. On the other hand, because h is a homeomorphism, it is easy to see that $M \cup_h N$ is also equal to $N \cup_{h^{-1}} M$, so q also restricts to a topological embedding of N with closed image. The union of the images of these embeddings is all of $M \cup_h N$, and their intersection is the set S defined above, which is exactly the image of either boundary. □

Here is an important example of the preceding construction.

Example 1.12.21 (The Double of a Manifold with Boundary). Suppose M is an ndimensional manifold with boundary. If $h : \partial M \to \partial M$ is the identity map, the resulting quotient space $M \cup_h M$ is denoted by $D(M)$ and called the **double of M**. It can be visualized as the space obtained by attaching two copies of M to each other along their common boundary. (If $\partial M = \varnothing$, then $D(M)$ is just the disjoint union of two copies of M)

The following proposition is an immediate consequence of Theorem 1.12.20.

Proposition 1.12.22. *Every n-manifold with boundary is homeomorphic to a closed subset of an n-manifold without boundary.*

This construction can be used to extend many results about manifolds to manifolds with boundary. For example, any property that holds for all closed subsets of manifolds is also shared by manifolds with boundary.

1.13 Paracompactness

1.13.1 Paracompact spaces

Let X be a topological space. A collection $\mathcal{A}$ of subsets of X is said to be **locally finite** if each point of X has a neighborhood that intersects at most finitely many of the sets in $\mathcal{A}$. Given a cover $\mathcal{A}$ of X, another cover $\mathcal{B}$ is called a **refinement** of $\mathcal{A}$ if for each $B \in \mathcal{B}$ there exists some $A \in \mathcal{A}$ such that $B \subseteq A$. It is an **open refinement** if each $B \in \mathcal{B}$ is an open subset of X. (Note that every subcover of $\mathcal{A}$ is a refinement of $\mathcal{A}$, but a refinement is not in general a subcover, because a refinement does not need to be composed of sets that are elements of $\mathcal{A}$.)

Here are some elementary properties of local finiteness. Given a collection $\mathcal{A}$ of subsets of a topological space, let us use the notation $\overline{\mathcal{A}}$ to denote the collection of closures of sets in $\mathcal{A}$:

$$\overline{\mathcal{A}} := \{\overline{A} : A \in \mathcal{A}\}$$

Lemma 1.13.1. *Let X be a topological space and $\mathcal{A}$ be a collection of subsets of X. Then $\mathcal{A}$ is locally finite if and only $\overline{\mathcal{A}}$ is locally finite.*

Proof. If $\overline{\mathcal{A}}$ is locally finite, then it follows immediately that $\mathcal{A}$ is locally finite. Conversely, suppose $\mathcal{A}$ is locally finite. Given $x \in X$, let W be a neighborhood of x that intersects only finitely many of the sets in $\mathcal{A}$, say $A_1, \dots, A_n$. If W contains a point a in $\overline{A}$ for some $A \in \mathcal{A}$, then $W \cap A \neq \varnothing$ since a is a limit point of A. It then follows that A is one of the sets $A_1, \dots, A_n$, and therefore W can only intersects finitely many sets in $\overline{\mathcal{A}}$. □

Lemma 1.13.2. *If $\mathcal{A}$ is a locally finite collection of subsets of X, then*

$$\overline{\bigcup_{A \in \mathcal{A}} A} = \bigcup_{A \in \mathcal{A}} \overline{A}$$

Proof. The right-hand side is contained in the lefthand side even without the assumption of local finiteness, so we only prove the reverse containment. We will prove the contrapositive: assuming $x \in X$ is not an element of $\bigcup_{A \in \mathcal{A}} \overline{A}$, we show it is not an element of $\overline{\bigcup_{A \in \mathcal{A}} A}$ either. By Lemma 1.13.1, x has a neighborhood U that intersects only finitely many sets in $\overline{A}$, say $\overline{A}_1, \dots, \overline{A}_k$. Then $U \setminus (\overline{A}_1 \cap \cdots \cap \overline{A}_1)$ is a neighborhood of x that intersects none of the sets in $\mathcal{A}$, so $x \notin \overline{\bigcup_{A \in \mathcal{A}} A}$. □

Definition 1.13.3. *A space X is said to be **paracompact** if every open cover of X admits a locally finite open refinement. Every compact space is paracompact, because a finite subcover is a locally finite open refinement.*

Proposition 1.13.4. *A closed subspace of a paracompact space is paracompact.*

Proof. If A is a closed subspace of a paracompact space X, every open cover of A is of the form $\{U_\alpha\} \cap A$, where U_α are open in X. Add in the open set $X - A$, we get an open cover of X, thus using paracompactness of X we get the claim. □

A key topological fact about manifolds, as we show below, is that they are all paracompact. This is a consequence of second countability, and in fact is one of the most important reasons why second countability is included in the definition of manifolds. For spaces that are Hausdorff and locally Euclidean with countably many components, the two conditions are equivalent.

Before we prove that manifolds are paracompact, we need a preliminary result. If X is a topological space, a sequence $\{K_i\}_{i \in \mathbb{N}}$ of compact subsets of X is called an **exhaustion** of X by compact sets if $X = \bigcup_i K_i$ and $K_i \subseteq \operatorname{Int} K_{i+1}$ for each i.

Proposition 1.13.5. *A σ-compact locally compact Hausdorff space admits an exhaustion by compact sets.*

Proof. Since X is a σ-compact, there exists a sequence $\{K_i\}$ of compact subsets such that $X = \bigcup_i K_i$. Every compact subset of X has a precompact open neighborhood by Proposition 1.9.3. Thus we may take U_1 to be a precompact open neighborhood of K_1, and then, proceeding inductively, take U_n to be a precompact open neighborhood of $\overline{U}_{i-1} \cup K_i$. It follows that the sequence $\{U_i\}$ satisfies $K_i \subseteq U_i$ and $\overline{U}_i \subseteq U_{n+1}$. Let $\widetilde{K}_i = \overline{U}_i$, then $\{\widetilde{K}_i\}$ is a exhaustion of X by compact sets. □

Theorem 1.13.6. *Every σ-compact locally compact Hausdorff space is paracompact. In fact, given such a space X, an open cover $\mathcal{U}$ of X, and any base $\mathcal{B}$ for the topology of X, there exists a countable, locally finite open refinement of $\mathcal{U}$ consisting of elements of $\mathcal{B}$.*

Proof. Given $X, \mathcal{U}$ and $\mathcal{B}$, by Proposition 1.13.5, let $(K_i)_{i\in\mathbb{N}}$ be an exhaustion of X by compact sets. For each i, let

$$V_i = K_{i+1} \setminus \operatorname{Int} K_i, \quad W_i = \operatorname{Int} K_{i+2} \setminus K_{i-1}$$

where we interpret $K_i = \varnothing$ if $i < 1$. Then V_i is a compact set contained in the open subset W_i. For each $x \in V_i$, there is some $U_x \in \mathcal{U}$ containing x, and because $\mathcal{B}$ is a base, there exists $B_x \in \mathcal{B}$ such that $x \in B_x \subseteq U_x \cap W_i$. The collection of all such sets B_x as x ranges over V_i is an open cover of V_i, and thus has a finite subcover. The union of all such finite subcovers as i ranges over the positive integers is a countable open cover of M that refines $\mathcal{U}$. Because the finite subcover of V_i consists of sets contained in W_i, and $W_i \cap W_j \neq \varnothing$ only for $i-2 < j < i+2$, the resulting cover is locally finite. □

In view of the theorem, one may wonder the connection between paracompactness and σ-compactness for a locally Hausdorff space. The following theorem answers this question.

Theorem 1.13.7. *A locally compact Hausdorff space X is paracompact if and only if it is a disjoint union of open σ-compact subsets.*

Proof. Assume that X is paracompact. Using local compactness, cover the space with open precompact sets U_α. Using paracompactness we may assum this cover is locally finite. We shall inductively construct open precompact sets V_i. We start with $V_1 = U_\beta$ for some given β. If V_i has been defined then consider all the U_α which intersect $\overline{V}_i$: By compactness of $\overline{V}_i$ and the local finiteness of the cover, this set of U_α's is finite. Let V_{i+1} be the union of these U_α. Then $\overline{V}_{i+1}$ is the union of the closures of this finite set of U_α's and so it is compact. Also $\overline{V}_i \subseteq V_{i+1}$. Put $V = \bigcup_i V_i$, then V is open. By Lemma 1.13.2 $\overline{V}$ is the union of the closures of these U_α's. But by construction each of these closures is contained in some $\overline{V}_i \subseteq V_{i+1} \subseteq V$. Thus $V = \overline{V}$ is closed and by construction, is σ-compact. Now since V is closed and open, it is a connected component of X. Thus X is a disjoint union of open σ-compact subsets.

Conversely, assume that X is a union of σ-compact subsets. It is clear that a disjoint union of open paracompact spaces is paracompact, and so we may as well assume the space X to be σ-compact. Let $X = \bigcup_i C_i$ where the C_i are compact. We define an exhaustion of X by compact sets K_i.

- Let $K_1 = C_1$. To define K_2, for each point $x \in C_1$ we find by local compactness a precompact neighborhood U_x of x. Then the collection $\{U_x\}$ covers C_1, hence has a subcover $\{U_1^{(1)}, \dots, U_{i_1}^{(1)}\}$. We set

$$K_2 = C_2 \cup \bigcup_{j=1}^{i_1} \overline{U}_j^{(1)}$$

  so K_2 is compact and $K_1 \subseteq \operatorname{Int} K_2$.

- Assume the ascending compact sets $K_1, \dots, K_n$ are defined. Now by the same argument we find precompact sets $\{U_1^{(n)}, \dots, U_{i_n}^{(n)}\}$ covers K_n. Then we set

$$K_{n+1} = C_n \cup \bigcup_{j=1}^{i_n} \overline{U}_j^{(n)}$$

Now K_{n+1} is compact and $K_n \subseteq \operatorname{Int} K_{n+1}$. By induction we get the sequence $\{K_i\}$, and since each C_i is contained in K_i, we have $X = \bigcup_i K_i$.

Now with this exhaustion by compact sets, by arguing as in the proof of Theorem 1.13.6, we can show that X is paracompact. □

One feature of paracompact Hausdorff spaces is that they satisfy a strengthened version of the Hausdorff property. A topological space X is said to be **normal** if it is Hausdorff and for every pair of disjoint closed subsets $A, B \subseteq X$, there exist disjoint open subsets $U, V \subseteq X$ such that $A \subseteq U$ and $B \subseteq V$. Similarly, X is said to be **regular** if it is Hausdorff and for every closed subset $B \subseteq X$ and point $a \in B$, there exist disjoint open subsets $U, V \subseteq X$ such that $a \in U$ and $B \subseteq V$. Briefly, in normal spaces, closed subsets can be separated by open subsets; and in regular spaces, closed subsets can be separated from points by open subsets.

Lemma 1.13.8. *Let X be a Hausdorff space. Then X is normal if and only if it satisfies the following condition: whenever A is a closed subset of X and U is a neighborhood of A, there exists a neighborhood V of A such that $\overline{V} \subseteq U$.*

Proof. This is easily seen to be equivalent to the definition of normality by taking $B = U^c$. □

Theorem 1.13.9. *Every paracompact Hausdorff space is normal.*

Proof. Suppose X is a paracompact Hausdorff space, and let A and B be disjoint closed subsets of X. We begin with the special case in which $B = \{q\}$ is a singleton; in other words, we prove that X is regular.

For each $p \in A$, because X is Hausdorff there exist disjoint open subsets U_p andV_p such that $p \in U_p$ and $q \in V_p$. The collection $\{U_p : p \in A\} \cup \{X \setminus A\}$ is an open cover of X. By paracompactness, it has a locally finite open refinement $\mathcal{W}$. Each of the open subsets in $\mathcal{W}$ is contained either in U_p for some p, or in $X \setminus A$. Let $\mathcal{U}$ be the collection of all the sets in $\mathcal{W}$ that are contained in some U_p. Then $\mathcal{U}$ is still locally finite, and it is an open cover of A. Moreover, if $U \in \mathcal{U}$, then there is a neighborhood V_p of q disjoint from U, so $\overline{U}$ does not contain q.

Let $\mathfrak{U} = \bigcup_{U \in \mathcal{U}} U$, and $\mathfrak{V} = X \setminus \overline{\mathfrak{U}}$. Because $\mathcal{U}$ is locally finite, $\overline{\mathfrak{U}} = \bigcup_{U \in \mathcal{U}} \overline{U}$ by Lemma 1.13.2. Thus $q \notin \overline{\mathfrak{U}}$, so $\mathfrak{U}$ and $\mathfrak{V}$ are disjoint open subsets of X containing A and q, respectively. This completes the proof that X is regular. Next consider arbitrary disjoint closed subsets A and B. Exactly the same argument works in this case, using regularity in place of the Hausdorff condition. □

The following result is a nontrivial property about normal spaces.

Theorem 1.13.10 (Urysohn's Lemma). *Suppose X is a normal topological space. If $A, B \subseteq X$ are disjoint closed subsets, then there exists a continuous function $f : X \to [0, 1]$ such that $f|_A \equiv 0$ and $f|_B \equiv 1$.*

Proof. We will construct for each rational number r an open subset $U_r \subseteq X$, such that the following properties hold

(a) $U_r = \varnothing$ when $r < 0$, and $U_r = X$ when $r > 1$.

(b) $A \subseteq U_0$.

(c) $U_1 = X \setminus B$.

(d) If $p < q$, then $\overline{U}_p \subseteq U_q$

we will do this by induction. We begin by defining $U_1 = X \setminus B$, and defining U_r for $r \notin [0,1]$ by (a). By normality, there exists a neighborhood U_0 of A such that $\overline{U}_0 \subseteq U_1$. Let $\{r_i\}_{i\in\mathbb{N}}$ be a enumeration of the rationals in $[0,1]$. By normality again, there exists an open subset $U_{r_1} \subseteq X$ such that $\overline{U}_0 \subseteq U_{r_1}$ and $\overline{U}_{r_1} \subseteq U_1$. Now use induction, suppose U_i has been defined for $i = 1, \dots, n$ such that $\overline{U}_0 \subseteq U_{r_i}$, $\overline{U}_{r_i} \subseteq U_1$ and $\overline{U}_{r_i} \subseteq U_{r_j}$ for $r_i < r_j$. Consider the next rational number r_{n+1} in the sequence, and let p be the largest number in the set $\{0, r_1, \dots, r_n, 1\}$ that is smaller than r_{n+1}, and q the smallest number in the same set that is larger than r_{n+1}. Then $\overline{U}_p \subseteq U_q$ By normality, there exists an open subset $U_{r_{n+1}}$ such that $\overline{U}_p \subseteq U_{r_{n+1}}$ and $\overline{U}_{r_{n+1}} \subseteq U_q$. Continuing by induction, we obtain open subsets U_r for all rational r satisfying the properties above.

Now, define $f : X \to \mathbb{R}$ by

$$f(x) = \inf\{r \in \mathbb{Q} : x \subseteq U_r\}.$$

Because of (a), f is well defined and takes its values in $[0,1]$. Properties (a) and (b) imply that $f(x) = 0$ for $x \in A$, and (a) and (c) imply that $f(x) = 1$ for $x \in B$. Thus it remains only to show that f is continuous.

Because sets of the form (a, ∞) and $(-\infty, a)$ form a subbase for the topology of $\mathbb{R}$, it suffices to show that the preimage under f of any such set is open. We begin with the following observations:

$$f(x) < a \iff x \in U_r \text{ for some rational } r < a \tag{13.1.1}$$

$$f(x) \leq a \iff x \in \overline{U}_r \text{ for any rational } r > a \tag{13.1.2}$$

The equivalence (13.1.1) is an easy consequence of the definition of f. To prove (13.1.2), suppose first that $f(x) \leq a$. If r is any rational number greater than a, then by definition of f, there is a rational number $s < r$ such that $x \in U_s \subseteq U_r \subseteq \overline{U}_r$. Conversely, suppose $x \in \overline{U}_r$ for every rational number greater than a. If $s > a$ is rational, choose a rational number r such that $s > r > a$; it follows from our hypothesis that $x \in \overline{U}_r \subseteq U_s$, which implies that $f(x) \leq s$. Since this is true for every rationals $s > a$, it follows that $f(x) \leq a$.

From (13.1.1) and (13.1.2) we conclude that

$$f^{-1}\big((-\infty, a)\big) = \bigcup_{\substack{r\in\mathbb{Q}\\ r<a}} U_r, \quad f^{-1}\big((a, \infty)\big) = X \setminus \bigcap_{\substack{r\in\mathbb{Q}\\ r>a}} \overline{U}_r$$

both of which are open. Thus f is continuous. □

The next corollary of Urysohn's lemma is often the most useful. If X is a topological space and $f : X \to \mathbb{R}$ is a continuous function, the support of f, denoted by $\operatorname{supp}(f)$, is the closure of the set $\{x \in X : f(x) \neq 0\}$:

$$\operatorname{supp}(f) := \overline{\{x \in X : f(x) \neq 0\}}$$

If A is a closed subset of X and U is a neighborhood of A, a continuous function $f : X \to [0,1]$ such that $f|_A \equiv 1$ and $\operatorname{supp}(f) \subseteq U$ is called a **bump function** for A supported in U.

Theorem 1.13.11. *Let X be a normal space. If A is a closed subset of X and U is a neighborhood of A, there exists a bump function for A supported in U.*

Proof. Just apply Urysohn's Lemma with $B = X \setminus U$. □

One immediate consequence of the Urysohn lemma is the useful theorem called the Tietze extension theorem. It deals with the problem of extending a continuous realvalued function that is defined on a subspace of a space X to a continuous function defined on all of X. This theorem is important in many of the applications of topology.

Theorem 1.13.12 (**Tietze extension theorem**). *Let X be a normal space and A be a closed subspace of X.*

(a) Any continuous map of A into a closed interval $[a,b]$ may be extended to a continuous map of all of X into $[a,b]$.

(b) Any continuous map of A into $\mathbb{R}$ may be extended to a continuous map of all of X into $\mathbb{R}$.

Proof. We first prove (a). The idea of the proof is to construct a sequence of continuous functions g_n defined on the entire space X, such that the sequence g_n converges uniformly, and such that the restriction of g_n to A approximates f more and more closely as n becomes large. Then the limit function will be continuous, and its restriction to A will equal f.

Without loss of generality, we may assume that $[a,b] = [0,1]$. We claim that there is a sequence $\{g_n : X \to [0, 2^{n-1}/3^n]\}$ of continuous functions such that $0 \le f - \sum_{i=1}^n g_i \le 2^{n-1}/3^n$ on A. To begin with, let $B = f^{-1}([0,1/3])$ and $C = f^{-1}([2/3,1])$. These are closed subsets of A, and since A itself is closed, they are closed in X. By Urysohn's lemma there is a continuous $g_1 : X \to [0,1/3]$ with $g_1 = 0$ on B and $g_1 = 1/3$ on C; it follows that $0 \le f - g_1 \le 2/3$ on A. In general, having found $g_1, \dots, g_{n-1}$, by the same reasoning we can find $g_n : X \to [0, 2^{n-1}/3^n]$ such that $g_n = 0$ on the set where $f - \sum_{i=1}^{n-1} g_i \le 2^{n-1}/3^n$ and $g_n = 2^{n-1}/3^n$ on the set where $f - \sum_{i=1}^{n-1} g_i \ge (2/3)^n$. Let $F = \sum_{n=1}^\infty g_n$. Since $|g_n| \le 2^{n-1}/3^n$, the partial sums of this series converge uniformly, so F is continuous. Moreover, on A we have $0 < f - F < (2/3)^n$ for all n, whence $F = f$ on A.

We now prove part (b) of the theorem, in which f maps A into $\mathbb{R}$. We can replace $\mathbb{R}$ by the open interval $(0,1)$, since this interval is homeomorphic to $\mathbb{R}$. So let f be a continuous map from A into $(0,1)$. The half of the Tietze theorem already proved shows that we can extend f to a continuous map $F : X \to [0,1]$ mapping X into the closed interval. Let us define a subset D of X by the equation

$$D = F^{-1}(0) \cup F^{-1}(1).$$

Since F is continuous, D is a closed subset of X. Because $F(A) = f(A)$, which is contained in $(0,1)$, the set A is disjoint from D. By the Urysohn lemma, there is a continuous function $\phi : X \to [0,1]$ such that $\phi(D) = \{0\}$ and $\phi(A) = \{1\}$. Define

$$\widetilde{F} = F(x)\phi(x).$$

Then $\widetilde{F}$ is continuous, being the product of two continuous functions. Also, $\widetilde{F}$ is an extension of F with values in $(0,1)$. This finishes the proof. □

1.13.2 Partitions of unity

The applications of paracompactness are all based on a technical tool called a partition of unity, which can be used to blend together locally defined continuous maps into a global one.

For this purpose, we need to consider open covers indexed by some set. (Of course any open cover $\mathcal{U}$ can be considered as an indexed family, just by taking the index set to be $\mathcal{U}$ itself.) In this context, an indexed family $\mathcal{U} = (U_\alpha)_{\alpha\in A}$ of subsets of a topological space X is said to be a **locally finite** family if each point of X has a neighborhood that intersects U_α for at most finitely many values of α.

If $\mathcal{U} = (U_\alpha)_{\alpha\in A}$ is an indexed open cover of X, a **partition of unity** subordinate to $\mathcal{U}$ is a family of continuous functions $\psi_\alpha : X \to \mathbb{R}$, indexed by the same set A, with the following properties:

(i) $0 \le \psi_\alpha(x) \le 1$ for all $\alpha \in A$ and all $x \in X$.

(ii) $\operatorname{supp}(\psi_\alpha) \subseteq U_\alpha$.

(iii) The family of supports $\{\operatorname{supp}(\psi_\alpha)\}_\alpha \in A$ is locally finite.

(iv) $\sum_{\alpha\in A} \psi_\alpha(x) = 1$ for all $x \in X$.

Because of the local finiteness condition (iii), the sum in (iv) has only finitely many nonzero terms in a neighborhood of each point, so there is no issue of convergence.

First we have a simple observation.

Proposition 1.13.13. *Suppose X is a topological space with the property that for every indexed open cover $\mathcal{U}$ of X, there exists a partition of unity subordinate to $\mathcal{U}$. Then X is paracompact.*

Proof. Let $\mathcal{U} = \{U_\alpha\}_{\alpha\in A}$ be any cover of X, and $\{\psi_\alpha\}_{\alpha\in A}$. Then since $\sum_{\alpha\in A} \psi_\alpha = 1$, the collection $\{\operatorname{supp}(\psi_\alpha)\}_{\alpha\in A}$ covers X. Moreover, by definition this collection is a locally finite refinement of $\mathcal{U}$. Thus X is paracompact. □

Now we want to prove the converse of Proposition 1.13.13. First we need some lemmas.

Lemma 1.13.14. *Suppose X is a paracompact Hausdorff space. If $\mathcal{U} = (U_\alpha)_{\alpha\in A}$ is an indexed open cover of X, then $\mathcal{U}$ admits a locally finite open refinement $\mathcal{V} = (V_\alpha)_{\alpha\in A}$ indexed by the same set, such that $\overline{V}_\alpha \subseteq U_\alpha$ for each α.*

Proof. By Lemma 1.13.8 and Theorem 1.13.9, each $x \in X$ has a neighborhood Y_x such that $\overline{Y}_x \subseteq U_\alpha$ for some $\alpha \in A$. Since X is paracompact, the open cover $\{Y_x : x \in X\}$ has a locally finite open refinement. Let us index this refinement by some set B, and denote it by $\mathcal{Z} = (Z_\beta)_{\beta\in B}$. For each β,there is some $x \in X$ such that $Z_\beta \subseteq Y_x$, and therefore there is some $\alpha \in A$ such that $\overline{Z}_\beta \subseteq \overline{Y}_x \subseteq U_\alpha$. Define a function $a : B \to A$ by choosing some such index $\alpha \in A$ for each $\beta \in B$, and setting $a(\beta) = \alpha$.

For each $\alpha \in A$, define an open subset $V_\alpha \subseteq X$ by

$$V_\alpha = \bigcup_{a(\beta)=\alpha} Z_\beta$$

(If there are no indices β such that $a(\beta) = \alpha$, then $V_\beta = \varnothing$.) Because the family $\mathcal{Z}$ is locally finite, the closure of V_α is equal to $\bigcup_{a(\beta)=\alpha} \overline{Z}_\beta$ by Lemma 1.13.2, which is contained in U_α as required. □

Theorem 1.13.15 (Existence of Partitions of Unity). *Let X be a paracompact Hausdorff space. If $\mathcal{U}$ is any indexed open cover of X, then there is a partition of unity subordinate to $\mathcal{U}$.*

Proof. Let $\mathcal{U} = (U_\alpha)_{\alpha\in A}$ be an indexed open cover of X. Apply Lemma 1.13.14 twice, we obtain locally finite open covers $\mathcal{V} = (V_\alpha)_{\alpha\in A}$ and $\mathcal{W} = (W_\alpha)_{\alpha\in A}$ such that $\overline{W}_\alpha \subseteq V_\alpha$ and $\overline{V}_\alpha \subseteq U_\alpha$.

Now, for each $\alpha \in A$, let $f_\alpha : X \to [0,1]$ be a bump function for $\overline{W}_\alpha$ supported in V_α. Define $f : X \to \mathbb{R}$ by $f(x) = \sum_\alpha f_\alpha(x)$. Because $\operatorname{supp}(f_\alpha) \subseteq V_\alpha$, the family of supports $\{\operatorname{supp}(f_\alpha)\}_{\alpha\in A}$ is locally finite; thus each point of X has a neighborhood on which only finitely many terms of this sum are nonzero, so f is continuous. Because the sets $\{W_\alpha\}$ cover X, for each $x \in X$ there is at least one α such that $x \in W_\alpha$ andthus $f_\alpha(x) = 1$, so f is everywhere positive. Therefore, we can define

$$\psi_\alpha(x) = \frac{f_\alpha(x)}{f(x)}$$

Then $\{\psi_\alpha\}_{\alpha\in A}$ is the desired partition of unity, as one may check. □

Theorem 1.13.16 (Embeddability of Compact Manifolds). *Every compact manifold is homeomorphic to a subset of some Euclidean space.*

Proof. Suppose M is a compact n-manifold. By compactness we can obtain a cover of M by finitely many open subsets $U_1, \dots, U_k$, each of which is homeomorphic to $\mathbb{R}^n$. For each i, let $\varphi_i : U_i \to \mathbb{R}^n$ be a homeomorphism. Let $\{\psi_i\}$ be a partition of unity subordinate to this cover, and define functions $F_i : M \to \mathbb{R}^n$ by

$$F_i(x) = \begin{cases} \psi_i(x)\varphi_i(x), & x \in U_i \\ 0, & x \in M \setminus \operatorname{supp}(\psi_i) \end{cases}$$

Each F_i is continuous by the pasting lemma.

Now define $F : M \to \mathbb{R}^{nk+k}$ by

$$F(x) = \big(F_1(x), \dots, F_k(x), \psi_1(x), \dots, \psi_k(x)\big)$$

Then F is continuous, and if we can show it is injective, it is a topological embedding by the closed map lemma.

Suppose $F(x) = F(y)$ for some points $x, y \in M$. Since $\sum_i \psi_i(x) \equiv 1$, there is some i such that $\psi_i(x) > 0$ and therefore $x \in U_i$. Because $F(x) = F(y)$ implies $\psi_i(y) = \psi_i(x) > 0$, it follows that $y \in U_i$ as well. Then we see that $F_i(x) = F_i(y)$ implies $\varphi_i(x) = \varphi_i(y)$, which in turn implies that $x = y$ since φ_i is injective on U_i. □

Theorem 1.13.17. *Suppose M is a topological manifold, and $B \subseteq M$ is any closed subset. Then there exists a continuous function $f : M \to [0,\infty)$ whose zero set is exactly B.*

Proof. First, consider the special case in which $M = \mathbb{R}^n$ and $B \subseteq \mathbb{R}^n$ is a closed subset. It is straightforward to check that

$$u(x) = \inf\{|x - y| : y \in B\}$$

does the trick.

Now, let M be an arbitrary n-manifold and let B be a closed subset of M. Let $\mathcal{U} = (u_\alpha)_{\alpha\in A}$ be a cover of M by open subsets homeomorphic to $\mathbb{R}^n$, and let $\{\psi_\alpha\}_{\alpha\in A}$ be a subordinate partition

of unity. For each ψ_α the construction in the preceding paragraph yields a continuous function $u_\alpha : U_\alpha \to [0, \infty)$ such that $u_\alpha^{-1}(0) = B \cap U_\alpha$. Define $f : M \to \mathbb{R}$ by

$$f(x) = \sum_{\alpha \in A} \psi_\alpha(x) u_\alpha(x)$$

where each summand is to be interpreted as zero outside the support of ψ_α. Each term in this sum is continuous by the pasting lemma, and only finitely many terms are nonzero in a neighborhood of each point, so this defines a continuous function on M. It is easy to check that it is zero exactly on B. □

Corollary 1.13.18. *Suppose M is a topological manifold, and A, B are disjoint closed subsets of M. Then there exists a continuous function $f : M \to [0, 1]$ such that*

$$f^{-1}(0) = A, \quad f^{-1}(1) = B$$

Proof. Using the previous theorem, we can find $u, v : M \to [0, \infty)$ such that u vanishes exactly on A and v vanishes exactly on B, and then the function $f(x) = v(x)/\big(u(x) + v(x)\big)$ satisfies the conclusion of the corollary. □

For our last application of partitions of unity, we need the following definition. If M is a topological space, an **exhaustion function** for M is a continuous function $f : M \to \mathbb{R}$ such that for every $c \in \mathbb{R}$, the sublevel set $f^{-1}\big((-\infty, c]\big)$ is compact. The name comes from the fact that as k ranges through the positive integers, the sublevel sets $f^{-1}\big((-\infty, k]\big)$ form an exhaustion of M by compact sets.

Theorem 1.13.19. *Every manifold admits a positive exhaustion function.*

Proof. Let M be a manifold, let $\{U_i\}$ be a countable open cover of M by precompact open subsets, and let $\{\psi_i\}$ be a partition of unity subordinate to this cover. Define $f : M \to \mathbb{R}$ by

$$f(x) = \sum_{k=1}^{\infty} k \psi_k(x)$$

Then f is continuous since only finite terms are nonzero in a neighborhood of each point, and positive because $f(x) \geq \sum_k \psi_k(x) = 1$. For any positive integer m, if $x \notin \bigcup_{k=1}^m \overline{U}_k$, then $\psi_k(x) = 0$ for $1 \leq k \leq m$, so

$$f(x) = \sum_{k=m+1}^{\infty} k\psi_k(x) > \sum_{k=m+1}^{\infty} m\psi_k(x) = m \sum_{k=m+1}^{\infty} \psi_k(x) = m$$

The contrapositive of this last statement is that $f(x) \leq m$ implies $x \in \bigcup_{k=1}^m \overline{U}_k$. Let $c \in \mathbb{R}$ be arbitrary, and let m be any positive integer greater that c. It follows that $f^{-1}\big((-\infty, c]\big)$ is a closed subset of the compact set $\bigcup_{k=1}^m \overline{U}_k$, and is therefore compact. □

Chapter 2

Uniform structures

2.1 Uniform spaces

Definition 2.1.1. *A **uniform structure** (or **uniformity**) on a set X is a structure given by a set $\mathfrak{U}$ of subsets of $X \times X$ whick satisfies the following axioms:*

(F1) If $U \in \mathfrak{U}$ and $U \subseteq V \subseteq X \times X$, then $V \in \mathfrak{U}$.

(F2) If $U \in \mathfrak{U}$ and $V \in \mathfrak{U}$, then $U \cap V \in \mathfrak{U}$.

(U1) Every set in $\mathfrak{U}$ contains the diagonal Δ.

*(U2) If $U \in \mathfrak{U}$ then $U^{-1} \in \mathfrak{U}$, where $U^{-1} := \{(y, x) : (x, y) \in U\}$ is the **inverse** of U.*

(U3) If $U \in \mathfrak{U}$ then there is $V \in \mathfrak{U}$ such that $V \circ V \subseteq U$, where the composite of two sets $V, W \subseteq X \times X$ is defined by

$$V \circ W := \{(x, z) : \textit{there exists } y \in X \textit{ such that } (x, y) \in V \textit{ and } (y, z) \in W\}.$$

*The sets of $\mathfrak{U}$ are called **entourages** of the uniformity defined on X by $\mathfrak{U}$. A set endowed with a uniformity is called a **uniform space**.*

If U is an entourage of a uniformity on X, we may express the relation $(x, y) \in U$ by saying that "x and y are U**-close**". Note that if X is nonempty then every set in $\mathfrak{U}$ is nonempty by (U1), and (F1) and (F2) impliy that $\mathfrak{U}$ is a filter on $X \times X$. There is only one uniformity on the empty set, namely $\{\varnothing\}$.

Throughout this part we shall also write V^2 instead of $V \circ V$, and in general $V^n = V \circ V^{n-1} = V^{n-1} \circ V$, for each integer $n > 1$ and each subset $V \subseteq X \times X$.

Lemma 2.1.2. *The conjunction of axioms (U2) and (U3) is equivalent (assuming the other axioms of uniform structures) to the following axiom:*

(U2′) For each $U \in \mathfrak{U}$ there exists $V \in \mathfrak{U}$ such that $V \circ V^{-1} \subseteq U$.

Proof. Clearly (U2) and (U3) imply (U2′). Conversely, if (U2′) is satisfied, then for every $U \in \mathfrak{U}$, there exists $V \in \mathfrak{U}$ such that $V \circ V^{-1} \subseteq U$, and so

$$V^{-1} = \Delta \circ V^{-1} \subseteq V \circ V^{-1} \subseteq U,$$

thus $V \subseteq U^{-1}$ and by (F1) we have $U^{-1} \in \mathfrak{U}$. This proves (U2). Let $W = V \cap V^{-1}$; then $W \in \mathfrak{U}$ by what we have just proved and (F2), and we have $W \circ W \subseteq V \circ V^{-1} \subseteq U$. □

Example 2.1.3. Let (X, d) be a metric space. Then a uniformity on X is given by subsets of the form

$$U_\varepsilon = \{(x, y) : d(x, y) < \varepsilon\}.$$

In this case, x and y are U_ε-close precisely when the distance between x and y is at most ε.

A **base** or **fundamental system** of entourages of a uniformity $\mathfrak{U}$ is any set $\mathfrak{B}$ of entourages such that every entourage contains a set belonging to $\mathfrak{B}$.

Example 2.1.4. Axiom (U3) shows that if n is any positive integer and V runs through a fundamental system of entourages, then the sets V^n (n times) again form a undamental system of entourages.

Entourages V such that $V = V^{-1}$ are called **symmetric**. If V is any entourage then $V \cap V^{-1}$ and $V \cup V^{-1}$ are symmetric entourages, and axioms (F2) and (U2) show that the symmetric entourages form a fundamental system of entourages.

Proposition 2.1.5. *A set $\mathfrak{B}$ of subsets of $X \times X$ is a fundamental system of entourages of a uniformity $\mathfrak{U}$ on X if and only if $\mathfrak{B}$ is a filterbase and satisfies the following axioms:*

(B1) Every set in $\mathfrak{B}$ contains the diagonal.

(B2) For every $V \in \mathfrak{B}$ there exists $W \in \mathfrak{B}$ such that $W \subseteq V^{-1}$.

(B3) For every $V \in \mathfrak{B}$ there exists $W \in \mathfrak{B}$ such that $W \circ W \subseteq V$.

Proof. If $\mathfrak{B}$ is a base for a uniformity $\mathfrak{U}$, then $\mathfrak{B}$ clearly satisfies the claimed properties. Conversely, assume the properties for $\mathfrak{B}$, and let $\mathfrak{U}$ be the filter in $X \times X$ generated by $\mathfrak{B}$. We prove that $\mathfrak{U}$ is a uniformity.

First, since $\mathfrak{U}$ is a filter, it satisfies (F1) and (F2). Also, by (B1) we see (U1) is satisfies. Now let $U \in \mathfrak{U}$, then $U \supseteq V$ for some $V \in \mathfrak{B}$. By (B2), there exists $W \in \mathfrak{U}$ such that $W \subseteq V^{-1} \subseteq U^{-1}$. Thus $U^{-1} \in \mathfrak{U}$ and (U2) holds. Also, by (B3) there also exists $W' \in \mathfrak{B}$ such that $W' \circ W' \subseteq V \subseteq U$. Since $W' \in \mathfrak{U}$, we see (U3) also holds. This completes the proof. □

Example 2.1.6. Let X be a set and R be an equivalence relation on X. Let $\Gamma \subseteq X \times X$ be the graph of R. Then $\Delta \subseteq \Gamma$ and $\Gamma \circ \Gamma = \Gamma^{-1} = \Gamma$. The set of subsets of $X \times X$ which consists of the set C alone is therefore a fundamental system of entourages of a uniformity on X. In particular, if we take R to be the relation of equality, then $C = \Delta$ and the entourages of the corresponding uniformity are all the subsets of $X \times X$ which contain Δ; this uniformity is called the **discrete uniformity** on X, and the set X endowed with this uniformity is called a **discrete uniform space**.

Example 2.1.7. On the set $\mathbb{Z}$ of rational integers we can define a uniformity, important in the theory of numbers, as follows: given a prime number p, let U_n be the set of all pairs $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ such that $x \equiv y \bmod p^n$, for each positive integer n. It is easily verified that the sets U_n (for a fixed p) form a fundamental system of entourages of a uniformity on $\mathbb{Z}$, called the ***p*-adic uniformity**.

Now let X and Y be two sets each endowed with uniformities whose sets of entourages are $\mathfrak{U}$ and $\mathfrak{V}$ respectively, then a bijection f of X onto Y is an isomorphism of the uniformity of X onto that of Y if $(f \times f)(\mathfrak{U}) = \mathfrak{V}$.

Now we define the topology induced by a uniformity.

Proposition 2.1.8. *Let X be a set endowed with a uniform structure $\mathfrak{U}$, and for each $x \in X$ let $\mathfrak{U}(x)$ be the set of subsets $U(x)$ of X, where*

$$U(x) = \{y \in X : (x, y) \in V\}$$

and U runs through the set of entourages of $\mathfrak{U}$. Then there is a unique topology on X such that, for each $x \in X$, $\mathfrak{U}(x)$ is the neighbourhood filter of x in this topology.

Proof. We have to show that the $\mathfrak{U}(x)$ satisfy conditions of Proposition 1.1.18. In view of the axoims of uniformity, we only need to prove (U4). To see this, let V be an entourage of $\mathfrak{U}$, W an entourage of $\mathfrak{U}$ such that $W \circ W \subseteq V$; then if $(x, y) \in W$ and $(y, z) \in W$ we have $(x, z) \in V$, so that $W(y) \subseteq V(x)$ for all $y \in W(x)$, and therefore $V(x) \in \mathfrak{U}(y)$ for all $y \in W(x)$. This completes the proof. □

The topology defined in Proposition 2.1.8 is called the **topology induced by the uniform structure** $\mathfrak{U}$.

Example 2.1.9. The topology induced by the additive uniformity on the set of real numbers is the topology of the real line. On any set X, the topology induced by the discrete uniformity is the discrete topology. The topology induced by the p-adic uniformity is the p-adic topology on $\mathbb{Z}$.

In the future, when we speak of the topology of a uniform space X, we shall always mean the topology induced by the uniform structure of the space, unless the contrary is expressly stated. The topological space obtained by putting this topology on the set X is sometimes called the topological space *underlying* the uniform space in question. For example, when we say that a uniform space is Hausdorff, or compact, or locally compact, etc., we mean that the underlying topological space has this property.

If X and Y are two uniform spaces, any isomorphism f of the uniform structure of X onto that of Y is also a homeomorphism of X onto Y; we say that f is an **isomorphism** of the uniform space X onto the uniform space Y. It should be noted that a homeomorphism of X onto Y is not necessarily an isomorphism of the uniform structure of X onto that of Y. In other words, distinct uniformities on the same set X can induce the same topology. For example, on $(0, +\infty)$, the additive and the multiplicative uniformities (which are distinct) induce the same topology.

Proposition 2.1.10. *Let X be a uniform space. For every symmetric entourage V of X and every subset S of $X \times X$, $V \circ S \circ V$ is a neighbourhood of S in the product space $X \times X$, and the closure of S in this space is given by the formula*

$$\overline{S} = \bigcap_{V \in \mathfrak{S}} V \circ S \circ V \tag{1.0.1}$$

where $\mathfrak{S}$ denotes the set of symmetric entourages of X.

Proof. Let V be a symmetric entourage of X. The relation $(x, y) \in V \circ S \circ V$ means that there is an element (p, q) of S such that $(x, p) \in V$ and $(q, y) \in V$: in other words (V being symmetric) $x \in V(p)$ andy $y \in V(q)$, that is $(x, y) \in V(p) \times V(q)$. Since $V(p) \times V(q)$ is a neighbourhood of (p, q) in $X \times X$, the first part of the proposition is proved. The relations $(x, p) \in V$, $(y, q) \in V$ can also be written $p \in V(x)$, $q \in V(y)$, or $(p, q) \in V(x) \times V(y)$. As V runs through $\mathfrak{S}$, the sets $V(x) \times V(y)$ form a fundamental system of neighbourhoods of (x, y) in $X \times X$; for if U and V are any two entourages there is always a symmetric entourage $W \subseteq U \cap V$, so that $W(x) \times W(y) \subseteq U(x) \times V(y)$. Hence $V(x) \times V(y)$ meets S for each $V \in \mathfrak{S}$ if and only if $(x, y) \in \overline{S}$, and formula (1.0.1) follows. □

Corollary 2.1.11. *If A is any subset of X and V is any symmetric entourage of X, then $V(A)$ is a neighbourhood of A in X, and*

$$\overline{A} = \bigcap_{V \in \mathfrak{S}} V(A) = \bigcap_{V \in \mathfrak{U}} V(A) \tag{1.0.2}$$

where $\mathfrak{U}$ denotes the set of all entourages in X.

Proof. If $S = A \times A$, then $V \circ S \circ V = V(A) \times V(A)$ for any $V \in \mathfrak{S}$; for the relation "there exists $p \in A$ such that $(x, p) \in V$" is by definition equivalent to $x \in V(A)$. The corollary now follows from $\overline{S} = \overline{A} \times \overline{A}$. □

The set $V(A)$ in Corollary 2.1.11 is called the V**-neighborhood** of A. It should be remarked that as V runs through the set of entourages of X, the sets $V(A)$ do not necessarily form a fundamental system of neighbourhoods of A in X.

Example 2.1.12. On the real line $\mathbb{R}$, carrying the additive uniformity, as V runs through the filter of entourages of $\mathbb{R}$ the sets $V(\mathbb{Z})$ do not form a fundamental system of neighbourhoods of the set $\mathbb{Z}$ of rational integers: the set

$$\bigcup_{n \in \mathbb{Z}} (n - \frac{1}{2^{|n|+1}}, n + \frac{1}{2^{|n|+1}})$$

is a neighborhood of $\mathbb{Z}$, but it can not contain any $V(\mathbb{Z})$ with V an entourage of $\mathbb{R}$.

Corollary 2.1.13. *The interiors (resp. the closures) of the entourages of X in $X \times X$ form a fundamental system of entourages of X.*

Proof. If V is any entourage of X, there is a symmetric entourage W such that $W \circ W \circ W \subseteq V$; since $W \circ W \circ W$ is a neighbourhood of W (Propositionuniformity on product space closure char), the interior of V in $X \times X$ contains W and is therefore an entourage. Furthermore, we have $W \subseteq \overline{W} \circ W \circ W \subseteq V$ by Proposition 2.1.10, and hence V contains the closure of an entourage. □

Corollary 2.1.14. *Let X be a uniform space. Then the set of closed neighbourhoods of a point of X is a fundamental system of neighbourhoods of the point. Therefore, a Hausdorff uniform space is regular.*

Proof. If x is any point of X and V runs through the entourages of X which are closed in $X \times X$, then the sets $V(x)$ form a fundamental system of neighbourhoods of x in X by Corollary 2.1.13, and they are closed in X as sections of V. □

Proposition 2.1.15. *A uniform space X is Hausdoiff if and only if the intersection of all the entourages of its uniform structure is the diagonal Δ of $X \times X$. Every Hausdoiff uniform space is regular.*

Proof. We have seen that the closed entourages form a fundamental system of entourages; if their intersection is Δ, then Δ is closed in $X \times X$ and consequently X is Hausdorff. Conversely, if X is Hausdorff then for every point $(x, y) \in \Delta$, there is an entourage V of X such that $y \notin V(x)$, or equivalently $(x, y) \notin V$; hence Δ is the intersection of all the entourages. □

If a uniform space X is Hausdorff, we say that the uniform structure of X is Hausdorff. If $\mathfrak{B}$ is a fundamental system of entourages for this structure, then X is Hausdorff if and only if the intersection of all the sets of $\mathfrak{B}$ is Δ.

2.1.1 Uniformly continuous functions

Proposition 2.1.16. *Let X and Y be uniform spaces and $f : X \to Y$ be a map and $g = f \times f$. Then the following conditions are equivalent:*

(i) For each entourage V of Y, there exists an entourage U of X such that if $(x, y) \in U$ then $(f(x), f(y)) \in V$.

(ii) For each entourage V of Y, $g^{-1}(V)$ is an entourage of X.

*In the admissible case, we say f is **uniformly continuous**.*

Proof. Assume (i). Then we see $g^{-1}(V)$ contains the entourage U in (i), so it is an entourage of X. Conversely, if (ii) holds, then it follows from $g(g^{-1}(V)) \subseteq V$ that (i) holds. □

It follows from definition that a uniformly continuous function must be continuous. On the other hand, a continuous mapping of a uniform space X into a uniform space Y need not be uniformly continuous, as is shown by the example $x \mapsto x^3$, a homeomorphism of $\mathbb{R}$ onto itself, which is not uniformly continuous with respect to the additive uniformity

Example 2.1.17 (Examples of uniformly continuous maps).

(a) The identity mapping of a uniform space onto itself is uniformly continuous.

(b) A constant mapping of a uniform space into a uniform space is uniformly continuous.

(c) Every mapping of a discrete uniform space into a uniform space is uniformly continuous.

The following properties of uniformly continuous maps are immediate.

Proposition 2.1.18.

(a) If $f : X \to Y$ and $g : Y \to Z$ are two uniformly continuous maps, then $g \circ f : X \to Z$ is uniformly continuous.

(b) A bijection f of a uniform space X onto a uniform space Y is an isomorphism if and only if f and f^{-1} are uniformly continuous.

Proof. The first claim follows from the interpretation of uniformly continuity in Proposition 2.1.16(i), and part (b) follows from Proposition 2.1.16(ii). □

Proposition 2.1.18 shows that we can take as morphisms of uniform structures the uniformly continuous mappings; we shall always assume in the future that the morphisms have been so chosen. In accordance with the general definitions, this allows us to define an order relation on the set of uniformities on a given set X:

Definition 2.1.19. *If $\mathfrak{U}_1$ and $\mathfrak{U}_2$ are two uniform structures on the same set X, then $\mathfrak{U}_1$ is said to be **finer** than $\mathfrak{U}_2$ (and $\mathfrak{U}_2$ **coarser** than $\mathfrak{U}_1$) if the identity map $(X, \mathfrak{U}_1) \to (X, \mathfrak{U}_2)$ is uniformlY continuous.*

If $\mathfrak{U}_1$ is finer than $\mathfrak{U}_2$ and distinct from $\mathfrak{U}_2$ we say that $\mathfrak{U}_1$ is strictly finer than $\mathfrak{U}_2$ (and that $\mathfrak{U}_2$ is strictly coarser than $\mathfrak{U}_1$). Two uniformities are said to be comparable if one is finer than the other. By definition, the following results is clear.

Proposition 2.1.20.

(a) If $\mathfrak{U}_1$ and $\mathfrak{U}_2$ are two uniformities on a set X, then $\mathfrak{U}_1$ is finer than $\mathfrak{U}_2$ if and only if every entourage of $\mathfrak{U}_2$ is an entourage of $\mathfrak{U}_1$.

(b) Let $\mathfrak{U}_1$ and $\mathfrak{U}_2$ be two uniformities on a set X and suppose that $\mathfrak{U}_1$ is finer than $\mathfrak{U}_2$; then the topology induced by $\mathfrak{U}_1$ is finer than the topology induced by $\mathfrak{U}_2$.

It can happen that a uniformity $\mathfrak{U}$ is strictly finer than a uniformity $\mathfrak{U}'$, but that the two induced topologies are identical. The following example shows this:

Example 2.1.21. Let X be a nonempty set. For each finite partition $\omega = (A_i)_{i=1}^n$ of X, let V_ω denote

$$\bigcup_{i=1}^{n} (A_i \times A_i)$$

The sets V_ω then form a fundamental system of entourage of a uniformity $\mathfrak{U}$ on X. For if ω is any finite partition of X we have $\Delta \subseteq V_\omega$ and $V_\omega \circ V_\omega = V_\omega^{-1} = V_\omega$; and if $\beta = (B_j)$ and $\delta = (C_k)$ are two finite partitions of X, then those of the sets $B_j \cap C_k$ which are not empty form a finite partition ω of X, and we have $V_\omega \subseteq V_\beta \circ V_\delta$. The uniformity $\mathfrak{U}$ is called the uniformity of finite partitions on X. The topology induced by $\mathfrak{U}$ is the discrete topology, since for each $x \in X$ the sets $\{x\}$ and $\{x\}^c$ form a finite partition of X. Nevertheless, if X is infinite, it is clear that $\mathfrak{U}$ is strictly coarser than the discrete uniformity.

2.1.2 Construction of uniform structures

Proposition 2.1.22. *Let X be a set, $(Y_i)_{i\in I}$ be a family of uniform spaces. For each $i \in I$ let $f_i : X \to Y_i$ be a mapping of X into Y_i and put $g_i = f_i \times f_i$. Let $\mathfrak{B}$ be the set of all finite intersections*

$$U(V_{i_1}, \ldots, V_{i_n}) = \bigcap_{k=1}^{n} g_{i_k}^{-1}(V_{i_k})$$

where V_{i_k} is an entourage of Y_{i_k}. Then $\mathfrak{B}$ is a fundamental system of entourages of a uniformity $\mathfrak{U}$ on X which is the initial uniform structure on X with respect to the family (Y_i), and in particular $\mathfrak{U}$ is the coarsest uniformity on X for which all the mappings f_i are uniformly continuous.

Proof. It is immediately seen that $\mathfrak{B}$ is a filterbase satisfies axioms (B1). If $W_i = g_i^{-1}(V_i)$, then $W_i^{-1} = g_i^{-1}(V_i^{-1})$ and $W_i \circ W_i = g_i^{-1}(V_i \circ V_i)$; hence $\mathfrak{B}$ also satisfies axioms (B2) and (B3) and is

therefore a fundamental system of entourages of a uniformity $\mathfrak{U}$ on X. Furthermore, it follows immediately from the definition of $\mathfrak{U}$ that f_i is uniformly continuous for each index $i \in I$; hence $f_i \circ h$ is uniformly continuous for each $i \in I$ if h is. Conversely, suppose that $f_i \circ h$ is uniformly continuous for each $i \in I$, and consider a set $U(V_{i_1}, \dots, V_{i_n})$; by hypothesis, for each $1 \leq j \leq n$, there is an entourage W_k of Z such that the relation $(z, z') \in W_k$ implies $(f_{i_k}(h(z)), f_{i_k}(h(z'))) \in V_k$; if $W = \bigcap_{j=1}^{n} W_k$, then these n relations are simultaneously satisfied whenever z and z' are W-close, so that we have then $(h(z), h(z')) \in U(V_{i_1}, \dots, V_{i_n})$ and the proof is complete. □

Corollary 2.1.23. *The topology on X induced by the coarsest uniformity $\mathfrak{U}$, for which the f_i are uniformly continuous is also the coarsest topology for which the f_i are continuous.*

Proof. This is an immediate consequence of the definition of the neighbourhoods of a point in this latter topology. □

The general properties of initial structures imply in particular the following transitivity property:

Proposition 2.1.24. *Let X be a set, $(Z_\beta)_{\beta \in J}$ a family of uniform spaces, $(J_\alpha)_{\alpha \in I}$ a partition of J and $(Y_\alpha)_{\alpha \in I}$ a family of sets indexed by I. For each $\alpha \in I$, let g_α be a mapping of X into Y_α; and for each $\beta \in J_\alpha$, let $h_{\beta\alpha}$ be a mapping of Y_α into Z_β, and put $f_\beta = h_{\beta\alpha} \circ g_\alpha$.*

$$X \xrightarrow{g_\alpha} Y_\alpha \xrightarrow{h_{\beta\alpha}} Z_\beta$$

If each Y_α carries the initial uniform structure induced by $(h_{\beta\alpha})_{\beta \in J_\alpha}$ then the initial uniform structure on X induced by $(f_\beta)_{\beta \in J}$ is the same as the initial uniform structure induced by $(g_\alpha)_{\alpha \in I}$.

Let X be a set, Y a uniform space, f a mapping of X into Y. The coarsest uniformity $\mathfrak{U}$ on X for which f is uniformly continuous is called the **inverse image** under f of the uniform structure of Y. It follows from Proposition 2.1.22 that the inverse images under $g = f \times f$ of the entourages of Y form a fundamental system of entourages for $\mathfrak{U}$. The topology induced by $\mathfrak{U}$ is the inverse image under f of the topology of Y. Note that if $f : X \to Y$ is surjective, then the entourages of Y are the **direct images** under g of the entourages of X.

Let A be a subset of a uniform space X. The uniformity induced on A by the uniformity of X is the inverse image of the latter under the canonical injection $A \hookrightarrow X$. By Proposition 2.1.22, this is equivalent to the following definition:

Definition 2.1.25. *Let A be a subset oj a uniform space X. The uniformity on A whose set of entourages is the trace on $A \times A$ of the set of entourages of X is called the uniformity induced on A by the uniformity of X.*

The topology induced by the uniformity induced on A is. the same as the topology induced on A by the topology of X; the set A, together with the uniformity and the topology induced by those of X, is called a **uniform subspace** of X.

If A is a subset of a uniform space X and if $f : X \to Y$ is a uniformly continuous mapping, then the restriction $f|_A$ is a uniformly continuous mapping of A into Y. If $B \subseteq Y$ is such that $f(X) \subseteq B$, then the mapping of X into the uniform subspace B of Y, having the same graph as f, is again uniformly continuous.

Proposition 2.1.26. *Let A be a dense subset of a uniform space X. Then the closures in $X \times X$ of the entourages of the uniform subspace A form a fundamental system of entourages of X.*

Proof. First we note that, if U is open in X then for any subset B of X we have $U \cap \overline{B} \subseteq \overline{U \cap B}$. In fact, if $x \in U \cap \overline{B}$, then for any neighborhood V of x, $U \cap V$ is also a neighborhood of x and thus $U \cap V \cap B \neq \varnothing$ (since $x \in \overline{B}$). This implies $x \in \overline{U \cap B}$.

Now let V be an open entourage of A; it is the intersection of $A \times A$ with an open entourage U of X. By what we have proved, $\overline{V} \subseteq U \subseteq \overline{V}$. Thus the claim follows. □

Note that every family $(\mathfrak{U}_i)_{i \in I}$ of uniformities on a set X has a **least upper bound** $\mathfrak{U}$ in the ordered set of all uniformities on X: we have only to apply Proposition 2.1.22, taking Y_i to be the set X with the unifonnity $\mathfrak{U}_i$ and f_i to be the identity mapping $X \to Y_i$. The topology induced by $\mathfrak{U}$ is just the least upper bound of the topologies induced by the $\mathfrak{U}_i$.

Example 2.1.27. If $\omega = (A_i)_{i=1}^n$ is any finite partition of a nonempty set X, the set $V_\omega = \bigcup_{i=1}^n A_i \times A_i$ by itself constitutes a fundamental system of entourages of a uniformity $\mathfrak{U}_\omega$ on X; the uniformity of finite partitions on X (Example 2.1.21) is then the least upper bound of the uniformities $\mathfrak{U}_\omega$.

Using initial uniformity, we can consider products of uniform spaces. If $(X_i)_{i \in I}$ is a family of uniform spaces, the product uniform space of this family is the product set $X = \prod_{i \in I} X_i$ endowed with the coarsest uniformity for which the projections $\pi_i : X \to X_i$ are uniformly continuous. This uniformity is called the **product** of the uniformities of the X_i and the uniform spaces X_i are called the **factors** of X. By Corollary 2.1.23, the topology induced by the product uniformity on X is same as the product of the topologies of the X_i.

Proposition 2.1.28. *Let $f = (f_i)$ be a mapping of a uniform space Y into a product uniform space $X = \prod_{i \in I} X_i$. Then f is uniformly continuous if and only if each f_i is uniformly continuous.*

Proof. Since $f_i = \pi_i \circ f$, this is a particular case of Proposition 2.1.22. □

Corollary 2.1.29. *Let $(X_i)_{i \in I}$ and $(Y_i)_{i \in I}$ be two families of uniform spaces indexed by the same set I. For each $i \in I$, let f_i be a mapping of X_i into Y_i. If each of the f_i is uniformly continuous, then so is the product mapping*

$$f : \prod_{i \in I} X_i \to \prod_{i \in I} Y_i, \quad (x_i) \mapsto (f_i(x_i)).$$

Conversely, if the X_i's are nonempty and f is uniformly continuous, then each f_i is uniformly continuous.

Proof. The map f can be written as $x \mapsto (f_i(\pi_i(x)))$, and the first part of the corollary therefore follows from Proposition 2.1.28. Conversely, choose $a = (a_i) \in \prod_{i \in I} X_i$. For each $j \in I$ let g_j be the mapping of X_j into $\prod_{i \in I} X_i$ such that $\pi_j(g_j(x)) = x_j$ and $\pi_i(g_j(x_j)) = a_i$, whenever $i \neq j$. Then g_j is uniformly continuous at the point a_j. Since $f_j = \pi_j \circ f \circ g_j$, it follows that if f is uniformly continuous at a, then f_j is uniformly continuous at a_j. □

The general criterion of transitivity of initial uniformities shows that, as for the product of topological spaces, the product of uniform spaces is associative and that the following is true:

Proposition 2.1.30. *Let X be a set, let $(Y_i)_{i\in I}$ be a family of uniform spaces, and for each $i \in I$ let f_i be a mapping of X into Y_i. Let f be the mapping $x \mapsto (f_i(x))$ of X into $Y = \prod_{i\in I} Y_i$ and let $\mathfrak{U}$ be the coarsest uniformity on X for which the f_i are uniformly continuous. Then $\mathfrak{U}$ is the inverse image under f of the uniformity induced on $f(X)$ by the product uniformity on Y.*

Corollary 2.1.31. *For each $i \in I$, let A_i be a subspace of X_i. Then the uniformity induced on $A = \prod_{i\in I} A_i$ by the product uniformity on $\prod_{i\in I} X_i$ is the same as the product of the uniformities of the subspaces A_i.*

To conclude this part, we introduce the inverse limit of uniform spaces. Let $(I, \preceq)$ be a partially ordered set. For each $\alpha \in I$ let X_α be a uniform space, and for each pair of indices α, β such that $\alpha \preceq \beta$ there is a map $f_{\alpha\beta} : X_\beta \to X_\alpha$. We shall say that $(X_\alpha, f_{\alpha\beta})$ is an inverse system of uniform spaces if

(a) $(X_\alpha, f_{\alpha\beta})$ is an inverse system sets.

(b) Each map $f_{\alpha\beta}$ is uniformly continuous.

On $X = \varprojlim X_i$ the coarsest uniformity for which the canonical mappings $f_\alpha : X \to X_\alpha$ are uniformly continuous is called the inverse limit (with respect to the $f_{\alpha\beta}$) of the uniformities of the X_α, and the set X endowed with this coarsest uniformity is called the **inverse limit of the inverse system of uniform spaces $X_\alpha, f_{\alpha\beta}$**.

Proposition 2.1.32. *Let I be a directed set, let $(X_\alpha, f_{\alpha\beta})$ be an inverse system of uniform spaces indexed by I, and let J be a cofinal subset of I. For each $\alpha \in I$ let f_α be the canonical mapping of $X = \varprojlim X_\alpha$ into X_α, and let g_α denote $f_\alpha \times f_\alpha$. Then the family of sets $g_\alpha^{-1}(V_\alpha)$, where α runs through J and where, for each $\alpha \in J$, V_α runs through a fundamental system of entourages of X_α, is a fundamental system of entourages of X.*

Finally, the topology on $X = \varprojlim X_\alpha$ induced by the inverse limit of the uniformities of the X_α is the inverse limit of the topologies of the X_α.

2.2 Complete spaces

2.2.1 Cauchy filters

Once a set X has been endowed with a uniform structure we can define what is meant by a "small" subset of X (relative to this structure): a "small" subset of X is one in which all the points are "very close" to each other. Precisely:

Definition 2.2.1. *If X is a uniform space and if V is an entourage of X, a subset A of X is said to be V-**small** if every pair of points of A are V-close (in other words, if $A \times A \subseteq V$).*

The following result can be viewed as a "triangle inequality" property for U-closeness.

Proposition 2.2.2. *In a uniform space X, if two sets A and B are V-small and intersect, then their union $A \cup B$ is $V \circ V$-small.*

Proof. Let x and y be any two points of $A \cup B$, and let $z \in A \cap B$. Then $(x, z) \in V$ and $(z, y) \in V$, so that $(x, y) \in V \circ V$. □

A filter $\mathfrak{F}$ on a uniform space X is a Cauchy filter if for each entourage V of X there is a subset of X which is V-small and belongs to $\mathfrak{F}$.

Remark 2.2.1. An infinite sequence (x_n) of points of a uniform space X is said to be a **Cauchy sequence** if the elementary filter associated with the sequence is a Cauchy filter. It comes to the same thing to say that for each entourage V of X there is an integer N such that for all integers $n, m > N$, we have $(x_n, x_m) \in V$.

Example 2.2.3 (Example of Cauchy filters).

(a) Let X be a discrete uniform space, then the Cauchy filters on X are trivial filters: since Δ is the unique entourage on X, any Cauchy filter must contains a singleton.

(b) Let X be an infinite set and endow X with the finite partition uniformity. Then any Cauchy filter $\mathfrak{F}$ on X is ultra: if $A \subseteq X$, then A and A^c form a partition of X, and with $V = (A \times A) \cup (A^c \times A^c)$, we see either A contains a set in $\mathfrak{F}$ of A^c contains a set in $\mathfrak{F}$. Thus by Theorem 1.7.21, $\mathfrak{F}$ is ultra.

Proposition 2.2.4. *On a uniform space X every convergent filter is a Cauchy filter.*

Proof. If x is any point of X and V is any symmetric entourage of X, then the neighbourhood $V(x)$ of x is $V \circ V$-small. If $\mathfrak{F}$ is a filter which converges to x, there is a set of $\mathfrak{F}$ contained in $V(x)$, and therefore $V \circ V$-small. Together with axoim (U3), this proves $\mathfrak{F}$ is Cauchy. □

Proposition 2.2.5. *Let $f : X \to Y$ he a uniformly continuous mapping. Then the image under f of a Cauchy filter base on X is a Cauchy filter base on Y.*

Proof. Let $g = f \times f$. If V is an entourage of Y, then $g^{-1}(V)$ is an entourage of X, and the image under f of a $g^{-1}(V)$-small set is V-small; hence the result. □

It follows in particular that if the uniformity of a uniform space X is replaced by a coarser uniformity, then every Cauchy filter with respect to the original uniformity remains a Cauchy filter with respect to the new uniformity. This fact can be easily remembered in the following form: the finer the uniformiyy, the fewer Cauchy filters there are.

Proposition 2.2.6. *Let X be a set, let $(Y_i)_{i \in I}$ be a family of uniform spaces, and for each $i \in I$ let f_i be a mapping of X into Y_i. Let X carry the coarsest uniformiry $\mathfrak{U}$ for which the f_i are uniformly continuous. Then in order that a filter base $\mathfrak{B}$ on X should be a Cauchy filter base it is necessary and sufficient that $f_i(\mathfrak{B})$ should be a Cauchy filter base on Y_i for each $i \in I$.*

Proof. The condition is necessary by Proposition 2.2.5. Conversely, suppose that it is satisfied, and let $U(V_{i_1}, \ldots, V_{i_n})$ be an entourage of the uniformity $\mathfrak{U}$. By hypothesis, for each index k there is a set $M_k \in \mathfrak{B}$ such that $f_{i_k}(M_k)$ is V_{i_k}-small. Let M be a set of $\mathfrak{B}$ contained in M_k for $1 \leq k \leq n$; then for each pair of points x, y of M we have $(f_{i_k}(x), f_{i_k}(y)) \in V_{i_k}$, $1 \leq k \leq n$, so that

$$(x, y) \in I(V_{i_1}, \ldots, V_{i_n}).$$

This completes the proof. □

Corollary 2.2.7. *If a Cauchy filter on a uniform space X induces a filter on a subset A of X, then this filter is a Cauchy filter on the uniform subspace A.*

Corollary 2.2.8. *A filter base $\mathfrak{B}$ on a product $\prod_{i\in I} X_i$ of uniform spaces is a Cauchy filter base if and only if, for each $i \in I$, $\pi_i(\mathfrak{B})$ is a Cauchy filter base on X_i.*

The minimal elements (with respect to inclusion) of the set of Cauchy filters on a uniform space X are called **minimal Cauchy filters** on X.

Proposition 2.2.9. *Let X be a uniform space. For each Cauchy filter $\mathfrak{F}$ on X there is a unique minimal Cauchy filter $\mathfrak{F}_0$ coarser than $\mathfrak{F}$. If $\mathfrak{B}$ is a base of $\mathfrak{F}$ and $\mathfrak{S}$ is a fundamental system of symmetric entourages of X, then the sets $\{V(M) : M \in \mathfrak{B}, V \in \mathfrak{S}\}$ form a base of $\mathfrak{F}_0$.*

Proof. If M, M' are in $\mathfrak{B}$ and V, V' are in $\mathfrak{S}$, then there is a set $N \in \mathfrak{B}$ and $W \in \mathfrak{S}$ such that $N \subseteq M \cap M'$ and $W \subseteq V \cap V'$. Hence

$$W(N) \subseteq V(M) \cap V'(M')$$

and therefore the sets $\{V(M) : M \in \mathfrak{B}, V \in \mathfrak{S}\}$ indeed form a base of a filter $\mathfrak{F}_0$ on X. Further, if M is V-small, then $V(M)$ is V^3-small; hence $\mathfrak{F}_0$ is a Cauchy filter and is clearly coarser than $\mathfrak{F}$. To complete the proof it is enough to show that if $\mathfrak{G}$ is a Cauchy filter coarser than $\mathfrak{F}$, then $\mathfrak{G}$ is finer than $\mathfrak{F}_0$. For each $M \in \mathfrak{B}$ and each $V \in \mathfrak{S}$ there is a set $N \in \mathfrak{G}$ which is V-small; since $N \in \mathfrak{F}$, N must meet M; hence $N \subseteq V(M)$ and so $V(M) \in \mathfrak{G}$. □

Corollary 2.2.10. *For each $x \in X$, the neighbourhood filter $\mathfrak{U}(x)$ of x in X is a minimal Cauchy filter.*

Proof. Take $\mathfrak{F}$ in Proposition 2.2.9 to be the filter of all subsets of X which contain x, and take $\mathfrak{B}$ to consist of the single element $\{x\}$. Then it is easy to see $\mathfrak{U}(x)$ is the minimal Cauchy filter contained in $\mathfrak{F}$. □

Corollary 2.2.11. *Every cluster point x of a Cauchy filter $\mathfrak{F}$ is a limit point of $\mathfrak{F}$.*

Proof. Since x is a cluster point of $\mathfrak{F}$, there is a filter $\mathfrak{G}$ which is finer than both $\mathfrak{F}$ and $\mathfrak{U}(x)$; since $\mathfrak{F}$ is a Cauchy filter, so is $\mathfrak{G}$. If $\mathfrak{F}_0$ is the unique minimal Cauchy filter coarser than $\mathfrak{F}$, then both $\mathfrak{F}_0$ and $\mathfrak{U}(x)$ are minimal Cauchy filters coarser than $\mathfrak{G}$. Hence $\mathfrak{F}_0 = \mathfrak{U}(x)$, which shows that $\mathfrak{F}$ converges to x. □

Corollary 2.2.12. *Every Cauchy filter $\mathfrak{F}$ which is coarser than a filter converging to a point x, also converges to x.*

Proof. This is a concequence of Corollary 2.2.11, since in this situation x is a cluster point of $\mathfrak{F}$. □

Corollary 2.2.13. *If $\mathfrak{F}$ is a minimal Cauchy filter, then every set of $\mathfrak{F}$ has a nonempty interior which also belongs to $\mathfrak{F}$ (in other words, $\mathfrak{F}$ has a base consisting of open sets).*

Proof. Let V be any entourage of X; then there is an open entourage $U \subseteq V$. For each subset M of X, $U(M)$ is open and contained in $V(M)$; hence the result, in view of Proposition 2.2.9. □

2.2.2 Complete spaces

In a uniform space X, a Cauchy filter need not have a limit point.

Example 2.2.14. Let X be an infinite set, and consider the uniformity of finite partitions on X. Every ultrafilter $\mathfrak{F}$ on X is a Cauchy filter with respect to this uniformity. For if $(A_i)_{i=1}^n$ is a finite partition of X and

$$V = \bigcup_{i=1}^{n} A_i \times A_i$$

is the corresponding entourage, then at least one of the A_i belongs to $\mathfrak{F}$, and A_i is V-small. On the other hand, X is an infinite discrete space, hence is not compact, and consequently there are ultrafilters on X which do not converge.

A **complete space** is a uniform space in which every Cauchy filter converges. For example, on a discrete uniform space X a Cauchy filter is a trivial ultrafilter, hence convergent; consequently, X is complete.

From definition and Proposition 2.2.4, we deduce the following proposition, known as Cauchy's criterion:

Proposition 2.2.15. *Let $\mathfrak{F}$ be a filter on a set X, and let f be a mapping of X into a complete uniform space Y. Then f has a limit with respect to $\mathfrak{F}$ if and only if the image of $\mathfrak{F}$ under f is a Cauchy filter base.*

This criterion shows the importance of complete spaces in all questions involving the notion of limit: if a function takes its values in a complete space we can prove the existence of a limit without knowing in advance the value of the limit; this would be impossible if the definition of limit were the only criterion of convergence at our disposal.

A uniformity which is finer than the uniformity of a complete space need not be a uniformity of a complete space. However, we have the following proposition:

Proposition 2.2.16. *Let $\mathfrak{U}_1$, $\mathfrak{U}_2$ be two uniformities on a set X, and let $\mathcal{T}_1$, $\mathcal{T}_2$ be the topologies induced by these uniformities respectively. Suppose that $\mathfrak{U}_1$ is finer than $\mathfrak{U}_2$, and that there is a fundamental system of entourages for $\mathfrak{U}_1$ which are closed in $X \times X$ in the topology $\mathcal{T}_2 \times \mathcal{T}_2$. Then a filter $\mathfrak{F}$ on X converges in the topology $\mathcal{T}_1$ if and only if it is a Cauchy filter in the uniformity $\mathfrak{U}_1$ and converges in the topology $\mathcal{T}_2$.*

Proof. The conditions are clearly necessary, because $\mathcal{T}_2$ is coarser than $\mathcal{T}_1$. Conversely, suppose that the conditions are satisfied, and let x be a limit point of $\mathfrak{F}$ with respect to $\mathcal{T}_2$; we shall show that x is a limit of $\mathfrak{F}$ with respect to $\mathcal{T}_1$. Let V be a symmetric entourage of $\mathfrak{U}_1$ which is closed in the topology $\mathcal{T}_2 \times \mathcal{T}_2$. By hypothesis, $\mathfrak{F}$ contains a set M which is V-small; hence if $y \in M$ we have $M \subseteq V(y)$. But $V(y)$ is closed in the topology $\mathcal{T}_2$; hence x, which lies in the closure of M with respect to $\mathcal{T}_2$ (Lemma 1.7.35), must belong to $V(y)$. It follows that $M \subseteq (V \circ V)(x)$, and the proposition is proved. □

Corollary 2.2.17. *In the conditions of Proposition 2.2.16, if $\mathfrak{U}_2$ is a uniformity of a complete space, then so is $\mathfrak{U}_1$.*

Proof. For every Cauchy filter with respect to $\mathfrak{U}_1$ is then a Cauchy filter with respect to $\mathfrak{U}_2$ and therefore converges in the topology $\mathcal{T}_2$. □

Now we consider completeness of subspaces. First, we have the following proposition.

Proposition 2.2.18. *Every closed subspace of a complete space is complete. Every complete subspace of a Hausdorff uniform space (complete or not) is closed.*

Proof. Let X be a complete space and let A be a closed subspace of X. If $\mathfrak{F}$ is a Cauchy filter on A, then it is a Cauchy filter base on X and therefore converges to a point $x \in X$; but since A is closed we have $x \in A$, and therefore $\mathfrak{F}$ converges in the subspace A.

Now let A be a non-closed subset of a Hausdorff uniform space X, and let $x \in \overline{A} \setminus A$. The trace $\mathfrak{B}_A$ on A of the neighbourhood filter $\mathfrak{B}$ of x in X is a Cauchy filter on A; but it cannot converge to a point $y \in A$, otherwise y would be a limit point of $\mathfrak{B}$ which is absurd since $x \neq y$ and X is Hausdorff. □

The following proposition says, for the completeness of X, it suffices to consider Cauchy filters on a dense subset of X. This will be useful when we consider completion of uniform spaces.

Proposition 2.2.19. *Let X be a uniform space and let A be a dense subset of X such that every Cauchy filter base on A converges in X. Then X is complete.*

Proof. It is enough to show that every minimal Cauchy filter $\mathfrak{F}$ on X is convergent. Since A is dense and since every set of $\mathfrak{F}$ has a non-empty interior (Corollary 2.2.13), the trace $\mathfrak{F}_A$ of $\mathfrak{F}$ on A is a Cauchy filter on A, hence converges to a point $x \in X$. Since $\mathfrak{F}$ is coarser than the filter on X generated by $\mathfrak{F}_A$, it follows that $\mathfrak{F}$ converges to x. □

2.2.3 Product and inverse limit of complete spaces

Proposition 2.2.20. *Every product of complete uniform spaces is complete. Conversely, if a product of nonempty uniform spaces is complete, then each of the factors is a complete uniform space.*

Proof. The first assertion is a consequence of the characterization of Cauchy filters and convergent filters on a product space. Conversely, suppose $X = \prod_{i \in I} X_i$ is complete (the X_i being nonempty) and let $\mathfrak{F}_j$ be a Cauchy filter on X_j. For each $i \neq j$ let $\mathfrak{F}_i$ be a Cauchy filter on X_i and consider the product filter

$$\mathfrak{F} = \prod_{i \in I} \mathfrak{F}_i.$$

Then $\mathfrak{F}$ is a Cauchy filter, hence is convergent, and therefore so is each $\mathfrak{F}_j = \pi_j(\mathfrak{F})$. □

Corollary 2.2.21. *Let $(X_\alpha, f_{\alpha\beta})$ be an inverse system of uniform spaces. if the X_α are Hausdorff and complete, then so is $X = \varprojlim X_\alpha$.*

Proof. For X is Hausdorff and X can be identified with a closed subspace of $\prod_{i \in I} X_i$, the corollary therefore follows from Proposition 2.2.18 and Proposition 2.2.20. □

An inverse limit of complete Hausdorff uniform spaces X_α can be empty, even if all the X_α are non-empty and all the $f_{\alpha\beta}$ are surjective, as is shown by the following example.

Example 2.2.22. For each finite subset α of the uncountable set $\mathbb{R}$, let X_α be the set of injections of α into the integers. Each X_α is countable, and for $\alpha \subseteq \beta$ the restriction map $X_\beta \to X_\alpha$ is surjective. But the inverse limit of the X_α is empty, since an element of it would give an injection of $\mathbb{R}$ into the integers.

However, we have the following theorem:

Theorem 2.2.23 (Mittag-Leffler). *Let $(X_\alpha, f_{\alpha\beta})$ be an inverse system of complete Hausdorff uniform spaces, indexed by a directed set I which has a countable cofinal subset; suppose also that, for each $\alpha \in I$, X_α has a countable fundamental system of entourages. Finally, suppose that for each $\alpha \in I$ there is an index $\beta \geq \alpha$ satisfying the following condition:*

(ML$_{\alpha\beta}$) For each $\gamma \geq \beta$, $f_{\alpha\gamma}(X_\gamma)$ is dense in $f_{\alpha\beta}(X_\beta)$.

Let $X = \varprojlim X_\alpha$ and let $f_\alpha : X \to X_\alpha$ be the canonical map. Then for each $\alpha \in I$ and each $\beta \geq \alpha$ satisfying (ML$_{\alpha\beta}$), $f_\alpha(X)$ is dense in $f_\beta(X)$ (and consequently X is nonempty if the X_α are all nonempty).

Proof. Let (λ_n) be a sequence of indices cofinal in I. Start with an index $\alpha_0 \in I$ and define recursively an increasing sequence (α_n) such that $\alpha_n \geq \lambda_n$ and (ML$_{\alpha_n\alpha_{n+1}}$) is true. Clearly the sequence (α_n) is cofinal in I. We shall write f_{mn} in place of $f_{\alpha_m\alpha_n}$ for $m \leq n$ and put $Y_n = f_{n,n+1}(X_{\alpha_{n+1}})$. For $m \leq n$, we see $f_{mn}(Y_n)$ is dense in Y_m: by definition $f_{m,n+1}(X_{\alpha_{n+1}})$ is dense in $f_{m,m+1}(X_{\alpha_{m+1}}) = Y_m$, and we have

$$f_{m,n+1}(X_{\alpha_{n+1}}) = (f_{mn} \circ f_{n,n+1})(X_{\alpha_{n+1}}) = f_{mn}(Y_n).$$

Now we define a fundamental system $(V_{kn})_{k\in\mathbb{N}}$ of closed symmetric entourages of X_{α_n} for each n such that

(a) $V_{k+1,n} \circ V_{k+1,n} \subseteq V_{kn}$.

(b) $(f_{n,n+1} \times f_{n,n+1})(V_{k,n+1}) \subseteq V_{kn}$.

We proceed by induction. Let $(U_{kn})_{k\in\mathbb{N}}$ be a fundamental system of entourages of X_{α_n}. If we suppose that the V_{kn} have been defined for a given n and for all $k \in \mathbb{N}$, then since $f_{n,n+1}$ is uniformly continuous we can define the entourage $V_{k,n+1}$ by induction on k so that (b) is satisfied and

$$V_{k+1,n+1} \circ V_{k+1,n+1} \subseteq V_{k,n+1} \cap U_{k+1,n+1}.$$

This gives the desired system (V_{kn}).

Now let $x_0 \in Y_0$. We shall show that for each positive integer k there is a point $z \in X$ such that $(x_0, f_{\alpha_0}(z)) \in V_{k-1,0}$; this will prove the theorem. Since $f_{n,n+1}(Y_{n+1})$ is dense in Y_n, we can define by induction a sequence of points $x_n \in Y_n$ such that

$$(x_n, f_{n,n+1}(x_{n+1})) \in V_{k+n,n}$$

By condition (b) it follows that if $m \leq n$ then

$$(f_{mn}(x_n), f_{m,n+1}(x_{n+1})) \in V_{k+n,m}. \tag{2.3.1}$$

From this we conclude that for fixed m the sequence $(f_{mn}(x_n))_{n\geq m}$ is a Cauchy sequence in X_{α_m} and therefore converges to a point z_m; for by induction it follows from (2.3.1) that, for each pair of integers $p, q \geq m$, we have

$$(f_{mp}(x_p), f_{mq}(x_q)) \in V_{k+q-1,m} \circ V_{k+q-2,m} \circ \cdots \circ V_{k+p,m} \tag{2.3.2}$$

and by virtue of (a) it is clear that the right-hand side of (2.3.2) is contained in $V_{k+p-1,m}$. Let q increase indefinitely; we infer in particular that, for $p = m = 0$, we have $(x_0, z_0) \in V_{k-1,0}$ since $V_{k-1,0}$ is closed. On the other hand, from the relations $z_m = \lim_n f_{mn}(x_n)$ and from the continuity of $f_{m,m+1}$ we deduce that $f_{m,m+1}(z_{m+1}) = z_m$ for each $m \geq 0$. For each $\gamma \in I$ there is at least one integer n such that $\alpha_n \succeq \gamma$; putting $z_\gamma = f_{\gamma,\alpha_n}(z_n)$ we verify immediately that z_γ does not depend on the value of n such that $\alpha_n \succeq \gamma$, and that the family $(z_\gamma)_{\gamma \in I}$ so defined is a point z of $X = \varprojlim X_\alpha$. Since $f_{\alpha_0}(z) = z_0$, the proof is complete. □

Corollary 2.2.24. *Let $(X_\alpha, f_{\alpha\beta})$ be an inverse system of sets indexed by a directed set I which has a countable cojinal subset, and suppose that the $f_{\alpha\beta}$ are surjective. Then if $X = \varprojlim X_\alpha$, the canonical mapping $f_\alpha : X \to X_\alpha$ is surjective for each $\alpha \in I$.*

Proof. Let each X_α carry the discrete uniformity, and apply Theorem 2.2.23. □

Corollary 2.2.25. *Let I be a directed set which has a countable cofinal subset. Let $(X_\alpha, f_{\alpha\beta})$ and $(Y_\alpha, g_{\alpha\beta})$ be two inverse systems of sets indexed by I and (ϕ_α) be an inverse system of maps with $\phi = \varprojlim \phi_\alpha$. Let $y = (y_\alpha)$ be an element of $Y = \varprojlim Y_\alpha$ which satisfies the following condition:*

- *For each $\alpha \in I$ there is an index $\beta \succeq \alpha$ such that for all $\gamma \succeq \gamma$ we have*

$$f_{\alpha\gamma}(\phi_\gamma^{-1}(y_\gamma)) = f_{\alpha\beta}(\phi_\beta^{-1}(y_\beta)).$$

Then there is an element $x \in X$ such that $\phi(x) = y$.

Proof. Apply Theorem 2.2.23 to the inverse system of sets $\phi_\alpha^{-1}(y_\alpha)$, each carrying the discrete uniformity. □

Example 2.2.26. Suppose we are given in $\mathbb{C}$:

(i) a sequence (a_n) of distinct points such that the sequence $(|a_n|)$ is increasing and tends to $+\infty$;

(ii) for each n a rational function $R_n(z)$ defined in $\mathbb{C} \setminus \{a_n\}$ and having a pole at a_n;

(iii) an increasing sequence (B_n) of open discs centred at 0 whose union is $\mathbb{C}$, and such that none of the a_n is on the boundary of any of the discs B_m.

For each n, define $C_n = \overline{B}_n \setminus \{a_n\}$, and let X_n denote the set of all mappings from C_n to $\mathbb{C}$ of the form

$$S(z) = P(z) + \sum_{a_k \in B_n} R_k(z)$$

where P is the restriction to C_n of a function which is continuous in $\overline{B}_n$ and holomorphic in B_n. We define a metric in X_n by putting

$$d_n(S_1, S_2) = \sup_{z \in C_n} |S_1(z) - S_1(z)|.$$

It is easily verified that X_n is complete with respect to this metric. Finally, for $n \leq m$, we define a mapping $f_{mn} : X_m \to X_n$ such that if $S \in X_m$ then $f_{nm}(S)$ is the restriction of S to C_n. It is clear that the f_{mn} are uniformly continuous and that (X_m, f_{mn}) is an inverse system of uniform

spaces. Now an element of the inverse limit $X = \varprojlim X_n$ can be canonically identified with a meromorphic function f in $\mathbb{C}$, whose only poles are the points a_n and which is such that for each n, $f(z) - R_n(z)$ is holomarphic at a_n. The classical theorem of Mittag-Leffler asserts that X is not empry; by virtue of Theorem 2.2.23, we have only to verify the condition (ML_{nn}) for all n. Let

$$S_n = P_n + \sum_{a_k \in B_n} R_k$$

be an element of X_n where P_n is continuous in $\overline{B}_n$ and holomorphic in B_n; for any $m \geq n$, let Q_{mn} be the restriction of $\sum_{a_i \in B_m \setminus B_n} R_i$ to C_n; this sum is a holomorphic function in some neighbourhood of $\overline{B}_n$, hence (by Taylor's theorem) for each $\varepsilon > 0$ there is a polynomial P_{mn} such that $|Q_{mn} - P_{mn}| < \varepsilon$ in B_n; if S_m is the restriction of $S_n + Q_{mn} - P_{mn}$ to C_m, we have $S_m \in X_m$ and $|S_m - S_n| < \varepsilon$ in B_n. This completes the proof.

2.2.4 Extension of uniformly continuous functions

The theorem of extension by continuity has important additions when the functions in question take their values in a complete Hausdorff uniform space.

Theorem 2.2.27. *Let A be a dense subset of a topological space X, and let f be a mapping of A into a complete Hausdorff uniform space X. Then f can be extended by continuity to X if and only if, for each $x \in X$, the image under f of the trace on A of the neighbourhood filter of x in X is a Cauchy filter base in X.*

Proof. This follows from the theorem of extension by continuity because Y is regular and because on Y convergent filters are the same as Cauchy filters. □

When X is also a uniform space, there is the following theorem:

Theorem 2.2.28. *Let f be a function defined on a dense subspace A of a uniform space X, taking its values in a complete Hausdorff uniform space Y, and suppose that f is uniformly continuous on A. Then f can be extended to the whole of X by continuity, and the extended function $\bar{f}$ is uniformly continuous.*

Proof. The existence of $\bar{f}$ is an immediate consequence of Theorem 2.2.27. Let us show that $\bar{f}$ is uniformly continuous. Let V be a closed symmetric entourage of Y, and let U be an entourage of X such that, when x and y are in A and are U-close, then $f(x)$ and $f(y)$ are V-close. We may assume that U is the closure $X \times X$ of an entourage W of A (Proposition 2.1.26). We have $(\bar{f}(x), \bar{f}(y)) \in V$ when $(x, y) \in W$; since $\bar{f} \times \bar{f}$ is continuous in $X \times X$ and V is closed, we see $(\bar{f}(x), \bar{f}(y)) \in V$ when $(x, y) \in U = \overline{W}$. This proves the claim. □

Corollary 2.2.29. *Let X_1, X_2 be two complete Hausdorff uniform spaces, and let A_1, A_2 be dense subspaces of X_1, X_2 respectively. Then every isomorphism $f : A_1 \to A_2$ extends to an isomorphism of X_1 onto X_2.*

Proof. The map f is uniformly continuous in A_1, hence extends to a uniformly continuous mapping $\bar{f} : X_1 \to X_2$. Likewise the inverse g of f extends to a uniformly continuous mapping $\bar{g} : X_2 \to X_1$. The function $\bar{g} \circ \bar{f}$ is therefore a continuous mapping of X_1 into itself whose restriction to A_1 is the identity mapping; by the desity of A_1 it follows that $\bar{g} \circ \bar{f}$ is the

identity mapping of X_1; similarly $\bar{f} \circ \bar{g}$ is the identity map of X_2. Consequently $\bar{f}$ and $\bar{g}$ are bijections and are inverses of each other; they are also uniformly continuous and are therefore isomorphisms. □

2.2.5 Completion of uniform spaces

Theorem 2.2.30. *Let X he a uniform space. Then there exists a complete Hausdorff uniform space $\widehat{X}$ and a uniformly continuous mapping $\iota : \widehat{X} \to X$ having the following property:*

(P) Given any uniformly continuous mapping f of X into a complete Hausdorff unfform space Y, there is a unique uniformly continuous mapping $g : X \to Y$ such that $f = g \circ \iota$.

If $(\widehat{X}', \iota')$ is another pair consisting of a complete Hausdorff uniform space $\widehat{X}'$ and a uniformly continuous mapping $\iota' : X \to \widehat{X}'$ having the properry (P), then there is a unique isomorphism $\phi : \widehat{X} \to \widehat{X}'$ such that $\iota' = \phi \circ \iota$.

Proof. Let X be the set ofminimal Cauchy filters on X. We shall define a uniform structure on X. For this purpose, if V is any symmetric entourage of X, let $\widehat{V}$ denote the set of all pairs $(\mathfrak{X}, \mathfrak{Y})$ of minimal Cauchy filters which have in common a V-small set. We shall show that the sets $\widehat{V}$ form a fundamental system of entourages of a uniform structure on $\widehat{X}$.

If V and V' are two symmetric entourages of X, then $W = V \cap V'$ is a symmetric entourage, and every set which is W-small is also V-small and V'-small; hence $\widehat{W} \subseteq \widehat{V} \cap \widehat{V}'$. Also, it is easy to see $\widehat{V} \neq \varnothing$ for any symmetric entourage V, therefore $\{\widehat{V}\}$ is a filter base. Now since each $\mathfrak{X} \in \widehat{X}$ is a Cauchy filter, we have by definition $(\mathfrak{X}, \mathfrak{X}) \in \widehat{V}$ for every symmetric entourage V of X; hence axiom (B1) is satisfied. The sets V are symmetric by definition, hence (B2) is satisfied. Finally, given a symmetric entourage V of X, let W be a symmetric entourage such that $W \circ W \subseteq V$. Consider three minimal Cauchy filters $\mathfrak{X}$, $\mathfrak{Y}$, $\mathfrak{Z}$ such that $(\mathfrak{X}, \mathfrak{Y}) \in \widehat{W}$ and $(\mathfrak{Y}, \mathfrak{Z}) \in \widehat{W}$; then there are two W-small sets M, N such that $M \in \mathfrak{X} \cap \mathfrak{Y}$ and $N \in \mathfrak{Y} \cap \mathfrak{Z}$. Since M and N belong to $\mathfrak{Y}$, $M \cap N$ is not empty and therefore $M \cup N$ is $W \circ W$-small (Proposition 2.2.2) and hence V-small; since $M \cup N$ belongs to $\mathfrak{X}$ and to $\mathfrak{Z}$, we have $\widehat{W} \circ \widehat{W} \subseteq \widehat{V}$, hence (B3) is satisfied.

We show next that the uniform space $\widehat{X}$ is Hausdorff. Let $\mathfrak{X}$, $\mathfrak{Y}$ be two ininimal Cauchy filters on $\widehat{X}$ such that $(\mathfrak{X}, \mathfrak{Y}) \in \widehat{V}$ for all symmetric entourages V of X. It follows immediately that the sets $M \cup N$, where $M \in \mathfrak{X}$ and $N \in \mathfrak{Y}$, form a base of a filter $\mathfrak{Z}$ coarser than $\mathfrak{X}$ and $\mathfrak{Y}$. Now $\mathfrak{Z}$ is a Cauchy filter, since for every symmetric entourage V of X there is by hypothesis a V-small set P belonging to both $\mathfrak{X}$ and $\mathfrak{Y}$ and therefore belonging to $\mathfrak{Z}$. By the definition of minimal Cauchy filters, we have $\mathfrak{X} = \mathfrak{Y} = \mathfrak{Z}$, and this shows that $\widehat{X}$ is Hausdorff.

Now we define the map ι. We know that for each $x \in X$ the neighbourhood filter $\mathfrak{U}(x)$ of x in X is a minimal Cauchy filter (Corollary 2.2.10). So we define $\iota(x) = \mathfrak{U}(x)$. Let $j = \iota \times \iota$; we shall show that for each symmetric entourage V of X we have $j^{-1}(\widehat{V}) \subseteq V \subseteq j^{-1}[\widehat{V^3}]$, and this will implies that X carries the initial uniformity with respect to $\widehat{X}$ and ι. Now, if $(\iota(x), \iota(y)) \in \widehat{V}$, there is a V-small set M which is a neighbourhood of each of x and y, hence $(x, y) \in V$. Conversely, if $(x, y) \in V$, it is immediately seen that the set $V(x) \cup V(y)$ is V^3-small and is a neighbourhood of each of x and y.

The trace on $\iota(X)$ of a neighbourhood $\widehat{V}(\mathfrak{X})$ of a point of $\mathfrak{X} \in \widehat{X}$ is the set of all $\iota(x)$ such that $(\mathfrak{X}, \iota(x)) \in \widehat{V}$. This relation means that there is a V-small neighbourhood of x in X which belongs to $\mathfrak{X}$, i.e. that x is an interior point of a V-small set of $\mathfrak{X}$. Let M be the union of the

interiors of all V-small sets of $\mathfrak{X}$; then M is nonempty by Corollary 2.2.13 and from what has been said it follows that $\widehat{V}(\mathfrak{X}) \cap \iota(x) = \iota(M)$. We conclude that

(i) $\widehat{V}(\mathfrak{X}) \cap \iota(X)$ is not empty, hence $\iota(X)$ is dense in $\widehat{X}$.

(ii) The trace of $\widehat{V}(\mathfrak{X})$ on $\iota(X)$ belongs to the filter base $\iota(\mathfrak{X})$ on $\widehat{X}$; hence this filter base converges in $\widehat{X}$ to the point $\mathfrak{X}$.

Now let $\mathfrak{F}$ be a Cauchy filter on $\iota(X)$; then from (ii) above and Proposition 2.2.6, $\iota^{-1}(\mathfrak{F})$ is a base of a Cauchy filter $\mathfrak{G}$ on X. Let $\mathfrak{X}$ be a minimal Cauchy filter coarser than $\mathfrak{G}$; then $\iota(\mathfrak{X})$ is a Cauchy filter base on $\iota(X)$, and $\mathfrak{F} = \iota(\iota^{-1}(\mathfrak{F}))$ is finer than the filter whose base is $\iota(\mathfrak{X})$. Since the latter converges in $\mathfrak{X}$, so does $\mathfrak{F}$, and Proposition 2.2.19 therefore shows that $\widehat{X}$ is complete.

We now verify the property (P). Let f be a uniformly continuous mapping of X into a complete Hausdorff uniform space Y. Let us first show that there is a unique uniformly continuous mapping $g_0 : \iota(X) \to Y$ such that $f = g_0 \circ \iota$. Since f is continuous, we have

$$f(x) = \lim f(\mathfrak{U}(x))$$

hence if we put $g_0(\iota(x)) = \lim f(\mathfrak{U}(x))$, we have $f = g_0 \circ \iota$; so it remains to show that g_0 is uniformly continuous in $\iota(X)$. Let U be an entourage of Y and let V be a symmetric entourage of X such that therelation $(x, y) \in V$ implies $(f(x), f(y)) \in U$; we have seen in (ii) that the relation $(\iota(x), \iota(y)) \in \widehat{V}$ implies $(x, y) \in V$, hence also implies $(g_0(\iota(x)), g_0(\iota(y))) \in U$, which proves our assertion.

Let g be the extension of g_0 by continuity to $\widehat{X}$ (Theorem 2.2.28); then $f = g_0 \circ \iota$, and it is clear that g is the unique continuous mapping of $\widehat{X}$ into Y satisfying this relation, since $\iota(X)$ is dense in $\widehat{X}$. With this, the uniqueness part of the pair $(\widehat{X}, \iota)$ is clear now, □

Definition 2.2.31. *The complete Hausdorff uniform space $\widehat{X}$ defined in the proof of Theorem 2.2.30 is called the* ***Hausdorff completion*** *of X, and the mapping $\iota : X \to \widehat{X}$ is called the* ***canonical mapping*** *of X into its Hausdorff completion.*

Proposition 2.2.32. *Let X be a uniform space and $\widehat{X}$ be its completion.*

(a) The subspace $\iota(X)$ is dense in $\widehat{X}$.

(b) The graph of the equivalence relation $\iota(x) = \iota(y)$ is the intersection of the entourages of X.

(c) The uniform structure of X is the inverse image under ι of that of $\widehat{X}$.

(d) The entourages of $\iota(X)$ are the images under $\iota \times \iota$ of the entourages of X, and the closures in $\widehat{X} \times \widehat{X}$ of the entourages of $\iota(X)$ form a fundamental system of entourages of $\widehat{X}$.

(e) The construction $X \mapsto \widehat{X}$ is functorial. That is, if X and Y be two uniform spaces and $f : X \to Y$ is a uniformly continuous map, then there is a unique uniformly continuous mapping $\hat{f} : \widehat{X} \to \widehat{Y}$ such that the diagram

$$\begin{tikzcd} \widehat{X} \arrow[r, "\hat{f}"] & \widehat{Y} \\ X \arrow[u] \arrow[r, "f"] & Y \arrow[u] \end{tikzcd}$$

is commutative. Moreover, if $f : X \to Y$ and $g : Y \to Z$ are two uniformly continuous mappings, then $\widehat{g \circ f} = \hat{g} \circ \hat{f}$.

Proof. Part (a) and (c) have been proved in the course of the proof of Theorem 2.2.30; (e) follows from Theorem 2.2.28, and (d) is a consequence of (a) and (c) by virtue of general results proved earlier. The relation $\iota(x) = \iota(y)$ means by definition that x and y have the same neighbourhood filter. But this implies, by definition, that $(x, y) \in V$ for every entourage V of X, and the converse is obvious. □

Corollary 2.2.33. *If X is a Hausdorff uniform space, then the canonical mapping $\iota : X \to \widehat{X}$ is an isomorphism of X onto the dense subspace $\iota(X)$ of $\widehat{X}$.*

When X is Hausdorff, $\widehat{X}$ is said to be the **completion** of X, and we generally identify X with a dense subset of $\widehat{X}$ by means of ι. Corollary 2.2.33 characterizes the completion of a Hausdorff uniform space:

Proposition 2.2.34. *If Y is a complete Hausdorif uniform space and X is a dense subspace of Y, then the canonical injection $X \to Y$ extends to an isomorphism of $\widehat{X}$ onto Y.*

Proof. By by Theorem 2.2.28, every uniformly continuous mapping of X into a complete Hausdorff uniform space Z extends uniquely to a uniformly continuous mapping of Y into Z. □

Proposition 2.2.35. *Let X be a complete Hausdorff uniform space, $\mathfrak{U}$ its uniformiry, and let Z be a dense subspace of X. If $\mathfrak{U}'$ is a uniformiry on X which is coarser than $\mathfrak{U}$, and which induces the same uniformiry as $\mathfrak{U}$ on Z, then $\mathfrak{U}' = \mathfrak{U}$.*

Proof. Let X' denote the set X with the uniformity $\mathfrak{U}'$, The composition of the identity mapping $X \to X'$ and the canonical mapping $X' \to \widehat{X'}$ is a uniformly continuous mapping $\varphi : X \to \widehat{X'}$. Since Z is Hausdorff for the uniform structure induced by $\mathfrak{U}'$, the restriction of φ to Z is by hypothesis an isomorphism of Z onto the dense subspace $\varphi(Z)$ of $\widehat{X'}$; it follows from Corollary 2.2.33 that φ itself is an isomorphism of X onto $\widehat{X'}$, hence $X = \widehat{X'}$ and $\mathfrak{U}' = \mathfrak{U}$. □

2.2.6 The Hausdorff space associated with a uniform space

We have seen that the completion of a uniform space is Hausdorff and complete. Since not all uniform space are Hausdorff, one may get from this a "Hausdorffication" functor on the category of uniform spaces.

Proposition 2.2.36. *Let X be a uniform space and ι the canonical mapping of X into its Hausdorff completion $\widehat{X}$. For each uniformly continuous mapping f of X into a Hausdorff uniform space Y, there is a unique uniformry continuous mapping $h : \iota(X) \to Y$ such that $f = h \circ \iota$.*

$$\begin{tikzcd} \iota(X) \arrow[dr, "h"] & \\ X \arrow[u, "\iota"] \arrow[r, "f"'] & Y \end{tikzcd}$$

Proof. We may identify Y with a subspace of its completion $\widehat{Y}$, and f can then be considered as a uniformly continuous mapping of X into $\widehat{Y}$. By virtue of Theorem 2.2.30, f is then of the form $f = g \circ \iota$, where g is a uniformly continuous mapping of $\widehat{X}$ into $\widehat{Y}$. If h is the restriction of g to $\iota(X)$, then clearly $f = h \circ \iota$, and h maps $\iota(X)$ into Y. The uniqueness of h is trivial. □

Definition 2.2.37. *The Hausdorff uniform space $\iota(X)$ defined in the proof of Theorem 2.2.30 is called the* ***Hausdorff uniform space associated with X****.*

The Hausdorff completion of X is thus the completion of the Hausdorff uniform space associated with X.

Corollary 2.2.38. *Let X, Y be two uniform spaces and X', Y' the associated Hausdorff spaces. For each uniformry continuous mapping $f : X \to Y$ there is a unique uniformry continuous mapping $f : X' \to Y'$ for which the diagram*

$$\begin{tikzcd} X' \arrow[r, "f'"] & Y' \\ X \arrow[u] \arrow[r, "f"] & Y \arrow[u] \end{tikzcd}$$

is commutative.

The Hausdorff space associated with a uniform space may also be characterized by the following property:

Proposition 2.2.39. *Let X be a uniform space, $\iota(X)$ its associated Hausdotff space, and let f be a mapping of X onto a Hausdorff uniform space X', such that the uniformiry of X is the inverse image under f of the uniformity of X'. Then the mapping $g : \iota(X) \to X'$ such that $f = g \circ \iota$ is an isomorphism.*

Proof. By Proposition 2.2.36, g is uniformly continuous; also g is obviously surjective, and is also injective because the relation $f(x) = f(y)$ implies by definition that (x, y) belongs to all the entourages of X, and therefore that $\iota(x) = \iota(y)$ (Proposition 2.2.32). Finally, the entourages of X' are the images under $f \times f$ of the entourages of X, hence they are also the images under $g \times g$ of the entourages of $\iota(X)$; hence the result. □

2.2.7 Completion of subspaces and product spaces

Proposition 2.2.40. *Let X be a set, let $(Y_i)_{i\in I}$ be a family of uniform spaces, and for each $i \in I$ let f_i be a mapping of X into Y_i. Let X carry the initial uniformity $\mathfrak{U}$ with respect to the maps $(f_i)_{i\in I}$. Then the Hausdorff completion $\widehat{X}$ of X carries the initial uniformity with respect to the maps $(\hat{f}_i)_{i\in I}$. Furthermore, if ι_i is the canonical mapping of Y_i into $\widehat{Y}_i$, and if $g_i = \iota_i \circ f_i$, then X may be identified with the closure in $\prod_{i\in I} \widehat{Y}_i$ of the image of X under the mapping $x \mapsto (g_i(x))$.*

Proof. Let X' (resp. Y_i') be the Hausdorff uniform space associated with X (resp. Y_i'), and let $f_i' : X' \to Y_i'$ be the uniformly continuous mapping which makes the diagram

$$\begin{tikzcd} X' \arrow[r, "f_i'"] & Y_i' \\ X \arrow[u, "\iota"] \arrow[r, "f_i"] & Y_i \arrow[u, "\iota_i"'] \end{tikzcd}$$

commutative. The transitivity of initial uniformities shows on the one hand that $\mathfrak{U}$ is the coarsest uniformity for which the mappings $\iota_i \circ f_i : X \to \widehat{Y}_i$ are uniformly continuous and on the other hand that $\mathfrak{U}$ is also the inverse image under ι of the coarsest uniformity $\mathfrak{U}'$ on the set $\widehat{X}$ for which the $\hat{f}_i$ are uniformly continuous. Now $\mathfrak{U}'$ is Hausdorff, for if x_1, x_2 are two points of X such that $\iota_i(f_i(x_1)) = \iota_i(f_i(x_2))$ for each $i \in I$, then (x_1, x_2) belongs to all the entourages of $\mathfrak{U}$

and hence $\iota(x_1) = \iota(x_2)$. It then follows from Proposition 2.2.39 that $\mathfrak{U}'$ is the uniformity of the Hausdorff space X' associated with X.

The bijection $x' \mapsto (f_i'(x'))$ identifies X' with a uniform subspace of the product $\prod_{i\in I} Y_i'$. Since the Y_i' are Hausdorff, each Y_i' can be identified with a dense subspace of its completion $\widehat{Y_i}$, and hence $\prod_{i\in I} Y_i'$ can be identified with a dense subspace of $\prod_{i\in I} \widehat{Y_i}$. But $\prod_{i\in I} \widehat{Y_i}$ is Hausdorff and complete; the closure $\overline{X'}$ of X' in $\prod_{i\in I} \widehat{Y_i}$ is therefore a complete Hausdorff subspace which can be identified with the Hausdorff completion $\widehat{X}$ of X; under this identification the mappings $\hat{f}_i$ become the projections onto the factors $\widehat{Y_i}$, and the proposition is proved. □

Corollary 2.2.41. *Let X be a uniform space and ι be the canonical mapping of X into its Hausdorff completion $\widehat{X}$; let A be a subspace of X and $j : A \to X$ the canonical injection. Then $\hat{j} : \widehat{A} \to \widehat{X}$ is an isomorphism of $\widehat{A}$ onto the closure of $\iota(A)$ in X.*

Corollary 2.2.42. *Let $(Y_i)_{i\in I}$ be a family of uniform spaces. Then the Hausdorff completion of the product space $\prod_{i\in I} Y_i$ is canonically isomorphic to the product $\prod_{i\in I} \widehat{Y_i}$.*

2.3 Compact space and uniform spaces

2.3.1 Uniformity for compact Hausdorff spaces

A uniformiry on a topological space X is said to be compatible with the topology of X if the latter coincides with the topology induced by the uniformiry. A topological space is said to be **uniformizable**, and its topology is said to be **uniformizable**, if there exists a uniformity on the space which is compatible with its topology. There are topological spaces which are not uniformizable, for example any space which is not T_3; hence the question arises of determining under what conditions a topological space is uniformizable.

We shall not give a complete answer to this question here. In this part we shall examine only one important particular case, that in which X is compact. We have then the following theorem:

Theorem 2.3.1. *On a Hausdorff compact space X there is exactly one uniformity compatible with the topology of X; the entourages of this uniformity are all the neighbourhoods of the diagonal Δ in $X \times X$. Furthermore, X endowed with this uniformity is a complete uniform space.*

Proof. The last part of the theorem is straightforward; for every Cauchy filter on X has a cluster point and is therefore convergent.

Let us show next that if there is a uniformity on X compatible with the topology of X, then the set $\mathfrak{U}$ of entourages of this uniformity is the set of all neighbourhoods of Δ. We know already that every entourage is a neighbourhood of Δ, hence we have to show that conversely every neighbourhood of Δ belongs to $\mathfrak{U}$. Suppose that there is a neighbourhood U of Δ which is not in $\mathfrak{U}$; then since no element in $\mathfrak{U}$ is contained in U, the sets $V \setminus U$, as V runs through $\mathfrak{U}$, form a base of a filter $\mathfrak{G}$ on the compact space $X \times X$; consequently $\mathfrak{G}$ has a cluster point (a, b) not belonging to Δ. Since $\mathfrak{U}$ is a filter coarser than $\mathfrak{G}$, (a, b) is also a cluster point of $\mathfrak{U}$. But the uniformity defined by $\mathfrak{U}$ is Hausdorff by hypothesis; hence the intersection of the closures of the sets of $\mathfrak{U}$ is Δ; thus we arrive at a contradiction.

It remains therefore to show that the set $\mathfrak{U}$ of neighbourhoods of Δ in $X \times X$ is the set of entourages of a uniformity compatible with the topology of X. For this it is enough to show

that $\mathfrak{U}$ is the set of entourages of a Hausdorff uniformity on X; for then the topology induced by this uniformity will be coarser than the topology of X and must therefore coincide with the latter.

It is clear that $\mathfrak{B}$ is a filter. Let us show that axioms (U2) and (U3) are also satisfied and that Δ is the intersection of the sets of $\mathfrak{B}$. Take the last point first: every set consisting of a single point $(x, y) \in X \times X$ is closed, since X is Hausdorff; hence if $x \neq y$, the complement of (x, y) in $X \times X$ is a neighbourhood of a. Since the symmetry $(x, y) \mapsto (y, x)$ is a homeomorphism of $X \times X$ onto itself, it follows that $V \in \mathfrak{B}$ implies $V^{-1} \in \mathfrak{B}$, whence (U2); Finally, suppose that (U3) is not satisfied; then there is a set $V \in \mathfrak{B}$ such that for all $W \in \mathfrak{B}$ the set $W^2 \setminus V$ is not empty; the sets $W^2 \setminus V$, as W runs through $\mathfrak{B}$, therefore form a filter base on $X \times X$, and this filter base has a cluster point (x, y) not in Δ. Now, since X is Hausdorff, it is regular, so there are disjoint open neighbourhoods U_1 of x and U_2 of y, and there are closed neighbourhoods $V_1 \subseteq U_1$, $V_2 \subseteq U_2$ of x and y respectively. Let $U_3 = (V_1 \cup V_2)^c$, and consider the following neighbourhood of Δ:

$$W = \bigcup_{i=1}^{3} (U_i \times U_i).$$

It follows immediately from these definitions that if $(u, v) \in W$ and $u \in V_1$ (resp. $u \in U_1$) then we must have $v \in U_1$ (resp. $v \in U_1 \cup U_3 = V_2^c$); hence the neighbourhood $V_1 \times V_2$ of (x, y) in $X \times X$ does not meet W, and we have a contradiction. This completes the proof. □

Remark 2.3.1. For every finite open covering $\mathfrak{R} = (U_i)_{i=1}^n$ of X, the set

$$V_{\mathfrak{R}} = \bigcup_{i=1}^{n} U_i$$

is a neighbourhood of Δ in $X \times X$, and these sets $V_{\mathfrak{R}}$ form a fundamental system of neighbourhoods of Δ (and therefore a fundamental system of entourages of the unique uniformity on X): Let W be any neighbourhood of Δ in $X \times X$; then for each $x \in X$ there is an open neighbourhood U_x of x in X such that $U_x \times U_x \subseteq W$. Since the $\{U_x : x \in X\}$ form an open covering of X, there exist a finite number of points $x_1, \ldots, x_n$ such that the $\{U_{x_i}\}_{i=1}^n$ form a covering $\mathfrak{R}$ of X. We have then $V_{\mathfrak{R}} \subseteq W$, which proves the assertion. For this reason the unique uniformity on X is often called the uniformity of finite open coverings.

Corollary 2.3.2. *Every subspace of a compact space is uniformizable, every locally compact space is uniformizable.*

Proof. Note that a locally compact space can be embedded into a compact space. □

It can happen that there are several distinct uniformities compatible with the topology of a locally compact space. For example, we have seen that on an infinite discrete space there is more than one distinct uniformity compatible with the discrete topology.

Theorem 2.3.3. *Every continuous mapping f of a compact space X into a uniform space Y is uniformly continuous.*

Proof. Let $g = f \times f$, then g is continuous on $X \times X$; hence for each open entourage V of Y, $g^{-1}(V)$ is an open subset of $X \times X$, which evidently contains the diagonal. The theorem thus

follows from Theorem 2.3.1, since the open entourages of Y form a fundamental system of entourages. □

Corollary 2.3.4. *Let A be a dense subspace of a compact space X, and let f be a mapping of A into a complete Hausdorff uniform space Y. Then f can be extended by continuity to the whole of X if and only if f is uniformly continuous.*

2.3.2 Compactness of uniform spaces

Definition 2.3.5. *A uniform space X is said to be precompact if its Hausdorff completion $\widehat{X}$ is compact. A subset A of a uniform space X is said to be a precompact subset if the uniform subspace A of X is precompact.*

Thus a subset A of a uniform space X is precompact if and only if the closure of $\iota(A)$ in $\widehat{X}$ is compact.

Example 2.3.6. In any uniform space X, the set of points of Cauchy sequence (x_n) is precompact. Since the images of the x_n in $\widehat{X}$ again form a Cauchy sequence, we can assume that X is Hausdorff; the closure in $\widehat{X}$ of the set of points x_n then consists of the points x_n and $\lim_n x_n$ and is therefore compact.

Besides precompactness, we introduce another concept which is frequently used. A subset A of a uniform space X is called totally bounded if, for each entourage V of X, there is a finite covering of A by V-small sets. The following theorem for precompactness and totally boundedness is fundamental and important.

Theorem 2.3.7. *A subset A of a uniform space X is precompact if and only if it is totally bounded.*

Proof. Since the completion $\widehat{A}$ is identified as a subspace of $\widehat{X}$, we may prove the result for X. Let $\iota : X \to \widehat{X}$ be the canonical mapping, then the entourages of X are the inverse images under $\iota \times \iota$ of the entourages of $\widehat{X}$. Suppose X is precompact, and let U be any entourage of $\widehat{X}$; then there is a symmetric entourage W of $\widehat{X}$ such that $W \circ W \subseteq U$. Since $\widehat{X}$ is compact, there exist a finite number of points $x_1, \dots, x_n \in \widehat{X}$ such that the $W(x_i)$ (which are U-small) cover X. If V is the inverse image of U by $\iota \times \iota$, then the sets $\iota^{-1}(W(x_i))$ are V-small and cover X. This proves X is totally bounded.

Conversely, suppose that for each entourage V of X there is a finite covering of X by V-small sets. We have to show that every ultrafilter $\mathfrak{F}$ on $\widehat{X}$ is convergent; since $\widehat{X}$ is complete, it is enough to show that $\mathfrak{F}$ is a Cauchy filter, i.e. that for each closed entourage U of $\widehat{X}$ there is a U-small set in $\mathfrak{F}$ (Corollary 2.1.14). Let V be the inverse image of U under $\iota \times \iota$, and let (B_j) be a finite covering of X by V-small sets; then the sets $C_j = \iota(B_j)$ are U-small and cover $\iota(X)$, so that

$$\widehat{X} = \bigcup_j \overline{C}_j.$$

On the other hand, since $C_j \times C_j \subseteq U$, and U closed in $X \times X$, we have $\overline{C}_j \times \overline{C}_j \subseteq U$, so that the $\overline{C}_j$ are also U-small. Since $\mathfrak{F}$ is an ultrafilter, one of the $\overline{C}_j$ belongs to $\mathfrak{F}$. □

Corollary 2.3.8. *A uniform space X is compact if and onry if it is Hausdorff, complete and totally bounded.*

Proposition 2.3.9. *In a uniform space every subset of a precompact set, every finite union of precompact sets and the closure of every precompact set are precompact.*

Proof. The first two assertions are immediate consequences of Theorem 2.3.7. Let X be a uniform space, A a precompact subset of X, and let $\iota : X \to \widehat{X}$ be the canonical mapping. By continuity, $\iota(\overline{A})$ is contained in the closure of $\iota(A)$ in X, hence the closure of $\iota(\overline{A})$ in $\widehat{X}$ is contained in a compact set and is therefore compact. □

Remark 2.3.2. In a uniform space X a relatively compact set A is precompact, since A is contained in a compact set. On the other hand, even if X is Hausdorff, a precompact set need not be relativefy compact in X, as is shown by the case where X itself is precompact but not compact.

Proposition 2.3.10. *Let $f : X \to Y$ be a uniformly continuous mapping. If A is any precompact subset of X, then $f(A)$ is a precompact subset of Y.*

Proof. For if $\iota_X : X \to \widehat{X}$ and $\iota_Y : Y \to \widehat{Y}$ are the canonical mappings, we have $\iota_Y(f(A)) = \hat{f}(\iota_X(A))$ and hence $\iota_Y(f(A))$ is relatively compact in Y. □

Proposition 2.3.11. *Let X be a set, let $(Y_i)_{i\in I}$ be a famiry of uniform spaces, and for each $i \in I$ let A be a mapping of X into Y_i. Let X carry the initial uniformity with respect to $(f_i)_{i\in I}$. Then a subset A of X is precompact if and onry if $f_i(A)$ is a precompact subset of Y_i for each $i \in I$.*

Proof. The condition is necessary by virtue of Proposition 2.3.10. Sufficiency follows from the characterization of the Hausdorff completion of X given in Proposition 2.2.40, and Tychonoff's theorem. □

To conclude, we prove the following two properties of compact subset of a uniform space.

Proposition 2.3.12. *In a uniform space X, let A be a compact set and B a closed set such that $A \cap B = \varnothing$. Then there is an entourage V of X such that $V(A)$ and $V(B)$ do not intersect.*

Proof. If the proposition were false, then none of the sets $A \cap V^2(B)$, where V runs through the set of symmetric entourages of X, would be empty; hence these sets would form a filter base on A, which would have a cluster a point $x_0 \in A$. Hence for each symmetric entourage V of X, $V(x_0)$ would meet B and therefore, as B is closed, we should have $x_0 \in B$, contrary to hypothesis. □

Corollary 2.3.13. *Let A be a compact set in a uniform space X; then as V runs through the set of entourages of X, the sets $V(A)$ form a fundamental system of neighbourhoods of A.*

Proof. Let U be any open neighbourhood of A, then $B = U^c$ is closed and does not meet A; hence, by Proposition 2.3.12, there is an entourage V such that $V(A) \cap V(B) = \varnothing$, and therefore $V(A) \subseteq U$. □

Chapter 3

Topological groups and rings

3.1 Topological groups

3.1.1 Topologies on groups

Definition 3.1.1. *A topological group is a set G which cames a group structure and a topology and satisfies the following two axioms:*

(GT1) The mapping $(x, y) \mapsto xy$ of $G \times G$ into G is continuous.

(GT2) The mapping $x \mapsto x^{-1}$ of G into G is continuous.

A group structure and a topology on a set G are said to be compatible if they satisfy (GT1) and (GT2). An immediate consequence of the axioms is that translation and inversion are homeomorphisms. We show next that translates of neighborhoods V of e constitute the neighborhoods of g.

Proposition 3.1.2. *If $\mathcal{B}$ is a neighborhood base at e in a topological group G, then for any $g \in G$, $g\mathcal{B}$ is a neighborhood base for $\mathfrak{B}(g)$.*

Proof. The map R_g is a homeomorphism taking e into g. Its inverse is the map $R_{g^{-1}}$. Thus if $V \in \mathfrak{U}(g)$, then $g^{-1}V$ is a neighborhood of 0. Since $\mathcal{B}$ is a base, there exists $B \in \mathcal{B}$ such that $B \subseteq g^{-1}V$. Hence $gB \subseteq V$ and $g\mathcal{B}$ is a neighborhood base at g. □

Recall that a topological space X is **homogeneous** if, given any two points $x, y \in X$ there is a homeomorphism of X onto X mapping x into y. If X is a topological group and $x, y \in X$, the translation map $R_{x^{-1}y}$ is a homeomorphism which takes x into y; hence any topological group is homogeneous. A consequence of this fact is the following.

Proposition 3.1.3. *A homomorphism mapping one topological group into another continuous at one point is continuous.*

Proof. Suppose that G aud H are topological groups and that $f : G \to H$ is a homomorphism. Suppose that f is continuous at $g_0 \in G$. To see that f is continuous everywhere, let $g \in G$ and suppose that the net $g_\alpha \to g$. Then $g_0 g^{-1} g_\alpha \to g_0$. Since f is continuous at g_0,

$$f(g_0 g^{-1} g_\alpha) = f(g_0) f(g^{-1}) f(g_\alpha) \to f(g_0).$$

which implies that $f(g_\alpha) \to g$ and proves the continuity of f at g. □

Finally, we consider the neighborhood base at e of a topological group G. Many important result depends on the property of $\mathfrak{B}(e)$, which we now establish.

Proposition 3.1.4. *Suppose G is a topological group and let $\mathfrak{B}$ be the neighbourhood filter of the identity element of G. Then $\mathfrak{B}$ satisfies the following conditions.*

(GV1) Given any $U \in \mathfrak{B}$, there exists $V \in \mathfrak{B}$ such that $VV \subseteq U$.

(GV2) Given any $U \in \mathfrak{B}$, we have $U^{-1} \in \mathfrak{B}$.

(GV3) For all $g \in G$ and all $V \in \mathfrak{B}$, we have $gVg^{-1} \in \mathfrak{B}$.

Conversely, if $\mathfrak{B}$ is a filter on G satisfying the three conditions, then there is a unique topology on G, compatible with the group structure of G, for which $\mathfrak{B}$ is the neighbourhood filter of the identity element e.

Proof. Since the may $(x, y) \mapsto xy$ and $x \mapsto x^{-1}$ are continuous at $x = y = e$, we obtain. Also, $x \mapsto gxg^{-1}$ is a homeomorphism which leaves e fixed, so (GV3) follows.

Conversely, assume that $\mathfrak{B}$ is a filter on G satisfying these properties. If there is a topology with the required properties, then by what has been said above the neighbourhood filter of g coincides with each of the filters $g\mathfrak{B}$ and $\mathfrak{B}g$; hence the topology is unique, if it exists. Its existence will be established if we show that the filters $g\mathfrak{B}$ are the neighbourhood filters of a topology on G, and that this topology is compatible with the group structure of G.

The filter $g\mathfrak{B}$ satisfies axiom (V3) by reason of (GV1) and (GV2) , as we have already seen; hence to show that $g\mathfrak{B}$ is the neighbourhood filter of g in a topology on G, we have to verify axiom (V4). Let then V be any set of $\mathfrak{B}$, and W a set of $\mathfrak{B}$ such that $WW \subseteq V$; then for any $x \in gW$ we have $xW \subseteq gWW \subseteq gV$, so that gV belongs to the filter $g\mathfrak{B}$; hence (V4) is satisfied.

Let us now show that the topology defined by the neighbourhood filters $g\mathfrak{B}$ satisfies (GT2) and (GT3). Let a, b be any two points of G; if we put $x = au$ and $y = bv$, then we have to show that xy^{-1} is as near as we please to ab^{-1} whenever u and v are close enough to e. Note that $(ab^{-1})^{-1}(xy^{-1}) = buv^{-1}b^{-1}$; let U be any neighbourhood of e, then we shall have $buv^{-1}b^{-1} \in U$ if $uv^{-1} \in b^{-1}Ub = V$. Now $V \in \mathfrak{B}$ by reason of (GV3), and by (GV1) and (GV2) there exists $W \in \mathfrak{B}$ such that $WW^{-1} \in V$; hence it is enough to take $u \in W$ and $v \in W$. This completes the proof. □

A neighbourhood of e which coincides with its image under the symmetry $x \mapsto x^{-1}$ is said to be **symmetric**. If V is any neighbourhood of e, then VV^{-1}, $V \cap V^{-1}$ and $V \cup V^{-1}$ are symmetric neighbourhoods. By (GV2), the symmetric neighbourhoods form a fundamental system of neighbourhoods of e. Also it follows from (GV1) that when V runs through a fundamental system of neighbourhoods of e, the sets V^n (where n is a fixed nonzero integer) form a fundamental system of neighbourhoods of e.

Corollary 3.1.5. *Suppose G is a topological group and $\mathfrak{B}(e)$ be the neighborhood base of the identity and $\mathfrak{S}(e)$ be the symmetric neighborhood base of the identity. Then*

$$\overline{\{e\}} = \bigcap \mathfrak{B}(e) = \bigcap \mathfrak{S}(e).$$

Proof. Since $\mathfrak{B}(e)$ is a neighborhood base of e, it suffices to prove $\overline{\{e\}} = \bigcap \mathfrak{B}(e)$. If $g \in \overline{\{e\}}$, then for every $U \in \mathfrak{S}(e)$, the set gU meets $\{e\}$. That is, $e \in gU$. Since U is symmetric, this implies

$g \in U$ for all $U \in \mathfrak{S}(e)$. Conversely, if $g \in \bigcap \mathfrak{S}(e)$ then $g^{-1} \in \bigcap \mathfrak{S}(e)$. Hence $e \in gU$ for any $U \in \bigcap \mathfrak{S}(e)$, which implies $g \in \overline{\{e\}}$. □

Corollary 3.1.6. *A topological group G is Hausdorff if and only if the intersection of the neighbourhoods of e consists only of the point e.*

Example 3.1.7. If $\mathfrak{B}$ is is a filter base on a group G consists of subgroups of G, then it is immediately seen that is satisfies axioms (GV1) and (GV2), since $HH^{-1} = H$ for any subgroup H of G. Hence the set $\mathcal{B}$ is will be a fundamental system of neighbourhoods of e in a topology compatible with the group structure of G, provided that is satisfies (GV3); this will in particular be the case if all the subgroups in $\mathfrak{B}$ are normal, hence always if G is commutative. The topology thus defined is Hausdorff, by Corollary 3.1.6, if and only if the intersection of all the subgroups in $\mathfrak{B}$ consists only of e. The most interesting cases are those in which the subgroup $\{e\}$ is not in $\mathfrak{B}$, since otherwise the topology defined by $\mathfrak{B}$ is the discrete topology: if $\{e\} \notin \mathfrak{B}$, the topology defined by $\mathfrak{B}$ is Hausdorff only if $\mathfrak{B}$ is an infinite set.

Since the intersection of two subgroups is a subgroup, we can define a topology on G, compatible with its group structure, starting from any set $\mathfrak{F}$ of subgroups of G: let $\mathfrak{S}$ be the set of all subgroups gHg^{-1}, where $H \in \mathfrak{F}$ and $g \in G$, and let $\mathfrak{B}$ be the set of all finite intersections of subgroups belonging to $\mathfrak{S}$. Then $\mathfrak{B}$ is a filter base and satisfies (GV3).

Consider in particular the additive group of a ring A. Every set $\mathfrak{F}$ of ideals of A defines a topology compatible with this additive group structure. This topology is Hausdorff if the intersection of all the ideals of $\mathfrak{F}$ is the zero ideal, and it is not discrete if no finite intersection of the ideals of $\mathfrak{F}$ is the zero ideal. Topologies defined in this way play a large part in the theory of numbers.

Proposition 3.1.8. *Let G be a topological group. If U is open in G and B is a subset of G, then UB and BU are open.*

Proof. Note that $BU = \bigcup_{b \in B} bU$ and $UB = \bigcup_{b \in B} Ub$, so the claim follows from the fact that $g \mapsto bg$ and $g \mapsto gb$ are homeomorphisms. □

Example 3.1.9. Let $G = (\mathbb{R}, +)$, the additive topological group of real numbers with the usual topology. The sets $A = \{n \in \mathbb{N} : n \geq 2\}$ and $B = \{-n - 1/n : n \geq 2\}$ are closed but $A + B$ contains $\{-1/n : n \geq 2\}$ which has 0 as a limit point so $A + B$ is not closed.

The product of a compact set and a closed set is generally closed, however. We prove this after establishing the following result.

Proposition 3.1.10. *Let G be a topological group, let K be a compact subset of G, and let U be an open neighborhood of K. Then there are open neighborhoods V_R and V_L of e such that $KV_R \subseteq U$ and $V_L K \subseteq U$.*

Proof. For each x in K choose open neighborhoods W_x and V_x of e such that $xW_x \subseteq U$ and $V_x V_x \subseteq W_x$. Then $\{xV_x\}_{x \in K}$ is an open cover of the compact set K, and so there is a finite collection $x_1, \ldots, x_n$ of points in K such that the sets $\{x_i V_{x_i} : i = 1, \ldots, n\}$ cover K. Let $V_R = \bigcap_{i=1}^n V_{x_i}$. If $x \in K$, then there is an index i such that $x \in x_i V_{x_i}$, and so

$$xV_R \subseteq x_i V_{x_i} V_{x_i} \subseteq x_i W_{x_i} \subseteq U.$$

Since x was an arbitrary element of K, it follows that $KV_R \subseteq U$. The construction of V_L is similar. □

Proposition 3.1.11. *Let G be a topological group. If K is compact in G and F is closed, then KF and FK are closed.*

Proof. Let $g \in \overline{KF}$. Then for any neighborhood U of e,

$$(gU) \cap (KF) \neq \varnothing \iff (K^{-1}gU) \cap F \neq \varnothing. \tag{1.1.1}$$

To show that $g \in KF$, first observe that if $K^{-1}g \cap F = \varnothing$, then the compact set $K^{-1}g$ is contained in F^c, so by Proposition 3.1.10 there is some neighborhood V of e such that $(K^{-1}gV) \cap F = \varnothing$. This contradicts (1.1.1), so the claim follows. The result for FK can be proved similarly, using a modified version of Proposition 3.1.10. □

As a final word on interior, closure, and multiplication, we prove the following result.

Proposition 3.1.12. *If A and B are subsets of a topological group, then*

$$\overline{A}\,\overline{B} \subseteq \overline{AB}, \quad (\operatorname{Int} A)(\operatorname{Int} B) \subseteq A(\operatorname{Int} B) \subseteq \operatorname{Int}(AB).$$

Proof. Let $g \in \overline{A}$ and $h \in \overline{B}$, and U be a neighborhod of e. By the continuity of product, there exists neighborhoods W_1, W_2 of e such that

$$(gW_1)(hW_2) \subseteq ghU.$$

Since $g \in \overline{A}$ and $h \in \overline{B}$, there exists $a \in A \cap (gW_1)$ and $b \in B \cap (hW_2)$. Then $ab \in AB \cap (ghU)$, and so $gh \in \overline{AB}$.

For the interiors, it is clear that $(\operatorname{Int} A)(\operatorname{Int} B) \subseteq A(\operatorname{Int} B)$. Also, by Proposition 3.1.8, $A(\operatorname{Int} B)$ is open. Since it is contained in AB, we get $A(\operatorname{Int} B) \subseteq \operatorname{Int}(AB)$. □

Proposition 3.1.13. *Let G be a topological group.*

(a) Suppose that G is connected and that the identity element of G has a compact neighborhood C. Then G is σ-compact.

(b) Suppose that G is σ-compact. Then there exists for every neighborhood U of the identity element e of G a sequence $\{g_n\}$ in G such that $G = \bigcup_n g_n U$.

(c) If G is σ-compact and first countable, then G is second countable.

Proof. First we prove (a). Since G is connected, G is generated by C. Replacing C by the compact subset $C \cup C^{-1}$, we see $G = \bigcup_n C^n$ with $C^n = \{g_1 g_2 \cdots g_n : g_i \in C\}$. But C^n is compact, as the image of the compact n-fold product $C \times \cdots \times C$ under the n-fold multiplication map $G \times \cdots \times G$. Therefore G is σ-compact.

Now for (b), suppose $G = \bigcup_n K_n$ with $K_n \subseteq G$ compact. For each fixed n, we have a cover of the compact set K_n:

$$\{gU : g \in K_n\}$$

Therefore there exist $g_{n,1}, \dots, g_{n,r_n} \in K_n$ with $K_n \subseteq \bigcup_{i=1}^{r_n} g_{n,i}U$, and hence

$$G \subseteq \bigcup_{n\in\mathbb{N}} \bigcup_{i=1}^{r_n} g_{n,i}U$$

Renumbering the countably many $g_{n,i}$ yields the desired result.

Finally, assume that G is σ-compact and first countable. Let $\{U_n\}_{n\in\mathbb{N}}$ be a fundamental system of neighborhoods of e. Then by Proposition 3.1.4, for all $n \in \mathbb{N}$ there exists $m \in \mathbb{N}$ such that $U_m^{-1}U_m \subseteq U_n$.

By (b), there exist for all $n \in \mathbb{N}$ sequences $(g_{n,k})_k$ in G such that $G = \bigcup_{k\in\mathbb{N}} g_{n,k}U_n$. We show that

$$\mathcal{U} := \{g_{n,k}U_n : k, n \in \mathbb{N}\}$$

is a basis of the topology of G. In fact, let V be an open subset of G and $g \in V$. Then there exists $n \in \mathbb{N}$ such that $gU_n \subseteq V$, and we may choose $m \in \mathbb{N}$ such that $U_m^{-1}U_m \subseteq U_n$. Since $\{g_{m,k}U_m\}$ covers G, there is some $k \in \mathbb{N}$ such that $g \in g_{m,k}U_m$. Now

$$g_{m,k}U_m \subseteq gU_m^{-1}U_m \subseteq gU_n \subseteq V$$

Thus the claim follows. □

Corollary 3.1.14. *A connected locally compact first countable topological group is second countable.*

Proof. This is a combination of Proposition 3.1.13 (a) and (c). □

3.1.2 Topological subgroups

Proposition 3.1.15. *Let G be a topological group and let $H \subseteq G$ be a subgroup. Then its closure $\overline{H}$ is also a subgroup. If H is normal, then $\overline{H}$ is also normal.*

Proof. Consider the continuous map $\sigma(x, y) = xy^{-1}$. It suffices if we show $\sigma(\overline{H} \times \overline{H}) \subseteq \overline{H}$, or equivalently $\overline{H} \times \overline{H} \subseteq \sigma^{-1}(\overline{H})$. First note that, since H is a subgroup,

$$H \times H \subseteq \sigma^{-1}(H) \subseteq \sigma^{-1}(\overline{H}),$$

thus, by taking closure we get $\overline{H \times H} \subseteq \sigma^{-1}(\overline{H})$. Now the claim follows from the inclusion $\overline{H} \times \overline{H} \subseteq \overline{H \times H}$.

If H is normal, then the map $(g, x) \mapsto gxg^{-1}$ is continuous and maps $G \times H$ into H. Then it maps $G \times \overline{H}$ into $\overline{H}$, so $\overline{H}$ is also continuous. □

As a result, it is clear that $\overline{\{e\}}$ is a subgroup in any topological group. An interesting consequence of thie proposition is the following.

Corollary 3.1.16. *A locally closed subgroup is closed.*

Proof. Let $H \subseteq G$ be a locally closed subgroup, then H is open and dense in $\overline{H}$, which is also a subgroup. Now let $h \in \overline{H}$, then hH and H are both open dense subset of $\overline{H}$, so they intersect: $hH \cap H \neq \varnothing$. This means $h \in H$, so $H = \overline{H}$ is closed. □

Proposition 3.1.17. *Suppose G is a topological group.*

(a) Every open subgroup of G is also closed, hence a union of components.

(b) For any neighborhood U of e, the subgroup $\langle U \rangle$ generated by U is open and closed in G.

(c) For any connected subset $U \subseteq G$ containing e, the subgroup $\langle U \rangle$ is connected.

(d) If G is connected, then every connected neighborhood of e generates G.

Proof. First, let H be an open subgroup of G, then every left coset $gH = \{gh : h \in H\}$ is also open in G because it is the image of H under the homeomorphism L_g. Because $G - H$ is the union of the cosets of H other than H itself, it is open, and therefore H is closed in G. Because H is both open and closed, it is a union of components. This proves (a).

For (b), let $U \subseteq G$ be any neighborhood of the identity, and let H be the subgroup generated by U. As a matter of notation, if A and B are subsets of G, let us write

$$AB = \{ab : a \in A, b \in B\}, \quad A^{-1} = \{a^{-1} : a \in A\}.$$

For each positive integer k, let W_k denote the set of all elements of G that can be expressed as products of k or fewer elements of $W \cup W^{-1}$. Then H is the union of all the sets W_k as k ranges over the positive integers. Now, W^{-1} is open because it is the image of W under the inversion map, which is a diffeomorphism. Thus, $W_1 = W \cup W^{-1}$ is open, and for each $k > 1$ we have

$$W_k = W_1 W_{k-1} = \bigcup_{g \in W_1} L_g(W_{k-1})$$

Because each L_g is a diffeomorphism, it follows by induction that each W_k is open, and thus H is open.

Now we prove (c). Suppose U is connected. Then W^{-1} is also connected because it is a homeomorphic image of W, and $W_1 = W \cup W^{-1}$ is connected because it is a union of connected sets with the identity in common. Therefore, $W_2 = m(W_1 \times W_1)$ is connected because it is the image of a connected space under the continuous multiplication map m, and it follows by induction that $W_k = m(W_1 \times W_{k-1})$ is connected for each k. Thus, $H = \bigcup_k W_k$ is connected because it is a union of connected subsets with the identity in common.

Finally, we deal with (d). Assume that G is connected. Since H is an open subgroup, it is also closed by (a), and it is not empty because it contains the identity. Thus $H = G$. □

Proposition 3.1.18. *In a topological group G, the component C of the identity element e is a closed normal subgroup. The component of a point $g \in G$ is the coset $gC = Cg$.*

The component of the identity element e of G is called the **identity component** of G.

Proof. If $a \in C$, then $a^{-1}C$ is connected and contains a; hence $C^{-1}C \subseteq C$, which shows that C is a subgroup of G. This subgroup is invariant under all automorphisms of G, and in particular under all inner automorphisms, therefore C is normal in G; also C is close since it is a maximal connected subset. Finally, the left translation $x \mapsto gx$ is a homeomorphism of G which sends e to g, and hence the component of g is gK. □

Proposition 3.1.19. *A subgroup H of a topological group G is:*

(a) open iff $\operatorname{Int} H \neq \varnothing$.

(b) closed if H is open.

(c) discrete iff H has an isolated point

Proof. If H is open then $e \in \operatorname{Int} H$. Conversely, suppose that H has an interior point g. For any h in H, the map $x \mapsto hg^{-1}x$ maps H homeomorphically onto H and maps g into h. Thus h is also an interior point of H. Thus H is open. Part (b) is established in Proposition 3.1.17, and (c) can be proved similarly. □

3.1.3 Group actions

If G is a topological group and $g \in G$, left translation by g is the map $L_g : G \to G$ defined by $L_g(g') = gg'$. It is continuous, because it is equal to the composition

$$G \xrightarrow{i_g} G \times G \xrightarrow{m} G$$

where $i_g(h) = (g, h)$ and m is group multiplication. Because $L_g \circ L_{g^{-1}} = \mathrm{id}_G$, left translation by any element of g is a homeomorphism of G. Similarly, right translation by g, $R_g(h) = hg$, is also a homeomorphism. A topological space X is said to be topologically homogeneous if for any $x, y \in X$, there is a homeomorphism $\varphi : X \to X$ taking x to y. Every topological group G is topologically homogeneous.

Definition 3.1.20. *Suppose G is a group (not necessarily a topological group for now), and X is a set. A left action of G on X is a map $G \times X \to X$, written $(g, x) \mapsto g \cdot x$, with the following properties:*

(a) $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$ for all $x \in X$ and all $g_1, g_2 \in G$.

(b) $1 \cdot x = x$ for all $x \in X$.

Similarly, a right action is a map $X \times G \to X$, written $(x, g) \mapsto x \cdot g$, with the same properties except that composition works in reverse: $(x \cdot g_1) \cdot g_2 = x \cdot (g_1 g_2)$.

Now, suppose X is a topological space and G is a group acting on X. The action is called an action by homeomorphisms if for each $g \in G$, the map $x \mapsto g \cdot x$ is a homeomorphism of X. If in addition G is a topological group, the action is said to be continuous if the map $G \times X \to X$ is continuous. The next proposition explains the relationship between the two concepts.

Proposition 3.1.21. *Suppose G is a topological group acting on a topological space X.*

(a) If the action is continuous, then it is an action by homeomorphisms.

(b) If G has the discrete topology, then the action is continuous if and only if it is an action by homeomorphisms.

Proof. First suppose the action is continuous. Then as the composition $x \mapsto (x, g) \mapsto g \cdot x$, the map $x \mapsto g \cdot x$ is continuous for each $g \in G$, and has a continuous inverse $x \mapsto g^{-1} \cdot x$. Thus G acts by homeomorphisms.

Now, suppose G has the discrete topology. If G acts by homeomorphisms, then the map $G \times X \to X$ defined by the action is continuous when restricted to each subset of the form $\{g\} \times X$. Since these subsets form an open cover of $G \times X$, this implies that the action is continuous. □

For any $x \in X$, the set $G \cdot x = \{g \cdot x : g \in G\}$ is called the **orbit** of x. The action is said to be transitive if for every pair of points $x, y \in X$, there is a group element g such that $g \cdot x = y$, or equivalently if the orbit of each point is the entire space X. The action is said to be **free** if the only element of G that fixes any point in X is the identity, that is, if $g \cdot x = x$ for some x implies $g = 1$.

Example 3.1.22 (Continuous Group Actions).

(a) The general linear group $\mathrm{GL}(n;\mathbb{R})$ acts on the left on $\mathbb{R}^n$ by matrix multiplication, considering each vector in $\mathbb{R}^n$ as a column matrix. The action is continuous, because the component functions of $g \cdot x$ are polynomial functions of the components of g and x. Given any nonzero vector $x \in \mathbb{R}^n$, we can find vectors $(x_2, \dots, x_n)$ such that $(x, x_2, \dots, x_n)$ is a basis for $\mathbb{R}^n$, and then the matrix G with columns $(x, x_2, \dots, x_n)$ is invertible and takes the vector $(1, 0, \dots, 0)$ to x. If y is any other nonzero vector, the same argument shows that there is a matrix $h \in \mathrm{GL}(n;\mathbb{R})$ taking $(1, 0, \dots, 0)$ to y, and then hg^{-1} takes x to y. Thus there are only two orbits: $\in \mathbb{R}^n \setminus \{0\}$ and $\{0\}$.

(b) The orthogonal group $\mathrm{O}(n)$ acts continuously on $\mathbb{R}^n$ by matrix multiplication as well. This is just the restriction of the action in part (a) to $\mathrm{O}(n) \times \mathbb{R}^n \subseteq \mathrm{GL}(n;\mathbb{R}) \times \mathbb{R}^n$. Since any unit vector x can be completed to an orthonormal basis $(x, x_2, \dots, x_n)$ the argument in the preceding paragraph shows that for any two unit vectors x and y there is an orthogonal matrix taking x to y. If x and y are any two nonzero vectors with the same length, there is an orthogonal matrix taking $x/|x|$ to $y/|y|$, and this matrix also takes x to y. Since multiplication by an orthogonal matrix preserves lengths of vectors, the orbits of the $\mathrm{O}(n)$ action on $\mathbb{R}^n$ are $\{0\}$ and the spheres centered at 0.

(c) The restriction of the action of $\mathrm{O}(n)$ to the unit sphere in $\mathbb{R}^n$ yields a transitive action on $\mathbb{S}^{n-1}$.

(d) The group $\mathbb{R}^*$ acts on $\mathbb{R}^n \setminus \{0\}$ by scalar multiplication. The action is free, and the orbits are the lines through the origin (with the origin removed).

(g) Any topological group G acts continuously, freely, and transitively on itself on the left by left translation: $g \cdot g' = L_g(g') = gg'$. Similarly, G acts on itself on the right by right translation.

(f) If H is a subgroup of the topological group G (with the subspace topology), then group multiplication on the left or right defines a left or right action of H on G; it is just the restriction of the action of G on itself to $H \times G$ or $G \times H$. This action is continuous and free, but in general not transitive.

(g) The two-element discrete group $\{\pm 1\}$ or $\mathbb{Z}/2\mathbb{Z}$ acts freely on $\mathbb{S}^n$ by multiplication: $\pm 1 \cdot x = \pm x$. This is an action by homeomorphisms, and because the group is discrete, it is continuous. Each orbit is a pair of antipodal points: $\{\pm x\}$.

Given an action of a group G on a space X (not necessarily continuous or even by homeomorphisms), we define a relation on X by saying $x_1 \sim x_2$ if there is an element $g \in G$ such that $g \cdot x_1 = x_2$. This is reflexive because $1 \cdot x = x$ for each x; it is symmetric because $g \cdot x_1 = x_2$ implies $g^{-1} \cdot x_2 = x_1$; and it is transitive because $g \cdot x_1 = x2$ and $g' \cdot x_2 = x_3$ imply $g'g \cdot x_1 = x_3$.

Thus it is an equivalence relation. The equivalence classes are precisely the orbits of the group action. The resulting quotient space is denoted by X/G, and is called the orbit space of the action. If the action is transitive, the orbit space is a single point, so only nontransitive actions yield interesting examples.

Let us examine the quotients determined by some of the group actions described in Example 3.1.22.

Example 3.1.23.

(a) As we mentioned above, the action of $\mathrm{GL}(n;\mathbb{R})$ on $\mathbb{R}^n$ has two orbits, so the quotient space has exactly two points: $a = q(\mathbb{R}^n \setminus \{0\})$ and $b = q(\{0\})$. The only saturated open subsets of $\mathbb{R}^n$ are $\mathbb{R}^n$, $\mathbb{R}^n \setminus \{0\}$ and $\{0\}$, so the open subsets of the quotient space are $\{a, b\}, \{a\}, \varnothing$. This quotient space is not Hausdorff.

(b) The quotient space of $\mathbb{R}^n$ by $\mathrm{O}(n)$ is homeomorphic to $[0, \infty)$.

(c) The real projective space $\mathbb{RP}^n$ is exactly the orbit space of the action of $\mathbb{R}^*$ on $\mathbb{R}^{n+1} \setminus \{0\}$ by scalar multiplication.

A particularly important special case arises when G is a topological group and we consider the action of a subgroup $H \subseteq G$ on G. An orbit of the right action of H on G is a set of the form $\{gh : h \in H\}$, which is precisely the left coset gH . Thus the orbit space of the right action of H on G is the set G/H of left cosets with the quotient topology. This quotient space is called the (left) coset space of G by H. (It is unfortunate but unavoidable that the right action produces a left coset space and vice versa. If G is commutative, the situation is simpler, because then the left action and right action of H are equal to each other.)

Proposition 3.1.24. *If a topological group G operates continuously on a topological space X, then the equivalence relation R defined by G is open.*

Proof. For the saturation with respect to R of an open subset U of X is the set $\bigcup_{g\in G} gU$, and each gU is open. □

Let X (resp. Y) be a set with a group of operators G (resp. H) and let $\phi : G \to H$ be a homomorphism and $\psi : X \to Y$ a mapping. Then ϕ and ψ are said to be compatible if $\psi(g \cdot x) = \phi(g) \cdot \psi(x)$ for all $g \in G$ and all $x \in X$. If ϕ and ψ are continuous and compatible, passing to the quotients, ψ then induces a continuous mapping $X/G \to Y/H$.

Let G be a topological group acting continuously on a topological space X, and let π be the canonical mapping of X onto the orbit space X/G. Let A be any subset of X, and let $R(A)$ be the subspace of X which is the saturation of A with respect to the equivalence relation R defined by G (thus $R(A)$ is the union of the orbits of points of A, and is said to be the saturation of A with respect to G). Then G acts continuously on $R(A)$ by the restriction of $(g, x) \mapsto g \cdot x$ to $G \times R(A)$. Moreover, since R is open and $R(A)$ is saturated, it follows that

Proposition 3.1.25. *The canonical bijection of the subspace $\pi(A)$ onto the orbit space $R(A)/G$ is a homeomorphism.*

Now let S be an equivalence relation on X such that, for each $g \in G$, the mapping $x \mapsto g \cdot x$ is compatible with S [in other words, such that the relation xSy implies $(g \cdot x)S(g \cdot y)$; for the

sake of brevity we shall say that the relation S is compatible with the group G. If π is the canonical mapping of X onto X/S, and if $g \cdot \bar{x}$ denotes the class of $g \cdot x$, then X/S has G as groups of operators with respect to the law $(g, \bar{x}) \mapsto g \cdot \bar{x}$. Moreover:

Proposition 3.1.26. *If the equivalence relation S on X is open and compatible with G, then G operates continuously on X/S.*

Proof. Since the relation of equality on G and the relation S on X are open, it is enough to show that the mapping $(g, x) \mapsto g \cdot \pi(x) = \pi(g \cdot x)$ of $G \times X$ into X/S is continuous; but this follows from the continuity of π and of the mapping $(g, x) \mapsto g \cdot x$. □

Let G be a topological group and H a subgroup of G. Then H acts continuously on the right on G according to the multiplication $(g, h) \mapsto gh$ and the orbit of a point $g \in G$ is the left coset gH. The set of orbits is therefore what we have called in algebra the **homogeneous space** G/H.

Whenever we speak of G/H as a topological space, we shall always mean the orbit space of G (with respect to H) unless the contrary is expressly stated; i.e. the quotient space of G by the equiva1ence relation $x^{-1}y \in H$. In conformity with the general definitions, we say that the topology of this space is the **quotient by H of the topology of G**.

Proposition 3.1.27. *The group G operates continuously on every homogeneous space G/H.*

Proof. Since the equivalence relation $x^{-1}y \in H$ is open, by Proposition 3.1.26 we see the claim. □

Proposition 3.1.28. *Let G be a topological group and let H be a subgroup of G. Then the homogeneous space G/H is Hausdorff if and only if H is closed in G.*

Proof. note that H is an equivalence class for the relation $x^{-1}y \in H$ and therefore, if G/H is Hausdorff, H is closed in G. Conversely, if H is closed, then the graph of this relation is closed in $G \times G$, since it is the inverse image of H under the continuous mapping $(x, y) \mapsto x^{-1}y$, so it follows from Proposition 1.3.15 that G/H is Hausdorff. □

Proposition 3.1.29. *Let G be a topological group and let H be a subgroup of G. Then the homogeneous space G/H is discrete if and only if H is open in G.*

Proof. For the inverse images in G of the points of G/H under the canonical mapping are the cosets gH, $g \in H$; and these sets are open in G if and only if H is open in G. □

Let X be a topological space on which a topological group G acts continuously and transitively. The space X is then (in the algebraic sense) a **homogeneous space** of G. Let x be a point of x, G_x its stabilizer. The continuous surjection $g \mapsto gx$ of G onto X factorizes canonically as

$$G \xrightarrow{\pi_x} G/G_x \xrightarrow{\phi_x} X$$

where π_x is the canonical mapping of G onto the homogeneous space G/G_x and ϕ_x is the bijection $gG_x \mapsto g \cdot x$ of G/G_x onto X. Since the composition $\phi_x \circ \pi_x$ is continuous, it follows from the property of the quotient toplogy that ϕ_x is continuous. However, ϕ_x is not necessarily a homeomorphism of G/G_x onto X. If ϕ_x is a homeomorphism for *each* $x \in X$, then we say that X is a topological homogeneous space (of the topological group G).

Proposition 3.1.30. *Let X be a topological space on which a topological group G acting continuously and transitively. For X to be a topological homogeneous space (relative to G) it is necessary and sufficient that for each $x \in X$, the orbit map $g \mapsto g \cdot x$ is open.*

Proof. For each $x \in X$, denote by θ_x the orbit map, which maps g to $g \cdot x$. Then for a subset $U \subseteq G/G_x$, we have

$$\phi_x(U) = \theta_x \pi_x^{-1}(U).$$

Therefore ϕ_x is an open map if and only if θ_x is open, and this proves the claim. □

Proposition 3.1.31. *Let X be a topological space on which a topological group G acting continuously and transitively. For X to be a topological homogeneous space (relative to G) it is sufficient that for some point $x_0 \in X$ the map θ_{x_0} transforms each neighbourhood of e in G into a neighbourhood of x_0 in X.*

Proof. Every $x \in X$ can be written as $x = g \cdot x_0$ for some $g \in G$. If V is a neighbourhood of e, consider the set $V \cdot x$. We can write

$$V \cdot x = (Vg) \cdot x_0 = [g(g^{-1}Vg)] \cdot x_0.$$

Note that $g^{-1}Vg$ is a neighborhood of e, so $(g^{-1}Vg) \cdot x_0$ is a neighborhood of x_0, by hypothesis. Since $y \mapsto g \cdot y$ is a homeomorphism of X onto it self, it follows that $[g(g^{-1}Vg)] \cdot x_0$ is a neighborhood of x, thus the map θ_x is open (by translation on G) and the claim follows. □

3.1.4 Product and quotient of topological groups

If H is a normal subgroup of G then we know the homogeneous space G/H becomes a group. We now prove that this makes G/H into a topological group.

Proposition 3.1.32. *Let G be a topological group and let H be a normal subgroup of G. Then the quotient by H of the topology of G is compatible with the group structure of G/H.*

Proof. If $\pi : G \to G/H$ is the canonical mapping, then we have to show that $(\pi(x), \pi(y)) \mapsto \pi(x)\pi(y)^{-1}$ is a continuous mapping of $(G/H)\times(G/H)$ into G/H. Since the equivalence relation $x^{-1}y \in H$ is open, it is enough to show that $(x, y) \mapsto \pi(x)\pi(y)^{-1}$ is a continuous mapping of $G \times G$ into G/H. But this map is the composition of the continuous mappings π and $(x, y) \mapsto xy^{-1}$, hence is continuous. □

Whenever in the sequel we consider a quotient group G/H of a topological group G as a topological group, it is always to be understood that the topology of G/H is the quotient by H of the topology of G, unless the contrary is expressly stated.

Proposition 3.1.33. *Let H be a subgroup of a topological group G. The canonical map $\pi : G \to G/H$ is open. If $\mathfrak{B}$ is a fundamental system of neighbourhoods of e in G, then $\pi(\mathfrak{B})$ is a fundamental system of neighbourhoods of the identity element $\pi(e)$ of G/H.*

Proof. Let $U \subseteq G$ be open, then we have $\pi^{-1}(\pi(U)) = \bigcup_{h\in H} hU$, which is open since U is. Thus by the definition of the quotient topology, $\pi(U)$ is open in G/H. The second claim therefore follows. □

In particular, Proposition 3.1.28 and Proposition 3.1.29 implies the following result.

Proposition 3.1.34. *Let G be a topological group and let H be a normal subgroup of G. Then G/H is Hausdorff if and only if H is closed, and is discrete if and only if H is open.*

If G is a topological group and N is the closure of $\{e\}$ in G, then N is a closed normal subgroup of G (Proposition 3.1.15), hence G/N is Hausdorff; G/N is called the **Hausdorff group associated with G**.

Proposition 3.1.35. *If H is a discrete normal subgroup of a topological group G, then G/H is locally isomorphic to G.*

Proof. Let V be a neighbourhood of e in G which does not contain any point of H other than e, and let W be a symmetric open neighbourhood of e in G such that $W^2 \subseteq V$. Then the restriction to W of the canonical mapping π of G onto G/H is injective; for if $x, y \in W$ and $\pi(x) = \pi(y)$, then $x^{-1}y \in W^2 \subseteq V$ and $x^{-1}y \in H$, so that $x = y$. By Proposition 3.1.33 it follows that the restriction of π to W is a homeomorphism of W onto $\pi(W)$; since moreover π is a homomorphism, we conclude that G and G/H are locally isomorphic. □

Proposition 3.1.36. *Let H be a normal subgroup of G and $f : G \to G$ a continuous homomorphism of G such that $f(H) \subseteq H$. Then the induced map $\tilde{f} : G/H \to G/H$ is continuous.*

Proof. We have the following commutative diagram:

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\pi"] & G \arrow[d, "\pi"] \\ G/H \arrow[r, "\tilde{f}"] & G/H \end{tikzcd}$$

Let $V \subseteq G/H$ be an open set. Then to show $\tilde{f}^{-1}(V)$ is open, we note that

$$\pi^{-1}(\tilde{f}^{-1}(V)) = f^{-1}(\pi^{-1}(V)).$$

Since f and π are continuous, we see $\pi^{-1}(\tilde{f}^{-1}(V))$ is open, whence the claim. □

Proposition 3.1.37. *Let $\phi : G \to H$ be a homomorphism between topological groups. Consider the following decomposition of ϕ:*

$$G \xrightarrow{\pi} G/\ker\phi \xrightarrow{\bar{\phi}} \operatorname{im}\phi \xrightarrow{\iota} H$$

Then ι is an embedding and $\bar{\phi}$ is a group isomorphism, and ϕ is continuous iff $\bar{\phi}$ is. Also, $\bar{\phi}$ is open if and only if ϕ is open.

Proof. Note that $\phi = \iota \circ \bar{\phi} \circ \pi$ and π, ι are continuous. Thus if $\bar{\phi}$ is continuous, then so is ϕ; if ϕ is continuous, then for any V open in H,

$$\bar{\phi}^{-1}(V \cap \operatorname{im}\phi) = \pi(\phi^{-1}(V))$$

is open in $G/\ker\phi$ since π is open. This shows the first claim, and the second can be proved similarly. □

Since ϕ may not be open, the bijection $\bar{\phi}$ in Proposition 3.1.37 may not be a homeomorphism. For example, let G' be a non-discrete topological group, and G the topological group obtained by giving G' the discrete topology; then the identity mapping of G into G' is a continuous bijective homomorphism, but is not bicontinuous.

Definition 3.1.38. *A continuous homomorphism ϕ of a topological group G into a topological group H is said to be a* ***strict morphism*** *of G into H if the bijective homomorphism $\bar{\phi}$, from $G/\ker\phi$ to $\operatorname{im}\phi$, associated with ϕ, is an isomorphism of topological groups.*

By Proposition 3.1.37, the following proposition is immediate.

Proposition 3.1.39. *Let ϕ be a continuous homomorphism of a topological group G into a topological group H. Then the following statements are equivalent:*

(i) ϕ is a strict homomorphism.

(ii) The image under ϕ of every open set in G is an open set in $f(G)$.

(iii) The image under ϕ of every neighbourhood of the identiry element in G is a neighbourhood of the identiry element in H.

Example 3.1.40. From condition (ii) of Proposition 3.1.39 it follows that every continuous homomorphism of a topological group into a discrete group is a strict morphism. If G is compact and $\phi(G)$ is Hausdorff, then the bijective homomorphism $\bar{\phi}$ associated with ϕ is bicontinuous. Hence every continuous homomorphism of a compact group into a Hausdorff group is a strict morphism.

Example 3.1.41. Let ϕ be a strict morphism of G into G' and let ψ be a strict morphism of G' into G''. If ϕ is surjective or if ψ is injective, it follows immediately from Proposition 3.1.39 that $\psi \circ \phi$ is a strict morphism of G into G''. But this conclusion is no longer necessarily valid if neither of the two preceding conditions is satisfied, even if ϕ is injective and ψ surjective.

Example 3.1.42. Let ϕ be a continuous homomorphism of a topological group G into a topological group G', and let H be a normal subgroup of G. Then ϕ induces a homomorphism $\bar{\phi}$ of the group G/H onto the quotient group $\phi(G)/\phi(H)$. This homomorphism $\bar{\phi}$ is continuous.

$$\begin{tikzcd} G \arrow[r, "\phi"] \arrow[d, "\pi"'] & \phi(G) \arrow[d, "\pi'"] \\ G/H \arrow[r, "\bar{\phi}"] & \phi(G)/\phi(H) \end{tikzcd}$$

Moreover, if ϕ is a strict morphism of G into G', then $\bar{\phi}$ is a strict morphism of G/H onto $\phi(G)/\phi(H)$: for if U is open in G/H, and if π (resp, π') denotes the canonical mapping of G onto G/H [resp. of $\phi(G)$ onto $\phi(G)/\phi(H)$], then we have $\bar{\phi}(U) = \pi'(\phi(\pi^{-1}(U)))$. Since $\pi^{-1}(U)$ is open in G, it follows that $\bar{\phi}(U)$ is open in $\phi(G)/\phi(H)$, which proves our assertion.

Now we consider subgroups of a quotient group. Let G be a topological group, let H be a normal subgroup of G, and let $\pi : G \to G/H$ be the canonical mapping. We know that if $\bar{K}$ is a subgroup of G/H, then $K := \pi^{-1}(\bar{K})$ is a subgroup of G which contains H. Conversely, if K is a subgroup of G, then $\pi(K)$ is a subgroup of G/H; moreover, there is a canonical bijection

of the quotient group $K/(K \cap H)$ onto the subgroup $\pi(K)$ of G/H, and a canonical bijection of $\pi(K)$ onto the quotient group KH/H, and both these bijections are isomorphisms for the group structures.

Proposition 3.1.43. *Let K be a subgroup of a topological group G, let H be a normal subgroup of G, and let π denote the canonical mapping of G onto G/H. Then the canonical bijection of $\pi(K)$ onto KH/H is an isomorphism of topological groups.*

Proof. Note that HK is the saturation of K, so this follows from Proposition 3.1.25. □

The canonical bijection of $K/(K \cap H)$ onto $\pi(K)$ is a continuous homomorphism, since it arises from the restriction of π to K by passing to the quotients; but in general the topological groups $K/(K \cap H)$ and KH/H are not isomorphic.

Example 3.1.44. For example, take G to be the additive group $\mathbb{R}$ of real numbers, take H to be the group $\mathbb{Z}$ of integers, and take K to be the group $\alpha\mathbb{Z}$ of integer multiples of an irrational number α. Then $K \cap H = \{0\}$, so that $K/(K \cap H)$ is a discrete group, isomorphic to $\mathbb{Z}$; on the other hand, $K + H$ is dense in $\mathbb{R}$, hence $(K + H)/H$, which is locally isomorphic to $K + H$, is not a discrete group and consequently is not isomorphic to $K/(K \cap H)$.

Let G be a topological group operating continuously on a topological space X, and let K be a normal subgroup of G which is contained in the stabilizer of each point of X. For each $x \in X$, the relation $g^{-1}h \in K$ therefore implies $g \cdot x = h \cdot x$, and passing to the quotient we define a mapping $\bar{g} \mapsto \bar{g} \cdot x$ of G/K into X. It is immediately verified that with respect to this definition G/K acts on X. Moreover, this action is continuous: the relation of equality on X and the relation $g^{-1}h \in K$ on G are both open equivalence relations, and therefore the result follows from the continuity of the mapping

$$(g, x) \mapsto \bar{g} \cdot x = g \cdot x$$

of $G \times X$ into X.

Now let G be a topological group acting continuously on a topological space X, and let H be any normal subgroup of G; then H acts continuously on X. Let R_H be the equivalence relation defined by H on X; then R_H is open. The relation R_H is compatible with the group G, for if $(x, y) \in R_H$ then there exists $h \in H$ such that $y = h \cdot x$, hence for all $g \in G$ we have $g \cdot y = (ghg^{-1})g \cdot x$, and $ghg^{-1} \in H$ since H is normal in G; thus $(g \cdot x, g \cdot y) \in R_H$. If $\bar{x}$ denotes the canonical image of X onto X/H, the group G therefore acts continuously on X/H by

$$(g, \bar{x}) \mapsto \overline{g \cdot x}.$$

Moreover, the group H is contained in the stabilizer of each of the points of X/H; as we have seen above, G/H then acts continuously on X/H by

$$(\bar{g}, \bar{x}) \mapsto \overline{g \cdot x}.$$

If R denotes the equivalence relation on X defined by G, then the relation R_H implies R, and the equivalence relation R/R_H on X/H is that defined by the group G/H. Hence we have the following result:

Proposition 3.1.45. *Let G be a topological group operating continuously on a topological space X, and let H be a normal subgroup of G. Then the canonical bijection of X/G onto $(X/H)/(G/H)$ is a homeomorphism.*

Corollary 3.1.46. *Let G be a topological group, H a normal subgroup of G, and K a normal subgroup of G which contains H. Then the canonical bijection of G/K onto $(G/H)/(K/H)$ is an isomorphism of topological groups.*

Proof. We know that this bijection is an isomorphism of groups, and Proposition 3.1.45 shows that it is a homeomorphism. □

Proposition 3.1.47. *Let G be a group and let $(G_i)_{i\in I}$ be a family of topological groups such that for each $i \in I$ there is a homomorphism $f_i : G \to G_i$. Then the initial topology on G with respect to (f_i) is a group topology.*

Proof. For each $i \in I$ let $\mathfrak{B}_i(e)$ denote the filter of neighborhoods of e in G_i. Then a base $\mathfrak{U}_{\mathcal{T}}(e)$ at e for the initial topology $\mathcal{T}$ for G determined by the family $(f_i)_{i\in I}$ is given by intersections of the form $\bigcap_{k\in K} f_k^{-1}(V_k)$, where K is a finite subset of I and $V_k \in \mathfrak{B}_k(e)$ for each $k \in K$. For $i_1, \dots, i_n$, let $V_{i_j} \in \mathfrak{B}_{i_j}(e)$, and choose symmetric $B_{i_j} \in \mathfrak{B}_{i_j}(e)$ such that $B_{i_j}B_{i_j}^{-1} \subseteq V_{i_j}$, then

$$\left(f_{i_j}^{-1}(B_{i_j})\right)\left(f_{i_j}^{-1}(B_{i_j})\right)^{-1} = f_{i_j}^{-1}(B_{i_j}B_{i_j}^{-1}) \subseteq f_{i_j}^{-1}(V_{i_j})$$

and therefore $(\bigcap_{j=1}^n f_{i_j}^{-1}(B_j))(\bigcap_{j=1}^n f_{i_j}^{-1}(B_j))^{-1} \subseteq (\bigcap_{j=1}^n f_{i_j}^{-1}(V_j))$. By Proposition 3.1.4, $\mathcal{T}$ is a group topology on G. □

An example is given by the product group topology. Let $\{G_i : i \in I\}$ be a family of topological groups and consider the product set $G = \prod_i G_i$. It is easy to verify that G is a group with respect to this pointwise operation and that each projection $\pi_i : G \to G_i$ is a homomorphism. The product topology $\mathcal{T}$, the coarsest topology with respect to which each projection is continuous, is the initial image topology determined by $\{\pi_i : i \in I\}$. Since projections are homomorphisms, it is a group topology.

Definition 3.1.48. *The topological group obtained by giving the product set*

$$G = \prod_{i\in I} G_i$$

the group structure which is the product of the group structures of the G_i and the topology which is the product of the topologies of the G_i is called the product of the topological groups G_i.

If H_i is a subgroup of G_i then the product of the topological groups H_i is isomorphic to the subgroup $\prod_i H_i$.

Proposition 3.1.49. *Let $(G_i)_{i\in I}$ be a family of topological groups, and let H be the normal subgroup of $G = \prod_i G_i$ consisting of all $x = (x_i)$ such that the x_i are equal to the identity element e_i of G_i except for a finite number of indices. Then the subgroup H is dense in G.*

Let $(X_i)_{i\in I}$ be a family of topological spaces, and for each $i \in I$ let G_i be a topological group acting continuously on X_i. It is clear that the product group $G = \prod_{i\in I} G_i$ then acts continuously

on the product space $X = \prod_{i\in I} X_i$ by

$$((g_i), (x_i)) \mapsto (g_i \cdot x_i).$$

Moreover the orbit under G of a point $x = (x_i)$ of X is the product of the orbits of the X_i (with respect to the groups G_i). Let π_i be the canonical mapping of X_i onto X_i/G_i and let $\pi = (\pi_i)$ be the product mapping of X onto $\prod_{i\in I}(X_i/G_i)$; then the preceding remark shows that the bijection canonically associated with π maps the orbit space X/G onto $\prod_{i\in I}(X_i/G_i)$. Moreover:

Proposition 3.1.50. *The bijection of X/G onto $\prod_{i\in I}(X_i/G_i)$ canonically associated with (π_i) is a homeomorphism.*

Proof. Since the π_i are surjective and open, it follows that $\pi = (\pi_i)$ is an open mapping. □

Corollary 3.1.51. *Let $(G_i)_{i\in I}$ be a family of topological groups, and for each $i \in I$ let H_i be a normal subgroup of G_i; let π_i denote the canonical mapping of G_i onto G_i/H_i. Let $G = \prod_{i\in I} G_i$ and $H = \prod_{i\in I} H_i$. Then the bijective homeomorphism of G/H onto $\prod_{i\in I}(G_i/H_i)$ associated with the continuous homomorphism $(x_i) \mapsto (\pi_i(x_i))$ is an isomorphism of topological groups.*

3.1.5 $\mathcal{S}$-topologies

Let G be an commutative topological group, $\mathfrak{U}(0)$ the neighborhood filter at 0, and X be a set. Let G^X denote the set of all functions mapping X into G. For $f, g \in G^X$ and $x \in X$, define $(f + g)(x) = f(x) + g(x)$. With respect to these pointwise operations, G^X is an commutative group.

We topologize G^X in various ways that make it a topological group. Various different notions of convergence of functions-uniform, pointwise, etc.–all fit under this umbrella. This was very important, historically, for it shows that general topology is a broad enough tool to encompass these diverse types of convergence. Our general remarks below apply just as well to any subgroup of G^X. When X is a topological space, we can consider the subgroup $C(X, G)$ of continuous maps of X into G. The building blocks for the topologies for G^X to come are the sets

$$N(S, V) = \{f \in G^X : f(S) \subseteq V\}, \quad S \subseteq X, V \in \mathfrak{U}(0).$$

Their vital properties follow. The proofs of all parts are immediate.

Proposition 3.1.52. *For any $S_1, S_2 \subseteq X$ and $U, V \in \mathfrak{U}(0)$,*

(a) $U \subseteq V \Rightarrow N(S, U) \subseteq N(S, V)$;

(b) $N(S, -V) = -N(S, V)$; *thus if V is symmetric, so is $N(S, V)$;*

(c) $N(S, U) - N(S, V) \subseteq N(S, U - V)$;

(d) $S_1 \subseteq S_2 \Rightarrow N(S_1, V) \supseteq N(S_2, V)$;

(e) for any family $\{S_i : i \in I\}$ of subsets of X, $N(\bigcup_i S_i, V) = \bigcap_i N(S_i, V)$.

(f) for any family $\{V_i : i \in I\}$ of neighborhoods of 0 in G, $N(S, \bigcap_i S_i) = \bigcap_i N(S, V_i)$.

Let $\mathcal{S}$ be a collection of subsets of X and consider $B_{\mathcal{S}}(0) = \{N(S,V) : S \in \mathcal{S}, V \in \mathfrak{U}(0)\}$. Since the 0 function belongs to each $N(S,V)$, finite intersections of sets from $B_{\mathcal{S}}(0)$ are nonempty. Let $S \in \mathcal{S}$ and $V \in \mathfrak{U}(0)$. Choose a symmetric neighborhood $U \subseteq V$ such that $U - U \subseteq V$. By Proposition 3.1.52, it follows that

$$N(S,U) - N(S,U) \subseteq N(S,U-U) \subseteq N(S,V)$$

thus showing that $B_{\mathcal{S}}(0)$ satisfies condition (FB) of Proposition 3.1.4. Thus $B_{\mathcal{S}}(0)$ forms a neighborhood subbase at 0 for a group topology $\mathcal{T}_{\mathcal{S}}$ for G^X, called the **topology of uniform convergence on $\mathcal{S}$**, or the **$\mathcal{S}$-topology**. We denote the neighborhood filter it determines at 0 by $\mathfrak{U}_{\mathcal{S}}(0)$.

Suppose the topological group (G,d) is metrizable and that $\mathcal{B}$ consists of the sets $B_r(0)$, $r > 0$. Then, for any collection $\mathcal{S}$ of subsets of X, the sets $N(S, B_r(0))$, $r > 0$, $S \in \mathcal{S}$, is a base at 0 for $\mathcal{T}_{\mathcal{S}}$.

Since $N(\bigcup_i S_i, V) = \bigcap_i N(S_i, V)$, if $\mathcal{S}$ is closed under the formation of finite unions, then the $N(S,V)$ form a base at 0 rather than just a subbase. Actually, we can always assume that $\mathcal{S}$ is closed with respect to the formation of finite unions in view of the following result.

Proposition 3.1.53. *Let $\mathcal{S}$ be a collection of subsets of the set X. The $\mathcal{S}$-topology $\mathcal{T}_{\mathcal{S}}$ is unaffected by replacing $\mathcal{S}$ by the collection $\mathcal{S}^*$ of all subsets of finite unions of sets of $\mathcal{S}$.*

Proof. Since $\mathcal{S} \subseteq \mathcal{S}^*$, clearly $\mathcal{T}_{\mathcal{S}} \subseteq \mathcal{T}_{\mathcal{S}^*}$, so it only remains to show that $\mathfrak{U}_{\mathcal{S}^*}(0) \subseteq \mathfrak{U}_{\mathcal{S}}(0)$. To this end, suppose that $S_1, \ldots, S_n \in \mathcal{S}$. By Proposition 3.1.52(d), for any neighborhood V of 0 in the topological group G,

$$N(\bigcup_{i=1}^{n} S_i, V) = \bigcap_{i=1}^{n} N(S_i, V)$$

This implies $N(\bigcup_{i=1}^{n} S_i, V) \in \mathfrak{U}_{\mathcal{S}}(0)$ and the result follows. □

Proposition 3.1.54. *Let $\mathcal{S}$ be a collection of subsets of the set X. If the topological group G is Hausdorff and $\mathcal{S}$ covers X then $(G^X, \mathcal{T}_{\mathcal{S}})$ is Hausdorff.*

Proof. It suffices to show that $\bigcap \mathfrak{U}_{\mathcal{S}}(0) = \{0\}$. To this end let $f \in \mathfrak{U}_{\mathcal{S}}(0)$ and choose any $x \in X$. Now select $S \in \mathcal{S}$ such that $x \in S$. Since $f \in \bigcap \mathfrak{U}_{\mathcal{S}}(0)$, $f(x) \in \bigcap \mathfrak{U}(0) = \{0\}$ (G is Hausdorff). It follows that $f(x) = 0$. Since x is arbitrary, $f = 0$. □

Proposition 3.1.54 is one instance of a somewhat more general phenomenon: namely, that the behavior of a function f on $\bigcup \mathcal{S}$ determines the position f will occupy in the $\mathcal{S}$-topology. For example, if f vanishes on $\bigcup \mathcal{S}$, then f is a limit point of the filter $\mathfrak{U}_{\mathcal{S}}(0)$.

We consider some particular $\mathcal{S}$-topologies next.

Example 3.1.55 (Topology of Uniform Convergence). Let $\mathcal{S} = \{X\}$. The sets $\mathfrak{U}_X(0) = \{N(X,V) : V \in \mathfrak{U}(0)\}$ form a filterbase in G^X by Proposition 3.1.52. The topology $\mathcal{T}_u$ obtained this way is called the **topology of uniform convergence**. It is clear that a net (f_α) from $(G^X, \mathcal{T}_u)$ converges to f iff for any $V \in \mathfrak{U}(0)$, $f_\alpha(x) - f(x) \in V$ eventually for all $x \in X$.

More generally, consider any subset S of X. The sets $\mathfrak{U}_S(0) = \{N(S,V) : V \in \mathfrak{U}(0)\}$ are a base at 0 for a group topology on G^X called the topology of uniform convergence on S.

Example 3.1.56. Let $\mathcal{S}$ denote the class of all singletons of X. In view of Proposition 3.1.52 we get the same $\mathcal{S}$-topology by taking $\mathcal{S}$ to be the set of all finite subsets of X. This $\mathcal{S}$-topology is called the **topology of pointwise convergence**; we denote $\mathcal{T}_p$ by this topology and the neighborhood filter by $\mathfrak{U}_p(0)$. It is clear that a net (f_α) from $(G^X, \mathcal{T}_p)$ converges to f iff the nets $(f_\alpha(x))$ in G converge to $f(x)$ for each $x \in X$. Another name for $\mathcal{T}_p$ is the point-open topology. If we replace X by a subset S of X, we call the resulting topology the topology of pointwise convergence on S.

Since the collection of all finite subsets of X is generally a rather small collection, the topology of pointwise convergence is a fairly weak topology. A subbasic $\mathcal{T}_p$-neighborhood of 0 is a set of the form $\{f \in G^X : f(x) \in V\}$ for some $x \in X$ and neighborhood V of 0 in X which is $V \times \prod_{s \in X, s \neq x} G_s$, where $G_s = G$ for all $s \neq x$, i.e., a subbasic neighborhood of 0 for the product topology on G^X; in other words the product and point-open topologies coincide on G^X. By Proposition 3.1.54, given any collection $\mathcal{S}$ of subsets of X, the point-open topology on $\bigcup \mathcal{S}$ is coarser than the $\mathcal{S}$-topology.

Example 3.1.57 (Compact-Open Topology). Let $\mathcal{S}$ be the collection of all compact subsets of a topological space X. We denote this $\mathcal{S}$-topology by $\mathcal{T}_c$. It is called variously the **compact-open topology**, **topology of uniform convergence on compact sets** and the **topology of compact convergence**. An open base at 0 for $\mathcal{T}_c$ is given by the sets $N(K, V)$, where K is a compact subset of X and V an open neighborhood of 0 in X. Since there are generally more compact sets than finite sets, $\mathcal{T}_c$ is generally finer than the topology of pointwise convergence.

3.1.6 Metrizability

In this part, G denotes a topological group. We show that a topological group is pseudometrizable iff it has a countable base at 0, in which case the topology is generated by an *invariant* pseudometric. After showing that quotients of pseudometrizable groups are pseudometrizable, we show that the topology of any topological group is generated by a family of invariant pseudometrics.

First, we exhibit a pseudometric that does not yield a group topology.

Example 3.1.58. We define a pseudometric d on the integers $\mathbb{Z}$ as follows

$$d(j,k) = d(k,j) = \begin{cases} 0 & \text{if } j = k \text{ or } j < k \leq 0, \\ 1 & \text{if } j \leq 0 \leq k \text{ or } j > k \geq 0. \end{cases}$$

It is trivial to verify that d is a pseudometric and any neighborhood of O must contain the negative integers. Note that $B_{1/2}(1) = \{1\}$. Writing 1 as $1 + 0$, there can be no neighborhoods U of 0 and V of 1 such that $U + V \subseteq B_{1/2}(1)$. This, then, d induces an incompatible pseudometric topology.

If G is a group and d a pseudometric on G, d is called **left invariant** if $d(gx, gy) = d(x, y)$ whenever $g, x, y \in G$, and **right invariant** if $d(xg, yg) = d(x, y)$, and **invariant** if it is both right and left invariant. If G is a topological space and d a pseudometric on G, we shall say that G admits d if the d-topology of G agrees with its original topology.

Metrizability of a topology depends on its separation and countability properties. Since

group topologies have a certain amount of inherent separation (namely, regularity) metrizability reduces to just a countability condition.

Theorem 3.1.59. *Let G be a topological group. Then G is pseudometrizable iff it has a countable base at e. If G is pseudometrizable then there exists a left invariant pseudometric d that generates its topology. Moreover, G is metrizable iff it is Hausdorff.*

Proof. That the condition is necessary is obvious. Therefore it is sufficient to prove that if G satisfies the first countability axiom, it is metrizible. To prove this, suppose that $\{V_n\}$ is a denumerable base of neighborhoods of 0. By Proposition 3.1.4(b), we can define a sequence $\{U_n\}$ of symmetric neighborhoods of e such that $U_1 = V_1$ and $U_{n+1}^3 \subseteq U_n \cap V_n$ for each $n \in \mathbb{N}$. Since $\{V_n\}$ is a base at e, so is $\{U_n\}$. As a first step toward getting a left invariant pseudometric that generates the topology, consider the function f defined as follows:

$$f(x,y) = \begin{cases} 1 & \text{if } x^{-1}y \notin U_1, \\ 2^{-n} & \text{if } x^{-1}y \in U_n \setminus U_{n+1}, \\ 0 & \text{if } x^{-1}y \in U_n \text{ for each } n. \end{cases}$$

Obviously $f(x,x) = 0$. Also, the sets $U_r(g) = \{x \in G : f(g,x) < r\}$ are a complete system of neighborhoods for any point $g \in G$. Moreover, since U_n are symmetric, $x^{-1}y \in U_n$ iff $y^{-1}x \in U_n$, whence $f(x,y) = f(y,x)$. And finally, since $U_iU_jU_k \subseteq U_n$ if $n > i,j,k$, one sees that

$$\text{If } f(x,y) < r, f(y,\tilde{y}) < r, f(\tilde{y},z) < r, \text{ then } f(x,z) < 2r. \tag{1.6.1}$$

The function d, defined next, is:

$$d(x,y) = \inf \sum_{i=0}^{p-1} f(z_i, z_{i+1})$$

where the infimum is taken over all finite sequences $z_0, \dots, z_p$ for which $z_0 = x$ and $z_p = y$. In effect, we are seeking a path of shortest distance from x to y. We show that d is a left invariant pseuclometric such that $f(x,y)/2 \le d(x,y) \le f(x,y)$. The second inequality is obvious; to prove the first, we show that

$$\sum_{i=0}^{p-1} f(z_i, z_{i+1}) \ge f(x,y)/2 \tag{1.6.2}$$

for any finite sequence $x = z_0, \dots, z_p = y$. We establish this by induction on p. Clearly, this holds for $p = 1$, so suppose that $p > 1$ and that (1.6.2) holds for all integers $q < p$ and x, y in G. Let A denote the sum on the left side of (1.6.2). Consider two possibilities: if $A \ge 1/2$, then (1.6.2) holds since $f(x,y) \le 1$. If $A < 1/2$, we can find an integer h such that

$$\sum_{i=0}^{h-1} f(z_i, z_{i+1}) \le A/2, \qquad \sum_{i=h+1}^{n} f(z_i, z_{i+1}) < A/2.$$

By the induction hypothesis, $f(x,z_h)/2 \le \sum_{i=0}^{h-1} f(z_i, z_{i+1})$, so $f(x,z_h) \le A$. Similarly we have $f(z_{h+1}, y) \le A$. Since clearly $f(z_h, z_{h+1}) \le A$, by (1.6.1) we get $f(x,y) \le 2A$.

If $A = 0$, then $f(z_i, z_{i+1}) = 0$ for $i = 0, \dots, p-1$, which implies that $z_i^{-1} z_{i+1} \in U_n$ for every n. Thus $x^{-1}y \in U_n^p$ for every n. It follows that $x^{-1}y \in \bigcap_n U_n$ so $f(x, y) = 0$. Thus (1.6.2) holds when $A = 0$ as well and the proof of the pseudometrizability of G is complete. □

If the topological group G is pseudometrizable then, for any normal subgroup H of G, so is the quotient group G/H. For this, it suffices to note that if G has a countable base $\{V_n\}$ at e, the canonical images $\pi(V_n)$ are a countable base at $\bar{e}$ in G/H. In fact, even more is true.

Proposition 3.1.60. *Let G be a pseudometrizable topological group and H be a normal subgroup of G. Then the function $\bar{d} : G/H \to \mathbb{R}$ defined by*

$$\bar{d}(\bar{x}, \bar{y}) = d(xH, yH) = \inf_{h_1, h_2 \in H} d(xh_1, xh_2)$$

is a pseudometric on G/H inducing the quotient topology. If d is a metric and H is closed, then $\bar{d}$ is a metric.

Proof. Let $\pi : G \to G/H$ denote the canonical map. We show that $\pi(B_r(e)) = B_r(\bar{e})$ for each $r > 0$. If $x \in B_r(0)$, then $d(\bar{x}, \bar{e}) \le d(x, e) < r$; hence $\pi(B_r(e)) \subseteq B_r(\bar{e})$. Conversely, if $\bar{x} \in B_r(\bar{e})$, then there exists $h \in H$ such that $d(xh, e) < r$. Hence $xh \in B_r(0)$ and $\pi(xh) = \pi(x) = \bar{x}$. This proves the first part.

Now assume that d is a metric and H is closed. Let $\bar{x}, \bar{y} \in G/H$ such that $\bar{d}(\bar{x}, \bar{y}) = 0$. Then there exists $h_1, h_2 \in H$ such that $d(xh_1, yh_2) = 0$. Since d is a metric, this implies $xh_1 = yh_2$, and thus $\bar{x} = \bar{y}$. □

Suppose that $\mathscr{D}$ is a family of left invariant pseudometrics on a group G. For each $d \in \mathscr{D}$, the symmetric sets $\{x \in G : d(x, e) < r\}$ where $d \in D$ and $r > 0$ form a filter subbase satisfying the conditions of Proposition 3.1.4, and therefore are a filter subbase of open sets for a group topology $\mathcal{T}$ on X. We call $\mathcal{T}$ the topology determined by the family of pseudometrics $\mathscr{D}$. It is trivial to verify that $\mathcal{T}$ is the weakest topology with respect to which each d is continuous. We show next that the topology of any topological group is generated by a family of left invariant pseudometrics.

Proposition 3.1.61. *The topology of any topological group $(G, \mathcal{T})$ is determined by a family of left invariant pseudometrics.*

Proof. Let $\mathfrak{U}(0)$ denote the collection of symmetric neighborhoods of 0 in the topological group $(X, \mathcal{T})$. For each $U \in \mathfrak{U}(0)$ we may inductively define a sequence $\{U_n\}$ of symmetric neighborhoods of 0 such that $U_1 = U$ and $U_{n+1}^3 \subseteq U_n$ for $n \in \mathbb{N}$ as in the proof of Theorem 3.1.59. Also as in the proof of Theorem 3.1.59, there is a left invariant pseudometric d_U associated with each $U \in \mathfrak{U}(0)$ such that $x \in U$ iff $d(x, U) \le 1$. In other words, the closed unit ball determined by d_U is just U so the topology generated by $\{d_U : U \in \mathfrak{U}(0)\}$ is finer than $\mathcal{T}$. By the proof of Theorem 3.1.59, each d_U is continuous; therefore each $\{x \in G : d_U(x, e) < r\}$, $r > 0$ is a neighborhood of 0 in G and the topology generated by $\{d_U : U \in \mathfrak{U}(0)\}$ is coarser than $\mathcal{T}$. □

3.2 Complete topological groups

In this section we discuss the completeness of an commutative topological group G by means of Cauchy nets. Without further specification, all groups in this part will be commuta-

tive.

3.2.1 Uniformity on topological groups

In a topological group a we can perceive the possibility of defining a notion of "sufficiently near points" and hence a uniform structure, by operating as follows: if x and y are any two points of G, we apply to both points the translation which sends one of them, say x, to the identity element e; the "proximity" of x and y is then evaluated in some sense by the neighbourhood V of e into which y is translated. This translation, which consists in multiplying both x and y by x^{-1}, can be carried out on the right or on the lift, and we shall see that in either case we obtain effectively a uniformity on a which is compatible with the topology of G. Let us take the case in which the translations are performed on the left; then to each neighbourhood V of e there corresponds the set L_V of pairs $(x, y) \in G \times G$ such that $x^{-1}y \in V$. Let $\mathfrak{L}$ be the family of sets L_V, as V runs through the neighbourhood filter $\mathfrak{B}$ of e. Then $\mathfrak{L}$ is a fundamental system of entourages. For since $e \in V$, the diagonal Δ of $G \times G$ is contained in L_V for each $V \in \mathfrak{B}$, hence $\mathfrak{L}$ is a filter base and satisfies axiom (B1); since the relations $x^{-1}y \in V$ and $y^{-1}x \in V^{-1}$ are equivalent, we have $L(V^{-1}) \in \mathfrak{L}$, so that (B2) is satisfied; and finally, the relations $x^{-1}y \in V$ and $y^{-1}z \in V$ imply $x^{-1}z \in V^2$; hence $L_V \circ L_V$ is contained in L_{V^2}, thus $\mathfrak{L}$ satisfies (B3).

The uniformity defined by $\mathfrak{L}$ is compatible with the topology of G, for the relations $y \in L_V(x)$ and $y \in xV$ are equivalent by definition; in other words $L_V(x) = xV$. We can also apply right translation to get another uniformity on G, which consists of set of the form

$$R_V = \{(x, y) \in G \times G : yx^{-1} \in V\}$$

with V a neighborhood of e in G. We may call this uniformity $\mathfrak{R}$. If $i : G \to G$ is the inverse map, then it is easy to see $i^{-1}(R_V) = L(V^{-1})$, so i is an isomorphism between the uniformities $\mathfrak{L}$ and $\mathfrak{R}$.

To each proposition on the topology of a uniform space there corresponds a proposition on the topology of a group; the translation is made according to the definition and the formulae $L_V(x) = xV$, $L_V(A) = AV$, $R_V(x) = V$, $R_V(A) = VA$, which are immediate consequences of the definition. For example, if A is any non-empty subset of G then we have

$$\bar{A} = \bigcap_{V \in \mathfrak{B}} AV = \bigcap_{V \in \mathfrak{B}} VA.$$

The left and right uniformities on a topological group are in general distinct, but they both induce the group topology on G. Obviously they coincide if the group is commutative, for then $L_V = R_V$; also they coincide if the group is compact and Hausdorff (by Theorem 2.3.1). In general, we shall denote by G_l (resp. G_r) the uniform space obtained by giving the set G its left (resp. right) uniformity.

Proposition 3.2.1. *The left and right translations are isomorphisms of the left uniformity onto itself.*

Proof. As to the left translations, the result is clear, since the relation $x^{-1}y \in V$ is equivalent to $(ax)^{-1}(ay) \in V$ [in other words, the mapping $(x, y) \to (ax, ay)$ leaves L_V fixed]. For the right translations, the result follows from the group axoim: for $x^{-1}y \in V$ if and only if $(xa)^{-1}(ya) \in a^{-1}Va$ hence $x \mapsto xa$ is uniformly continuous on G_l. □

Every inner automorphism $x \mapsto axa^{-1}$ of G is therefore an automorphism for the group structure of G, for the topology of G, and for both the uniformities of G.

Proposition 3.2.2. *Every continuous homomorphism f of a topological group G into a topological group H is uniformly continuous when considered as a mapping of G_l into H_l (or of G_r into H_r).*

Proof. For if V is a neighbourhood of the identity element in H, and $U = f^{-1}(V)$, then the relation $x^{-1}y \in U$ implies

$$f(x)^{-1}f(y) = f(x^{-1}y) \in V.$$

This proves the claim. □

3.2.2 Complete groups

Definition 3.2.3. *A topological group is said to be* ***complete*** *if its left and right uniformities are structures of complete spaces.*

Since the left and right uniformities are isomorphic, for a group to be complete it is sufficient that one of its uniformities is a structure of a complete space. Every closed subgroup of a complete group is complete. Every product of complete groups is complete.

Example 3.2.4. Consider the additive group $\mathbb{R}$ of real numbers. A metric for $\mathbb{R}$ is given by $d(x, y) = |\arctan x - \arctan y|$. As a metric space $(\mathbb{R}, d)$ is not complete for $\{n\}$ is a nonconvergent Cauchy sequence. Since, for $r > 0$, $B_r(0) = \{x \in \mathbb{R} : |\arctan x| < r\} = (-\tan r, \tan r)$, d induce the usual Euclidean topology on $\mathbb{R}$, so $(\mathbb{R}, d)$ is a complete topological group. Note that $\{n\}$ is a Cauchy sequence in $(\mathbb{R}, d)$ but not in the topological group $\mathbb{R}$ with its usual topology.

The metric of Example 3.2.4 is not invariant, yet it induces a group topology on $\mathbb{R}$. Invariance, or rather the lack of it, is really the key to the situation of the example. If d is an invariant pseudometric, then $d(x_\alpha, x_\beta)$ goes to 0 iff $d(x_\alpha - x_\beta, 0)$ goes to 0, so what occurred in Example 3.2.4 cannot happen. In summary:

Proposition 3.2.5. *If d is an invariant pseudometric on the group G then (G, d) is complete as a pseudometric space iff it is complete as a topological group.*

We show next that the existence of a complete neighborhood of e implies that the group is complete.

Proposition 3.2.6. *If the topological group G has a complete neighborhood V of e then G is complete.*

Proof. Let V be a complete neighborhood of e. If (x_α) is a Cauchy net, there is some index β such that $x_\alpha \in x_\beta + V$ for $\alpha \geq \beta$. As a translate of a complete set, $x_\beta + V$ is complete. Since $\{x_\alpha : \alpha \geq \beta\}$ is also a Cauchy net, it converges to some $x \in x_\beta + V$; clearly, x is also a limit of (x_α). □

The most important fact about completeness is of course, that, compact sets are complete:

Proposition 3.2.7. *A compact subset of a topological group G is complete. Hence any locally compact topological group G is complete.*

Proof. If K is compact, then any filter in K has a cluster point, hence converges. As for the second statement, it suffices to note that a locally compact topological group has a compact neighborhood of 0, hence a complete neighhorhood of 0. □

Proposition 3.2.8. *Let G_1 be a topological group, G_2 be a complete Hausdorff topological group, and let H_1 (resp. H_2) be a dense subgroup of G_1 (resp. G_2). Then every continuous homomorphism $f : H_1 \to H_2$ can be uniquely extended to a continuous homomorphism $\tilde{f}$ of G_1 into G_2. Furthermore, if G_1 is Hausdorff and complete, and if f is an isomorphism of H_1 onto H_2, then $\tilde{f}$ is an isomorphism of G_1 onto G_2.*

Proof. The map f is uniformly continuous with respect to the left uniformities of H_1 and H_2 by Proposition 3.2.2, hence admits a unique extension to a mapping $\tilde{f}$ of G_1 into G_2 which is uniformly continuous with respect to the left uniformities of these groups (Theorem 2.2.28). Moreover, by virtue of the principle of extension of identities, $\tilde{f}$ is a homomorphism of G_1 into G_2, whence the first assertion of the Proposition. To prove the second assertion, it is enough to consider the isomorphism g of H_2 onto H_1, which is the inverse of f, and its extension $\tilde{g}$ to a continuous homomorphism of G_2 into G_1; by reason of the uniqueness of the extension, $\tilde{f}$ and $\tilde{g}$ are inverse of each other, hence are bijective. □

Now let G be an commutative topological group. If X is any set, the set G^X of all maps of X into G forms a group with respect to pointwise addition of functions. We also discussed a class of group topologies for G^X called **$\mathcal{S}$-topologies**: $\mathcal{S}$ is any family of subsets of X and the basic neighborhoods of 0 for the $\mathcal{S}$-topology are the sets

$$N(S, V) = \{f \in G^X : F(S) \subseteq V\}$$

zwhere $S \in \mathcal{S}$ and V is a neighborhood of 0 in X. By Proposition 3.1.53, we may suppose that S is closed with respect to the formation of subsets of finite unions. The result below provides a necessary and sufficient condition for $\mathcal{S}$-convergence and also relates $\mathcal{S}$-convergence and pointwise convergence. We denote the $\mathcal{S}$-topology by $\mathcal{T}_{\mathcal{S}}$.

Proposition 3.2.9. *With notation as above, a net (f_α) from G^X is $\mathcal{T}_{\mathcal{S}}$-convergent to f iff (f_α) is a $\mathcal{T}_{\mathcal{S}}$-Cauchy net and $f_\alpha(x) \to f(x)$ for each $x \in \bigcup \mathcal{S}$.*

Proof. Suppose that $f_\alpha \to f$ with respect to $\mathcal{T}_{\mathcal{S}}$. Then (f_α) is a $\mathcal{T}_{\mathcal{S}}$-Cauchy net. Since $\mathcal{S}$ may be supposed to contain all subsets of finite unions of sets of $\mathcal{S}$, given any neighborhood V of 0 in G and any $x \in \bigcup \mathcal{S}$, $f_\alpha(x) - f(x) \in V$ eventually and the conditions are seen to be necessary.

Conversely, suppose that the $\mathcal{T}_{\mathcal{S}}$-Cauchy net $f_\alpha \to f$ pointwise on $\bigcup \mathcal{S}$. Since (f_α) is $\mathcal{T}_{\mathcal{S}}$-Cauchy, given any neighborhood V of 0, there exists an index γ such that $f_\alpha - f_\beta \in N(S, V)$ for $\alpha, \beta \geq \gamma$. Since $f_\alpha \to f$ pointwise on S, for any $x \in S$, there is an index $\alpha(x) \geq \gamma$ such that $f_{\alpha(x)}(x) - f(x) \in V$. Hence, for any $x \in S$ and $\alpha \geq \gamma$,

$$f_\alpha(x) - f(x) = f_\alpha(x) - f_{\alpha(x)}(x) f_{\alpha(x)}(x) - f(x) \in V + V.$$

Since V is arbitrary, the desired result follows. □

The next result provides a sufficient condition for the completeness of a function group $(G^X, \mathcal{T}_{\mathcal{S}})$.

Proposition 3.2.10. *If the topological group G is complete, then so is $(G^X, \mathcal{T}_S)$ for any collection $\mathcal{S}$ of subsets of X.*

Proof. Let (f_α) be a Cauchy net in G^X and let $H = \bigcup \mathcal{S}$. Since $\mathcal{S}$ may be assumed to contain singletons, given any $x \in H$ and neighborhood V of 0 in G, $f_\alpha - f_\beta \in N(\{x\}, V)$ eventually, i.e., $f_\alpha(x) - f_\beta(x) \in V$ eventually. For each $x \in H$, then $(f_\alpha(x))$ is a Cauchy net in G. Since G is complete, each $(f_\alpha(x))$ converges; we call the limit $f(x)$. For $x \notin H$, take $f(x) = 0$. Thus $f_\alpha \to f$ pointwise on H so, by Proposition 3.2.9, $f_\alpha \to f$ in the $\mathcal{S}$-topology. □

3.2.3 Completion of Hausdorff groups

For a Hausdorff topological group G, we know the uniform space G_l may be considered as a dense subspace of its completion $\widehat{G}_l$. We shall investigate whether G can be considered as a dense subgroup of a complete Hausdorff group $\widehat{G}$. If so, then the uniform space G must be isomorphic to $\widehat{G}_l$, and we must therefore be able to define on $\widehat{G}_l$ a topological group structure which induces the given topological group structure on G. Consequently we have to examine:

(a) Whether we can extend by continuity the functions $(x, y) \mapsto xy$ and $x \mapsto x^{-1}$ to $\widehat{G}_l \times \widehat{G}_l$ and $\widehat{G}_l$ respectively;

(b) whether the functions thus extended do indeed define a group structure on $\widehat{G}_l$;

(c) when the preceding operations are possible, the topological group which they define is complete;

(d) if there is a complete group satisfying the given conditions, then it is unique up to isomorphism.

Since the functions xy and x^{-1} are not in general uniformly continuous, we cannot apply the theorem of extension of uniformly continuous functions. Neverthdess, we can extend xy, by virtue of Theorem 2.2.27 and the following Proposition:

Proposition 3.2.11. *Let $\mathfrak{F}$ and $\mathfrak{G}$ be two Cauchy filters on G_l Then the image of the filter $\mathfrak{F} \times \mathfrak{G}$ under the mapping $(x, y) \mapsto xy$ is a Cauchy filter base on G_l.*

Proof. Let us evaluate the "proximity" of xy and $\tilde{x}\tilde{y}$ in G_l; in other words, let us form the product $(xy)^{-1}(\tilde{x}\tilde{y}) = y^{-1}x^{-1}\tilde{x}\tilde{y}$. For each $a \in G$, we can also write

$$(xy)^{-1}(\tilde{x}\tilde{y}) = (y^{-1}a)(a^{-1}x^{-1}\tilde{x}a)(a^{-1}\tilde{y}).$$

We shall see that by suitable choice of a, each of the three factors of this product is very small whenever the pairs (x, y) and $(\tilde{x}, \tilde{y})$ bdong to a sufficiently small set of $\mathfrak{F} \times \mathfrak{G}$. Let V be any neighbourhood of e in G; then there is a L_V-small set $B \in \mathfrak{G}$. Choose a in A, then if y and $\tilde{y}$ are any two points of B, we have $y^{-1}a \in V$ and $a^{-1}\tilde{y} \in V$. On the other hand, the relation $a^{-1}x^{-1}\tilde{x}a \in V$ is equivalent to $x^{-1}\tilde{x} \in aVa^{-1} =: W$, and since W is a neighbourhood of e, there is a $L(W)$-small set $A \in \mathfrak{F}$. Hence for all (x, y) and $(\tilde{x}, \tilde{y})$ in $A \times B$, we have $(xy)^{-1}(\tilde{x}\tilde{y}) \in V^3$, and this completes the proof. □

In order that $x \mapsto x^{-1}$ can be extended by continuity to G_l, it is necessary and sufficient that the image, under the symmetry $x \mapsto x^{-1}$, of a Cauchy filter on G_l is a Cauchy filter on

G_l (Theorem 2.2.27). There are examples of topological groups in which this condition is not satisfied; we shall see this condition is sufficient for $\widehat{G}_l$ being a group.

Theorem 3.2.12. *A Hausdorff topological group G is isomorphic to a dense subgroup of a complete group $\widehat{G}$ if and only if the image, under the symmetry $x \mapsto x^{-1}$, of a Cauchy filter with respect to the left uniformity of G is a Cauchy filter with respect to this uniformity. The complete group $\widehat{G}$ (which is called the completion of G) is then unique (up to isomorphism).*

Proof. We prove that the extended functions $(x, y) \mapsto xy$ and $x \mapsto x^{-1}$ define a group structure on $\widehat{G}_l$. First, the functions $x(yz)$ and $(xy)z$, defined on $\widehat{G}_l \times \widehat{G}_l \times \widehat{G}_l$ and equal on the dense subspace $G_l \times G_l \times G_l$, so the law of composition $(x, y) \mapsto xy$ is associative on $\widehat{G}_l$. For the same reason, the functions $x \mapsto x$, $x \mapsto ex$, $x \mapsto xe$ are identical on $\widehat{G}_l$, and the functions $x \mapsto e$, $x \mapsto xx^{-1}$, $x \mapsto x^{-1}x$ are identical on $\widehat{G}_l$.

We now prove the topological group $\widehat{G}_l$ is complete. Let $\mathfrak{L}$ be its left uniformiry, and let $\mathfrak{U}$ be the uniformity on $\widehat{G}_l$ obtained by completing the left uniformity of G. Then $\mathfrak{U}$ and $\mathfrak{L}$ induce the same uniformity on G, and therefore every Cauchy filter base $\mathfrak{B}$ on G with respect to $\mathfrak{L}$ is also a Cauchy filter base with respect to $\mathfrak{U}$. Now $\mathfrak{B}$ converges in $\mathfrak{U}$, since $\mathfrak{U}$ is a complete uniformity; and since $\mathfrak{U}$ and $\mathfrak{L}$ induce the same topology on $\widehat{G}$ it follows that $\mathfrak{L}$ is a complete uniformity and $\mathfrak{U}$ and $\mathfrak{L}$ coincide. The uniqueness is now clear. □

Example 3.2.13. Let $\mathbb{R}_t$ denote $\mathbb{R}$ endowed with the trivial topology. The nonempty basic open sets in $\mathbb{R} \times \mathbb{R}_t$ are of the form $(a, b) \times \mathbb{R}$ where (a, b) is an open interval in $\mathbb{R}$. Each $(a, b) \times \mathbb{R}$ intersects $\mathbb{R} \times \{0\}$ in $(a, b) \times \{0\}$ so $\mathbb{R} \times \{0\}$ is dense in $\mathbb{R} \times \mathbb{R}_t$. Since $\mathbb{R}_t$ is obviously complete, so is $\mathbb{R} \times \mathbb{R}_t$. Thus, even though $\mathbb{R} \times \{0\}$ is complete, $\mathbb{R} \times \mathbb{R}_t$ is a completion of $\mathbb{R} \times \{0\}$ which is not topologically isomorphic to the Hausdorff space $\mathbb{R} \times \{0\}$ since $\mathbb{R} \times \mathbb{R}_t$ is not Hausdorff.

Proposition 3.2.14. *Let G be a Hausdorff topological group which has a completion $\widehat{G}$. Then the closures in $\widehat{G}$ of the neighbourhoods of the identity element in G form a fundamental system of neighbourhoods of the identity element in $\widehat{G}$.*

Proof. Since $\widehat{G}$ is regular, every neighbourhood of the identity element in $\widehat{G}$ contains the closure V of an open neighbourhood U of e in G, and V is also the closure of the trace of U on G. □

Let G be a group which is not necessarily Hausdorff; let $N = \overline{\{e\}}$ and let $G' = G/N$ be the Hausdorff group associated with G. If G' has a completion $\widehat{G}'$, this completion is called the **Hausdorff completion** of G and is denoted by $\widehat{G}$.

Proposition 3.2.15. *Let G be a topological group which has a Hausdorff completion $\widehat{G}$. Then every continuous homomorphism f of G into a complete Hausdorff group H can be uniquely factorized into $f = g \circ \iota$ where g is a continuous homomorphism of $\widehat{G}$ into H and ι is the canonical mapping of G into $\widehat{G}$.*

$$\begin{tikzcd} \widehat{G} \arrow[r, "g"] & H \\ G \arrow[u, "\iota"] \arrow[ur, "f"'] & \end{tikzcd}$$

Proof. Since the kernel of f is closed and contains e, it contains N, and hence f can be written as $f = g \circ \pi$, where g is a continuous homomorphism of G/N into H; now apply Proposition 2.2.32 to g. □

Proposition 3.2.16. *Let G and H be topological groups and $f : G \to H$ be a continuous homomorphism, then there a unique continuous homomorphism $\hat{f} : \widehat{G} \to \widehat{H}$ such that the diagram*

$$\begin{tikzcd} \widehat{G} \arrow[r, "\hat{f}"] & \widehat{H} \\ G \arrow[u] \arrow[r, "f"] & H \arrow[u] \end{tikzcd}$$

3.2.4 Completeness of commutative topological groups

We have already remarked that the left and right uniformities coincide on a commutative topological group G; whenever we speak of the uniformity of G, it is this unique uniformity to which we refer.

Theorem 3.2.17. *Let G be a commutative topological group. Then the functions $x \mapsto x^{-1}$ and $(x, y) \mapsto xy$ are uniformly continuous on G and $G \times G$ respectively. Moreover G admits a Hausdorff completion $\widehat{G}$, and $\widehat{G}$ is commutative.*

Proof. The uniform continuity of $x \mapsto x^{-1}$ follows from Proposition 3.2.2, and that of $(x, y) \mapsto xy$ from Proposition 3.2.11, since $(x, y) \mapsto xy$ is a continuous homomorphism of $G \times G$ into G. If G is Hausdorff, it satisfies the condition of Theorem 3.2.12 (as does every Hausdorff group whose left and right uniformities coincide); moreover the functions $(x, y) \mapsto xy$ and $(x, y) \mapsto yx$ are equal on $G \times G$, hence on $\widehat{G} \times \widehat{G}$; hence the second part of the theorem, by considering in the general case the Hausdorff group associated with G. □

It follows in particular from this theorem that if f and g are two uniformly continuous mappings of a uniform space X into a commutative group G, written additively, then the functions $-f$ and $f + g$ are uniformly continuous.

Completeness of a commutative topological group G does not generally imply completeness of $\widehat{G}/H$ even when H is closed subgroup of G. If G is metrizable, it does, however, as we show next.

Proposition 3.2.18. *If H is a closed subgroup of a complete commutative pseudometrizable topological group (G, d) where d is invariant, then G/H is complete.*

Proof. By Proposition 3.1.60 the quotient G/H can be pseudometrizable by the metric $\bar{d}$. Let $(\bar{x}_n)$ be a Cauchy sequence from G/H. By choosing a subsequence if necessary, we may assume that $\bar{d}(\bar{x}_{n+1}, \bar{x}_n) < 2^{-n}$ for each $n \in \mathbb{N}$. Choose $h_1 \in H$ and let $w_1 = x_1 + h_1$. Then, for each n, choose $h_n \in H$ such that $w_n = x_n - x_{n-1} + h_n$ and $d(w_n, 0) < 2^{-(n-1)}$. Now form the sums $y_n = w_1 + \cdots + w_n$ and note that

$$y_n = (x_1 + h_1) + (x_2 - x_1 + h_2) + \cdots + (x_n - x_{n-1} + h_n) = x_n + (h_1 + \cdots + h_n)$$

so that the canonical image $\pi(y_n) = \bar{x}_n$. Since, for each $n \in \mathbb{N}$,

$$d(y_n, y_{n+1}) = d(y_n - y_{n+1}, 0) = d(w_n, 0) \leq 2^{-(n-1)},$$

it follows that (y_n) is a Cauchy sequence in G and therefore has a limit y. By the continuity of π, $\bar{x}_n = \pi(y_n) \to \pi(y)$ and G/H is complete. □

Proposition 3.2.19. *Let G be a commutative group, and let $\mathcal{T}_1$, $\mathcal{T}_2$ be two Hausdorff topologies compatible with the group structure of G. Suppose that $\mathcal{T}_1$ is finer than $\mathcal{T}_2$ and that there is a fundamental system of neighbourhoods of 0 for $\mathcal{T}_1$ which are closed for $\mathcal{T}_2$. Let $\widehat{G}_1$, $\widehat{G}_2$ be the completions of G with respect to the topologies $\mathcal{T}_1$, $\mathcal{T}_2$, respectively, and let $f : \widehat{G}_1 \to \widehat{G}_2$ be the continuous homomorphism which extends the identity mapping of G. Then f is injective.*

Proof. Suppose that G is written additively. Let $\mathcal{U}_1$ be the uniformity on G corresponding to $\mathcal{T}_1$: it will suffices to show that if $\mathfrak{F}$ and $\mathfrak{F}'$ are two minimal Cauchy filters with respect to $\mathcal{U}_1$, which converges in G_2 to the same point a, then $\mathfrak{F} = \mathfrak{F}'$. For this, it is enough to show that $\mathfrak{F} \cap \mathfrak{F}'$ is a Cauchy filter with respect to $\mathcal{U}_1$. Let V be a neighborhod of 0 in G with respect to $\mathcal{T}_1$, such that V is closed in $\mathcal{T}_2$, and let W be a symmetric neighborhood of 0 in G with respect to $\mathcal{T}_1$, such that $W + W \subseteq V$. By hypothesis, there is a W-small set M (resp. M') in $\mathfrak{F}$ (resp. $\mathfrak{F}'$); if $x \in M$ and $y \in M$ we have $y - x \in W$, i.e., $y \in x + W$. If $\overline{W}$ and $\overline{V}$ are the closures of W and V in G_2, it follows that $y \in x + \overline{W}$, and therefore, since a is in the closure of M, that $a \in x + \overline{M}$ for each $x \in M$. Similarly, $a \in x' + \overline{W}$ for each $x' \in M'$, and hence $x - x' \in \overline{W} + \overline{W}$; but since $(x, y) \mapsto x + y$ is a continuous map of $G_2 \times G_2$ into G_2, we have $\overline{W} + \overline{W} \subseteq \overline{W + W} \subseteq \overline{V}$. It follows that if $x \in M$ and $x' \in M'$, then $x - x' \in \overline{V} \cap G = V$, because V is closed in $\mathcal{T}_2$; and this completes the proof. □

Corollary 3.2.20. *Under the hypotheses of Proposition 3.2.19, if A is a subset of G which is a complete subspace with respect to the uniformity corresponding to $\mathcal{T}_2$, then A is also a complete subspace with respect to the uniformity corresponding to $\mathcal{T}_1$.*

Proof. If A_1 is the closure of A in G_1, then $f(A_1)$ is contained in the closure of A in G_2, which by hypothesis is equal to A. Since $f(A) = A$ by definition and f is injective, we have $A_1 = A$. □

3.3 Topological group with operators, topological rings, modules and fields

3.3.1 Topological group with operators

A **group with operators** (or **Ω-group**) (G, Ω) is defined as a group G together with an action of a set Ω on G:

$$\Omega \times G \to G, \quad (\omega, g) \mapsto g^{\omega}$$

that is distributive relative to the group law:

$$(g \cdot h)^{\omega} = g^{\omega} \cdot h^{\omega}$$

for all $g, h \in G$ and $\omega \in \Omega$. For each $\omega \in \Omega$, the application $g \mapsto g^{\omega}$ is then an endomorphism of G. From this, a Ω-group can also be viewed as a group G with an indexed family $(f_{\omega})_{\omega \in \Omega}$ of endomorphisms of G. The set Ω is called the **operator domain** and f_{ω} are called the **homotheties** of G.

Given two groups G, H with same operator domain Ω, a **homomorphism of groups with operators** is a group homomorphism $\phi : G \to H$ satisfying

$$\phi(g^{\omega}) = \phi(g)^{\omega}$$

for all $g \in G$ and $\omega \in \Omega$. A subgroup S of G is called a **stable subgroup**, **Ω-subgroup** or **invariant subgroup** if it respects the homotheties, that is, $s^\omega \in S$ for all $s \in S$ and $\omega \in \Omega$,

On a set G, a structure of a group with operators and a topology are said to be **compatible** if the topology and the group structure of G are compatible and if in addition the endomorphisms of G produced by the operators are continuous. The set G, together with the given topology and structure of group with operators, is then said to be a **topological group with operators**.

If H is a stable subgroup of a topological group G with operators, then the topology induced on H by the topology of G is compatible with the structure of group with operators on H. Furthermore:

Proposition 3.3.1. *If H is a stable subgroup of a topological group G with operators, then the closure $\overline{H}$ of H in G is a stable subgroup of G.*

Proof. We know already that $\overline{H}$ is a subgroup of G. Also if f_ω is any operator on G, the image of $\overline{H}$ under the continuous mapping f_ω is contained in $\overline{H}$, so the claim follows. □

Let H be a stable normal subgroup of a topological group G with operators. Then for each operator f_ω on G, the mapping of G/H into itself induced by f_ω is continuous by Proposition 3.1.36, and the structure of group with operators on G/H is therefore compatible with the quotient topology on G/H. We therefore have the following result.

Proposition 3.3.2. *Let H be a stable normal subgroup of a topological group G with operators, then G/H is also a topological group with operators.*

Let $(G_i)_{i\in I}$ be a family of topological groups with operators, where each G_i is assumed to have the same operator domain Ω. For each $\omega \in \Omega$, the mapping $(x_i) \mapsto (x_i^\omega)$ of $G = \prod_{i\in I} G_i$ into itself is continuous, and the structure of groups with operators on G is therefore compatible with the product topology on G. This defines G into a topological group with operators.

If G is a Hausdorff topological group with operators and if G has a completion G, then every endomorphism f_ω of G defined by an operator on G can be extended by continuity to an endomorphism of G (Theorem 2.2.28). Hence $\widehat{G}$ has the structure of a topological group with operators, and the operator set is the same for $\widehat{G}$ as for G.

3.3.2 Topological direct sum of stable subgroups

Since the study of commutative groups with operators is equivalent to the study of modules we shall sometimes allow ourselves to use the terminology proper to modules for arbitrary commutative groups with operators; thus we may speak of linear mappings instead of homomorphisms of commutative groups with operators, and we may use the word projector to denote an idempotent endomorphism of a commutative group with operators.

If a commutative topological group G with operators is the direct sum of a finite family $(G_i)_{i=1}^n$ of stable subgroups, then the canonical bijection $(x_i) \to \sum_{i=1}^n x_i$ of the product group $\prod_{i=1}^n G_i$ onto G is continuous, but is not necessarily a homeomorphism.

Definition 3.3.3. *Let G be a commutative topological group with operators, and let $(G_i)_{i=1}^n$ be a finite family of stable subgroups of G, such that G is the direct sum of the G_i. Then G is said to be the*

topological direct sum *of the G_i if the canonical mapping $(x_i) \mapsto \sum_{i=1}^n x_i$ of the product group $\prod_{i=1}^n G_i$ onto G is a homeomorphism.*

Proposition 3.3.4. *Let G be a commutative topological group with operators which is the direct sum of stable subgroups $(G_i)_{i=1}^n$. Let $(P_i)_{i=1}^n$ be the family of projections associated with the decomposition $G = \sum_{i=1}^n G_i$. Then G is the topological direct sum of the G_i if and only if the P_i are continuous.*

Proof. Note that the mapping $x \mapsto (P_i(x))$ is the inverse of the mapping $(x_i) \mapsto \sum_{i=1}^n x_i$. □

If G is the topological direct sum of two stable subgroups H, K, then K is said to be a topological complement of H in G; this is the case if and only if the canonical mapping of G/H onto K an isomorphism of topological groups with operators.

Corollary 3.3.5. *Let G be a commutative topological group with operators, and let H be a stable subgroup of G. Then the following conditions are equivalent:*

(i) H has a topological complement in G.

(ii) There is a continuous projection P on G such that $P(G) = H$.

(iii) The identity mapping of H can be extended to a continuous linear mapping of G onto H.

Proof. It follows from Proposition 3.3.4 that (i) implies (ii), and it is clear that (ii) implies (iii). Finally, if P is a continuous linear mapping of G onto H which extends the identity mapping of H, then P is a continuous projection, and the projections P and $I - P$ are associated with the direct sum decomposition $G = H + K$, where $K = P^{-1}(0)$. □

Corollary 3.3.6. *If a Hausdorff commutative topological group with operators is the topological direct sum of a family $(G_i)_{i=1}^n$ of stable subgroups, then each of the subgroups G_i is closed in G.*

3.3.3 Topological rings and modules

Definition 3.3.7. *A **topological ring** is a set A which carries a ring structure and a topology satisfying the following axioms:*

(RT1) The mapping $(x, y) \mapsto x + y$ of $A \times A$ into A is continuous.

(RT2) The mapping $x \mapsto -x$ of A into A is continuous.

(RT3) The mapping $(x, y) \mapsto xy$ of $A \times A$ into A is continuous.

The first two axioms express that the topology of A is compatible with its additive group structure. If a ring structure and a topology are given on a set A, they are said to be compatible if they satisfy these axioms.

In a topological ring every left homothety $x \mapsto ax$ (resp. every right homothety $x \mapsto xa$) is continuous (and is a homeomorphism if a is a unit of A). Since we can write identically

$$xy - ab = (x - a)(y - b) + (x - a)b + a(y - b)$$

the axiom (RT3) [in view of (RT1) and (RT2) is equivalent to the conjunction of the following two axioms:

(RT3a) Given any $a \in A$, the mappings $x \mapsto ax$ and $x \mapsto xa$ are continuous at the point 0.

(RT3b) The mapping $(x, y) \mapsto xy$ of $A \times A$ into A is continuous at the point $(0, 0)$.

From this we can deduce a necessary and sufficient set of conditions which the filter $\mathfrak{B}$ of neighbourhoods of 0 in a ring A must satisfy in order to define a topology on A compatible with its ring structure: $\mathfrak{B}$ must satisfy axioms (GV1) and (GV2), and also the following two axioms: (note that (GV3) is automatically satisfied since we are considering abelian groups)

(RV1) For all $a \in A$ and all $V \in \mathfrak{B}$, there exists $W \in \mathfrak{B}$ such that $aW \subseteq V$ and $Wa \subseteq V$.

(RV2) For all $V \in \mathfrak{B}$, there exists $W \in \mathfrak{B}$ such that $WW \subseteq V$.

Example 3.3.8. Let $\mathfrak{B}$ be a filter base on a ring A, consisting of two-sided ideals. Then $\mathfrak{B}$ is a fundamental system of neigbourhoods of 0 for a topology compatible with the additive group structure of A, and it follows immediately from (RV1) and (RV2) that this topology is compatible with the ring structure of A. This case happens, for example, if $\mathfrak{a}$ is an ideal of A and we set

$$\mathfrak{B} = \{\mathfrak{a}^n : n \in \mathbb{N} \text{ and } n > 0\}.$$

The topology therefore defined by $\mathfrak{B}$ can be used to produce the $\mathfrak{a}$-adic completion of A.

If B is a subring of a topological ring A, then the topology induced on B by that of A is compatible with the ring structure of B. The topological ring structure thus defined on B is said to be induced by that of A. Similar to subgroups, we have the following result.

Proposition 3.3.9. *Let B be a subring (resp. left ideal, right ideal, two-sided ideal) of a topological ring A. Then the closure $\overline{B}$ of $\overline{B}$ in A is a subring (resp. left ideal, right ideal, two-sided ideal) of A.*

Let I be a two-sided ideal in a topological ring A. By the same argument as for quotient groups, we see that the quotient of the topology of A by the relation $x - y \in I$ is compatible with the ring structure of A/I. In particular, if A is not Hausdorff, then the closure N of $\{0\}$ in A is a closed two-sided ideal, by Proposition 3.3.9; the quotient ring, which is Hausdorff, is called the Hausdorff ring associated with A.

Let $(A_i)_{i \in I}$ be a family of topological rings. On the set $A = \prod_{i \in I} A_i$ the product of the topologies of the A_i is compatible with the product of the ring structures of the A_i (same proof as for product groups); the topological ring A thus defined is called the **product** of the topological rings A_i.

When we speak of the uniformity of a topological ring, we always mean the uniformity of its additive group, unless the contrary is expressly stated; in particular, A is said to be a complete ring if the additive group of A is complete. Let A be a Hausdorff topological ring; as an additive group A can be considered as a dense subgroup of a complete Hausdorff commutative group A, which is determined up to isomorphism. In order that we should be able to consider A as a subring of a complete ring, it is necessary to be able to extend the function $(x, y) \mapsto xy$ by continuity to the space $\widehat{A} \times \widehat{A}$. The possibility of this extension will follow from the following more general theorem:

Theorem 3.3.10. *Let E, F, G be three complete Hausdorff commutative groups; let A be a dense subgroup of E and let B be a dense subgroup of F. If $f : A \times B \longrightarrow G$ is a continuous $\mathbb{Z}$-bilinear mapping, then f can be extended by continuity to a continuous $\mathbb{Z}$-bilinear mapping of $E \times F$ into G.*

Proof. Let (a, b) be an arbitrary point of $E \times F$, and let $\mathfrak{A}$, $\mathfrak{B}$ be the traces on A, B respectively of the neighbourhood filters of (x_0, y_0) ($\mathfrak{A}$ and $\mathfrak{B}$ are filters, by hypothesis). To show that f can be extended by continuity, it is enough to show that $f(\mathfrak{A} \times \mathfrak{B})$ is a Cauchy filter-base on G (by Theorem 2.2.27). Consider the identity

$$\begin{aligned} f(\tilde{x}, \tilde{y}) - f(x, y) &= f(\tilde{x} - x, y) + f(x, \tilde{y} - y) + f(\tilde{x} - x, \tilde{y} - y) \\ &= f(\tilde{x} - x, b) + f(a, \tilde{y} - y) + f(\tilde{x} - x, \tilde{y} - b) + f(x - a, \tilde{y} - y) + f(\tilde{x} - x, \tilde{y} - y). \end{aligned}$$

We shall show that by taking (x, y) and $(\tilde{x}, \tilde{y})$ in a sufficiently small set of $\mathfrak{A} \times \mathfrak{B}$, and by choosing a and b suitably, we can make each of the terms on the right-hand side very small. Let W be any neighbourhood of 0 in G; since f is continuous at $(0, 0) \in A \times B$, there is a set $U \in \mathfrak{A}$ and a set $V \in \mathfrak{B}$ such that $f(\tilde{x} - x, \tilde{y} - y) \in W$ whenever $x, \tilde{x} \in U$ and $y, \tilde{y} \in V$. Take a point $a \in U$ and a point $b \in V$, then for all $x, \tilde{x} \in U$ and $y, \tilde{y} \in V$, we have

$$f(\tilde{x} - x, \tilde{y} - b) + f(x - a, \tilde{y} - y) \in W + W.$$

On the other hand, the partial mapping $x \mapsto f(x, b)$ is continuous on A; hence there is a set $U' \subseteq U$ belonging to $\mathfrak{A}$ and such that $f(\tilde{x} - x, b) \in W$ whenever $x, \tilde{x} \in U'$. Likewise, there exists $V' \subseteq V$ belonging to $\mathfrak{B}$ such that $f(a, \tilde{y} - y) \in W$ whenever $y, \tilde{y} \in V'$. Consequently, if (x, y) and $(\tilde{x}, \tilde{y})$ are any two points of $U' \times V'$, then we have

$$f(\tilde{x}, \tilde{y}) - f(x, y) \in W + W + W + W + W.$$

This proves the existence of the extension $\bar{f}$ of f. The fact that $\bar{f}$ is $\mathbb{Z}$-bilinear is an immediate consequence of the principle of extension of identities. □

In the application of this theorem to a Hausdorff topological ring A, we take E, F and G to be $\widehat{A}$, A and B to be the ring A, and f to be the $\mathbb{Z}$-bilinear mapping $(x, y) \mapsto xy$, which by hypothesis is continuous. We denote again by xy the value of the extended function on $\widehat{A} \times \widehat{A}$; this function is a law of composition on $\widehat{A}$, and to say that it is $\mathbb{Z}$-bilinear means that it is distributive on both sides with respect to addition; and it is also associative, by the principle of extension of identities. Consequently,

Proposition 3.3.11. *A Hausdorff topological ring A is isomorphic to a dense subring of a complete Hausdorff ring $\widehat{A}$, which is determined up to isomorphism (and is called the* ***completion*** *of A). If A is commutative (resp. has an identity element) then the same is true for $\widehat{A}$.*

Let A be a topological ring, not necessarily Hausdorff; let I be the closure of $\{0\}$ in A, and let $A' = A/I$ be the Hausdorff ring associated with A. Then $\widehat{A'}$, the completion of A', is called the **Hausdorff completion** of A and is also denoted by $\widehat{A}$. One in the case of topological groups, the following results are valid.

Proposition 3.3.12. *Let A be a topological ring and C a complete Hausdorff topological ring. Then every continuous ring homomorphism f of A with a can be uniquely factorized as $f = g \circ \iota$, where g is a continuous homomorphism of $\widehat{A}$ into C and ι is the canonical mapping of A into $\widehat{A}$.*

Proposition 3.3.13. *If A, B are two topological rings, and $f : A \to B$ is a continuous homomorphism,*

there is therefore a unique continuous homomorphism $\hat{f} : \widehat{A} \to \widehat{B}$ *such that the diagram*

$$\begin{tikzcd} \widehat{A} \arrow[r, "\hat{f}"] & \widehat{B} \\ A \arrow[u] \arrow[r, "f"] & B \arrow[u] \end{tikzcd}$$

is commutative.

Definition 3.3.14. *Given a topological ring A with an identity element, a* ***topological left A-module*** *is a set M carrying a left A-module structure and a topology compatible with the additive group structure of M, and satisfying the following axiom:*

(MT) The mapping $(a, x) \mapsto ax$ of $A \times M$ into M is continuous.

We define similarly the notion of a topological right A-module; since every right A-module can be considered as a left A^{op}-module, where A^{op} is the opposite ring of A, and since the topology of A is compatible with the ring structure of A^{op}, there is no need to distinguish between topological right A-modules and topological left A^{op}-modules.

Example 3.3.15. Let A be a ring and let $\mathfrak{B}$ be a filter base on A consisting of two-sided ideals of A; let M be a left A-module. If we give A the topology (compatible with its ring structure) for which $\mathfrak{B}$ is a fundamental system of neighbourhoods of 0 (Example 3.3.8), and M the topology (compatible with its additive group structure) in which the sets IM, as I runs through $\mathfrak{B}$, form a fundamental system of neighbourhoods of 0, it is immediately verified that M is a topological A-module.

Example 3.3.16. Every commutative topological group is a topological $\mathbb{Z}$-module when the ring $\mathbb{Z}$ is given the discrete topology.

Given a topological ring A, consider, on a left A-module M, a topology compatible with the additive group structure of M. By virtue of the identity

$$ax - a_0x_0 = (a - a_0)x_0 + a_0(x - x_0) + (a - a_0)(x - x_0)$$

the axiom (MT) is equivalent to the conjunction of the following three axioms:

(MT1) For each $x_0 \in M$, the mapping $a \mapsto ax_0$ is continuous at the point 0.

(MT2) For each $a_0 \in A$, the mapping $x \mapsto a_0x$ is continuous at the point 0.

(MT3) The mapping $(a, x) \mapsto ax$ is continuous at the point $(0, 0)$.

We deduce from this a necessary and sufficient set of conditions that the filter $\mathfrak{B}$ of neighbourhoods of 0 in an A-module M must satisfy in order to define a topology on M compatible with its module structure; $\mathfrak{B}$ must satisfy the axioms (GV1) and (GV2), and in addition must satisfy the following three axioms:

(MV1) For each $x_0 \in M$ and $V \in \mathfrak{B}$, there is a neigbourhood S of 0 in A such that $Sx_0 \subseteq V$.

(MT2) For each $a_0 \in A$ and $V \in \mathfrak{B}$, there exists $W \in \mathfrak{B}$ such that $a_0W \subseteq V$.

(MT3) For each $V \in \mathfrak{B}$ there exists $U \in \mathfrak{B}$ and a neighbourhood T of 0 in A such that $TU \subseteq V$.

If N is a submodule of a topological A-module M, it is clear that the topology induced on N by the topology of M is compatible with the module structure of N. As before, we have the following result on closure of a submodule.

Proposition 3.3.17. *Let M be a topological A-module, and N a submodule of M. Then $\overline{N}$ is a submodule of M.*

On the quotient A-module M/N, the topology which is the quotient by N of the topology of M is compatible with the A-module structure. To see this it is enough to show that the mapping $(a, \bar{x}) \mapsto a\bar{x}$ onto M/N is continuous. Now, since we may identify the additive topological groups $A \times (M/N)$ and $(A \times M)/(\{0\} \times N)$, it is enough to show that the mapping $(a, x) \mapsto a\bar{x}$ of $A \times M$ into M/N is continuous; and this is immediate, since the mapping in question is the composition of $x \mapsto \bar{x}$ and $(a, x) \mapsto ax$.

Let $(M_i)_{i \in I}$ be an arbitrary family of topological A-modules, and let $M = \prod_{i \in I} M_i$ be the A-module which is the product of the M_i. Then the product topology on M is compatible with the A-module structure of M. To prove this it is enough to show that the mapping $(a, x) \mapsto (a\pi_i(x))$ of $A \times M$ into M is continuous, or that for each index $i \in I$ the mapping $(a, x) \mapsto a\pi_i(x)$ is a continuous mapping of $A \times M \to M_i$, which is obvious.

Let A be a Hausdorff topological ring and M a Hausdorff topological A-module. Let $\widehat{M}$ be the additive group which is the completion of the commutative topological group M. The $\mathbb{Z}$-bilinear mapping $(a, x) \mapsto ax$ of the product $A \times M$ of the additive groups A, M into the additive group M can be extended by continuity to a $\mathbb{Z}$-bilinear mapping of $A \times M$ into M by Theorem 3.3.10, and this mapping we continue to denote by $(a, x) \mapsto ax$. By virtue of the principle of extension of identities, this map then defines an $\widehat{A}$-module structure on $\widehat{M}$ compatible with its topology. The topological $\widehat{A}$-module $\widehat{M}$ thus defined is called the completion of the topological A-module M.

Let M be a topological module over a topological ring A, where neither A nor M is necessarily Hausdorff. Let I (resp. N) be the closure of $\{0\}$ in A (resp. M). Then I is a two-sided ideal of A and N is a sub-A-module of M; furthermore, by continuity we have $ax \in N$ whenever $a \in I$ or $x \in N$. We can therefore define, by passing to the quotients, a mapping $(\bar{a}, \bar{x}) \mapsto \bar{a}\bar{x}$ of $(A/I) \times (M/N)$ into M/N; it is easily verified (by use of Corollary 3.1.51) that this mapping is continuous, and therefore defines a structure of a topological (A/I)-module on M/N. If we put $A' = A/I$ and $M' = M/N$, then the A'-module M' is called the **Hausdorff module associated with M**; its completion is a topological module over the Hausdorff completion $\widehat{A}$ of A, and this module is called the Hausdoiff completion of M and is denoted by $\widehat{M}$.

Proposition 3.3.18. *every continuous homomorphism $f : M \to N$ of M into a complete Hausdorff A-module N factorizes uniquely into $f = g \circ \iota$, where g is a continuous homomorphism of $\widehat{M}$ into N and ι is the canonical mapping of M into $\widehat{M}$.*

Proposition 3.3.19. *If M, N are two topological A-modules and $f : M \to N$ is a continuous homomorphism, then there is a unique continuous homomorphism $\hat{f} : \widehat{M} \to \widehat{N}$ such that the diagram*

$$\begin{tikzcd} \widehat{M} \arrow[r, "\hat{f}"] & \widehat{N} \\ M \arrow[u] \arrow[r, "f"] & N \arrow[u] \end{tikzcd}$$

is commutative.

3.3.4 Topological division ring and fields

Definition 3.3.20. *A topological division ring is a set K carrying a division ring structure and a topology compatible with the ring structure of K, and satisfying in addition the following axiom:*

(KT) The mapping $x \mapsto x^{-1}$ of $K^\times$ into $K^\times$ is continuous.

A commutative topological division ring is called a ***topological field****.*

A division ring structure and a topology on a set K are said to be compatible if the corresponding ring structure and the topology are compatible and if in addition axiom (KT) is satisfied.

Example 3.3.21. On any division ring K, the discrete topology is compatible with the division ring structure. A topological division ring whose topology is discrete is called a **discrete division ring**.

By definition, if K is a topological division ring, then the topology induced by that of K on the multiplicative group $K^\times$ is compatible with the group structure of $K^\times$.

If $a \in K^\times$, the homotheties $x \mapsto ax$ and $x \mapsto xa$ are homeomorphisms of K onto itself; and so is the mapping $x \mapsto ax + y$ for all $y \in K$. Note that the homotheties $x \mapsto ax$ and $x \mapsto xa$ are automorphisms of the (topological) additive group of K. If V is any neighbourhood of 0 in K, it follows therefore that aV and Va are neighbourhoods of 0. If A is a division subring of a topological division ring K, then the topology induced on A by the topology of K is compatible with the division ring structure of A. The structure of a topological division ring thus defined on A is said to be induced by that of K. Furthermore, $\overline{A}$ is also a division subring of K.

If K is a topological division ring it is necessary to distinguish between:

(a) the uniformity of the additive group of K, which is defined on K and is called the **additive uniformity** of K;

(b) the left and right uniformities of the multiplicative group $K^\times$, which are defined on $K^\times$ and are called (by abuse of language) the multiplicative uniformities of K

The uniformity induced on $K^\times$ by the additive uniformity of K is in general distinct from the multiplicative uniformities of K. By Proposition 3.3.11, a Hausdorff topological division ring K can be considered as a dense subring of a complete Hausdorff ring $\widehat{K}$. In order that $\widehat{K}$ should be a topological division ring it is necessary that the mapping $x \mapsto x^{-1}$ be extendable by continuiry to $\widehat{K}^\times$; and this necessary condition is also sufficient, for the functions $x \mapsto xx^{-1}$, $x \mapsto x^{-1}x$ and $x \mapsto 1$ are then equal on $\widehat{K}^\times$ by reason of the principle of extension of identities, and therefore the value of the extended function is the inverse of x for each $x \in \widehat{K}^\times$. In other words,

Proposition 3.3.22. *The completion $\widehat{K}$ of a Hausdorff topological division ring K is a topological division ring if and only if the image under the mapping $x \mapsto x^{-1}$ of every Cauchy filter (with respect to the additive structure) which does not have a cluster point at 0, is a Cauchy filter (with respect to the additive structure).*

There are topological division rings in which this condition is not satisfied and in which the ring $\widehat{K}$ has zero divisors. Moreover, even if the completion $\widehat{K}$ is a topological division ring, there is no a priori reason to assume that the multiplicative structures of $\widehat{K}$ are structures of a complete space. However, this will be the case for division rings K such that $\widehat{K}$ is locally compact, and for topological fields; for the latter, we have the following proposition:

Proposition 3.3.23. *If the additive uniform structure of a topological field K is a structure of a complete Hausdorff space, then the multiplicative structure on $\widehat{K}^\times$ is a structure of a complete space.*

Proof. We shall show that if $\mathfrak{F}$ is a Cauchy filter with respect to the multiplicative structure on $K^\times$, then $\mathfrak{F}$ is a Cauchy filter with respect to the additive structure on K, and does not converge to 0; this will establish the result. Let U be any neighbourhood of 0 in K, let V be a closed neighbourhood of 0 such that $V \subseteq U$, $VV \subseteq U$ and $-1 \notin U$; then by hypothesis there is a set $A \in \mathfrak{F}$ such that, for all $x \in A$ and $y \in A$, we have $x^{-1}y \in 1+A$. Let $a \in A$, then $A \subseteq a+aV$, and $a+aV$ is a closed set which does not contain 0 hence 0 is not in the closure of A and is therefore not a cluster point of $\mathfrak{F}$. Let W be a neighbourhood of 0 such that $aW \subseteq V$; then by hypothesis there is a set $B \in \mathfrak{F}$ such that $B \subseteq A$ and, for all $x \in B$ and $y \in B$, we have $x^{-1}y \in 1+W$, hence

$$y - x \in xW \subseteq AW \subseteq aW + aVW.$$

But K is commutative, and therefore $aVW = aWV \subseteq VV \subseteq U$; consequently $y - x \in U + U$ and the proposition is proved. □

3.3.5 Inverse limits of topological groups and rings

Throughout this part, I denotes a non-empty directed set and $\preceq$ denotes the partial order relation in I. Unless the contrary is expressly stated, all the inverse systems considered are indexed by I.

Let $(X_\alpha, f_{\alpha\beta})$ be an inverse system of sets, and suppose that each X_α is endowed with an internal law of composition, everywhere defined, and written multiplicatively. Suppose also that the $f_{\alpha\beta}$ are homomorphisms with respect to these internal laws. Since

$$f_{\alpha\beta}(x_\beta y_\beta) = f_{\alpha\beta}(x_\beta) f_{\alpha\beta}(y_\beta)$$

whenever $\alpha \preceq \beta$ and x_α and y_β belong to X_β, it is clear that $X = \varprojlim X_\alpha$ is a stable subset of the product $\prod X_\alpha$, with respect to the internal law $(x_\alpha) \cdot (y_\alpha) = (x_\alpha y_\alpha)$. Let $(\Omega_\alpha, \varphi_{\alpha\beta})$ be another inverse system of sets, indexed by I, and suppose that each X_α carries an external law of composition, everywhere defined, written multiplicatively and having Ω_α as a set of operators, such that whenever $\alpha \preceq \beta$ we have

$$f_{\alpha\beta}(\lambda_\beta x_\beta) = \varphi_{\alpha\beta}(\lambda_\alpha) f_{\alpha\beta}(x_\beta)$$

for $\lambda_\alpha \in \Omega_\alpha$ and $x_\beta \in X_\beta$. Then we can define an external law on $\prod X_\alpha$ having $\prod \Omega_\alpha$ as a set of operators, by $(\lambda_\alpha) \cdot (x_\alpha) = (\lambda_\alpha \cdot x_\alpha)$. Restricting the set of operators to $\Omega = \varprojlim \Omega_\alpha$, we have an external law on $\prod X_\alpha$ with respect to which X is again a stable subset. The internal (resp. external) law thus defined on X is said to be the **inverse limit** of the internal (resp. external) laws of the X_α. In the case of external laws, it may happen that all the Ω_α are identical with the

same set Ω_0 and that all the $\varphi_{\alpha\beta}$ are identity mappings; then, since I is a directed set, Ω can be identified with Ω_0.

It is immediately verified that the usual properties of associativity, commutativity, existence of an identity element for an internal law (provided that the $f_{\alpha\beta}$'s map identity element to identity element), distributivity of an external law with respect to an internal law, etc., are preserved under passage to the inverse limit.

Let Σ be a species of algebraic structure and let Σ_0 be the impoverished structure corresponding to Σ. Whenever we speak of an inverse system of sets $(X_\alpha, f_{\alpha\beta})$ endowed with structures of species Σ, we shall always suppose that the $f_{\alpha\beta}$ are homomorphisms for these structures. If we endow $X = \varprojlim X_\alpha$ with the internal and external laws which are the respective inverse limits of the internal and external laws of the X_α, then X carries an algebraic structure of species Σ_0. Naturally it remains to be seen in each particular case whether or not this structure is of species Σ. For example, if $(G_\alpha, f_{\alpha\beta})$ is an inverse system of groups (resp. rings), then $\varprojlim G_\alpha$ is a subgroup (resp. subring) of $\prod X_\alpha$ and is called the inverse limit of the system $(G_\alpha, f_{\alpha\beta})$ of groups (resp. rings).

Let $(X_\alpha, f_{\alpha\beta})$ be an inverse system of sets and let $(G_\alpha, \varphi_{\alpha\beta})$ be an inverse system of groups; suppose that each X_α has G_α as a group of operators and that whenever $\alpha \preceq \beta$ have

$$f_{\alpha\beta}(g_\beta \cdot x_\beta) = \varphi_{\alpha\beta}(g_\beta) \cdot f_{\alpha\beta}(x_\beta) \tag{3.5.1}$$

for $x_\beta \in X_\beta$ and $g_\beta \in G_\beta$. Then $X = \varprojlim X_\alpha$ has $G = \varprojlim G_\alpha$ as group of operators. It follows from (3.5.1) that, if $\alpha \preceq \beta$, the mappings $f_{\alpha\beta}$ and $\varphi_{\alpha\beta}$ are compatible and hence define a mapping $\pi_{\alpha\beta} : X_\beta/G_\beta \to X_\alpha/G_\alpha$ of the quotient sets, such that $(X_\alpha/G_\alpha, \pi_{\alpha\beta})$ is an inverse system. Moreover, if $f_\alpha : X \to X_\alpha$ and $\varphi_\alpha : G \to G_\alpha$ are the canonical mappings, then f_α and φ_α are compatible and consequently define a mapping $\eta_\alpha : X/G \to X_\alpha/G_\alpha$ of the quotient sets; it is clear that the η_α form an inverse system of mappings, whose inverse limit is therefore a mapping $\eta : X/G \to \varprojlim X_\alpha/G_\alpha$, which is not necessarily either injective or surjective.

Again, let $(A_\alpha, f_{\alpha\beta})$ be an inverse system of rings and let $(M_\alpha, \phi_{\alpha\beta})$ be an inverse system of commutative groups; and suppose that each M_α carries a left A_α-module structure in such a way that whenever $\alpha \preceq \beta$ we have

$$f_{\alpha\beta}(\lambda_\beta \cdot x_\beta) = \varphi_{\alpha\beta}(\lambda_\beta) \cdot f_{\alpha\beta}(x_\beta) \tag{3.5.2}$$

for $x_\beta \in M_\beta$ and $\lambda_\beta \in A_\beta$; then $\varprojlim M_\alpha$ has a structure of a left module over $\varprojlim A_\alpha$. If we suppose in addition that, for each α, A_α is commutative and that each M_α has an A_α-algebra structure, and finally that $(M_\alpha, \phi_{\alpha\beta})$ is an inverse system of rings, then $\varprojlim M_\alpha$ has a structure of an algebra over $\varprojlim A_\alpha$.

Let $(G_\alpha, \phi_{\alpha\beta})$ be an inverse system of groups, and for each α let H_α be a subgroup of G_α. If $\phi_{\beta\alpha}(H_\beta) \subseteq H_\alpha$ whenever $\alpha \preceq \beta$, then the inverse system of subsets H_α of G_α is an inverse system of groups with respect to the restrictions of the $\phi_{\alpha\beta}$, and $H = \varprojlim H_\alpha$ is a subgroup of $G = \varprojlim G_\alpha$. If each H_α is a normal subgroup of G_α, then H is a normal subgroup of G. If $(G'_\alpha, \psi_{\alpha\beta})$ is another inverse system of groups and, for each α, $u_\alpha : G_\alpha \to G'_\alpha$ is a homomorphism such that the u_α's form an inverse system of mappings, then, if H_α is the kernel of u_α, we have $\psi_{\alpha\beta}(H_\beta) \subseteq H_\alpha$ whenever $\alpha \preceq \beta$. Thus $u = \varprojlim u_\alpha$ is a homomorphism of G into $G' = \varprojlim G'_\alpha$, and $H = \varprojlim H_\alpha$ is the kernel of u. If we put $K_\alpha = u_\alpha(G_\alpha)$, then we have

$\psi_{\alpha\beta}(K_\beta) \subseteq K_\alpha$ whenever $\alpha \preceq \beta$, so that the K_α form an inverse system of subgroups of the G_α; but $K = \varprojlim K_\alpha$ is not necessarily the image of G under u.

We shall say that an inverse system $(G_\alpha, \phi_{\alpha\beta})$ is an **inverse system of topological groups** if the G_α are topological groups and the $\phi_{\alpha\beta}$ are continuous homomorphisms. Then $G = \varprojlim G_\alpha$ is a subgroup of the product group $\prod G_\alpha$; if we endow G with the topological group structure induced by at that of $\prod G_\alpha$, then the topological group so obtained is called the inverse limit of the inverse system of topological groups $(G_\alpha, \phi_{\alpha\beta})$. If the G_α are Hausdorff (resp. Hausdorff and complete) then G is Hausdorff and closed in $\prod G_\alpha$ (resp. Hausdorff and complete). If $(G'_\alpha, \psi_{\alpha\beta})$ is another inverse system of topological groups and if, for each α, $u_\alpha : G_\alpha \to G'_\alpha$ is a continuous homomorphism such that the u_α form an inverse system of mappings, then $u = \varprojlim u_\alpha$ is a continuous homomorphism of G into $G' = \varprojlim G'_\alpha$. The same results are valid when "topological group" is replaced by "topological ring".

Let $(X_\alpha, f_{\alpha\beta})$ be an inverse system of topological spaces, and let $(G_\alpha, \phi_{\alpha\beta})$ be an inverse system of topological groups. Suppose that each G_α operates continuously on X_α and that the relations (3.5.1). We have seen that $X = \varprojlim X_\alpha$ has $G = \varprojlim G_\alpha$ as group of operators; furthermore, G operates continuously on X. For if f_α (resp. ϕ_α) is the canonical mapping $X \to X_\alpha$, (resp. $G \to G_\alpha$), then by definition

$$f_\alpha(g \cdot x) = \phi_\alpha(g) \cdot f_\alpha(x)$$

and therefore the mappings $(g, x) \mapsto f_\alpha(g \cdot x)$ are continuous on $X \times G$, which shows the continuity of $(g, x) \mapsto (g \cdot x)$. The mapping $\eta_\alpha : X/G \to X_\alpha/G_\alpha$, induced by f_α and ϕ_α is therefore continuous, and so is the mapping $\eta : X/G \to \varprojlim X_\alpha/G_\alpha$ defined by the η_α's.

Proposition 3.3.24. *Suppose that the X_α and the G_α satisfy the above hypotheses.*

(a) If the stabilizer of each point of X_α is a compact subgroup of G_α for each $\alpha \in I$, then the stabilizer of each point $x = (x_\alpha)$ of X is a compact subgroup of G, then the orbit of x (with respect to G) is canonically homeomorphic to the inverse limit of the orbits of the x_α (with respect to G_α), and the canonical mapping $\eta : X/G \to \varprojlim X_\alpha/G_\alpha$ is injective.

(b) If, for each $\alpha \in I$, every orbit of a point of X_α (with respect to G_α) is compact, then every orbit of a point of X (with respect to G) is relatively compact, and η is surjective. If also η is bijective, then every orbit of a point of X is compact.

Proof. Let $x = (x_\alpha) \in X$ and for each $\alpha \in I$ let $Y_\alpha = G_\alpha \cdot x_\alpha$ be the orbit of x_α. If $\alpha \preceq \beta$, it follows from (3.5.1) and the relation $f_{\beta\alpha}(x_\beta) = x_\alpha$ that $f_{\alpha\beta}(Y_\beta) = Y_\alpha$, and hence that (Y_α) is an inverse system of subsets of the X_α. For each $\alpha \in I$ let $\theta_\alpha : G_\alpha \to Y_\alpha$ be the continuous mapping $g_\alpha \to g_\alpha \cdot x_\alpha$. Then the θ_α form an inverse system of mappings, and $\theta = \varprojlim \theta_\alpha$ is the continuous mapping $g \mapsto g \cdot x$ of G into the subspace $Y = \varprojlim Y_\alpha$ of X. The hypothesis of (a) implies that $\theta_\alpha^{-1}(y_\alpha)$ is compact for each $y_\alpha \in Y_\alpha$. Since also θ_α is surjective, the conditions of Corollary 1.8.24 are satisfied, and the first two assertions of (a) are therefore established. Hence, if $x = (x_\alpha)$ and $y = (y_\alpha)$ are such that x_α and y_α belong to the same orbit with respect to G_α for each $\alpha \in I$, then x and y belong to the same orbit with respect to G, and therefore η is injective.

Likewise, the hypothesis of (b) implies that the inverse system of canonical mappings $\pi_\alpha : X_\alpha \to X_\alpha/G_\alpha$ satisfies the conditions of Corollary 1.8.24, and therefore its inverse limit

$\pi = \varprojlim \pi_\alpha : X \to \varprojlim X_\alpha/G_\alpha$ is surjective, and the inverse image under π of every point of $\varprojlim X_\alpha/G_\alpha$ is compact. Since π factorizes into

$$X \to X/G \to \varprojlim X_\alpha/G_\alpha$$

where $X \to X/G$ is the canonical mapping, the assertions of (b) follow. □

Corollary 3.3.25. *If the G_α are compact and the X_α are Hausdorff, then the conclusions of (a) and (b) in Proposition 3.3.24 are valid.*

Proof. The hypotheses of (a) and (b) are satisfied since every closed subgroup of G_α is compact and $u_\alpha : G_\alpha \to Y_\alpha$ is a continuous mapping of a compact space into a Hausdorff space. □

Corollary 3.3.26. *If for each $\alpha \in I$, the group G_α operates transitively on the space X_α and if the stabilizer of each point of X_α is a compact subgroup of G_α, then G operates transitively on X and the stabilizer of each point of X is a compact subgroup of G.*

Proof. In this case we have $Y_\alpha = X_\alpha$ and the hypotheses of (a) is satisfied. □

Corollary 3.3.27. *Suppose that the G_α are Hausdorff. For each $\alpha \in I$ let K_α be a compact subgroup of G_α such that $\phi_{\alpha\beta}(K_\beta) \subseteq K_\alpha$ whenever $\alpha \preceq \beta$. Then, if $K = \varprojlim K_\alpha$, the canonical mapping h of the homogeneous space G/K into $\varprojlim G_\alpha/K_\alpha$ is a homeomorphism.*

Proof. The fact that h is bijective follows from Corollary 3.3.25, applied by replacing X_α by G_α, and G_α by K_α operating by right translations. Let π be the canonical mapping $G \to G/K$, and for each α let ϕ_α be the canonical mapping $G \to G_\alpha$. If, for each α, V_α runs through a fundamental system of open neighbourhoods of the identity element e_α of G_α, then the sets $f_\alpha^{-1}(V_\alpha)$ form a fundamental system of neighbourhoods of the identity element e in G, and the sets $\pi(V \cdot K)$ form a fundamental system of neighbourhoods of $\pi(e)$ in G/K. We have to show that the image of $\pi(V \cdot K)$ under h contains a neighbourhood of $h(\pi(e))$, that is, there exists $\beta \succeq \alpha$ and a neighbourhood W_β of e_β in G_β such that $\phi_\beta^{-1}(W_\beta \cdot K_\beta) \subseteq V \cdot K$. Now, the relation $x \in V \cdot K$ is equivalent to the existence of y in K such that $\phi_\alpha(xy^{-1}) \in V_\alpha$, i.e., $\phi_\alpha(x) \in V_\alpha \cdot \phi_\alpha(K)$. Thus we get $V \cdot K = \phi_\alpha^{-1}(V_\alpha \cdot \phi_\alpha(K))$. Let $U_\alpha = V_\alpha \cdot \phi_\alpha(K)$, we shall see that there exists $\beta \succeq \alpha$ such that if we set $U_\beta = \phi_{\alpha\beta}^{-1}(U_\alpha)$, then $K_\beta \subseteq U_\alpha$. It will then follow from Corollary 2.3.13 that there is a neighbourhood W_β of e_β in G_β such that $W_\beta K_\beta \subseteq V_\alpha$, and this will establish the relation

$$\phi_\beta^{-1}(W_\beta \cdot K_\beta) \subseteq \phi_\beta^{-1}(U_\beta) = V \cdot K.$$

We proceed by reductio ad absurdum: for each $\beta \succeq \alpha$, let M_β denote $K_\beta \setminus U_\beta$. Since $\phi_{\beta\gamma}^{-1}(U_\beta) = U_\gamma$ if $\gamma \succeq \beta$, the M_β form an inverse system of compact subsets of the G_β (for $\beta \succeq \alpha$). If they were all nonempty, then their inverse limit M would also be non-empty (Proposition 1.8.23). It is clear that $M \subseteq K$ and $\phi_\alpha(M) \subseteq M_\alpha$; but this is absurd since $\phi_\alpha(K) \subseteq U_\alpha$, and the proof is therefore complete. □

Let G be a group and let (H_α) be a family of normal subgroups of G such that $H_\alpha \supseteq H_\beta$ whenever $\alpha \preceq \beta$. For each α let $G_\alpha = G/H_\alpha$ and $\pi_{\alpha\beta}$ be the canonical homomorphism $G/H_\beta \to G/H_\alpha$, which therefore maps a coset of H_β in G to the coset of H_α in G. Clearly $(G_\alpha, \pi_{\alpha\beta})$ is an inverse system of groups; the elements of $\widetilde{G} = \varprojlim G_\alpha$ are families $(T_\alpha)_{\alpha \in I}$ where T_α is a coset of H_α in G for each α, and $T_\alpha \supseteq T_\beta$ whenever $\alpha \preceq \beta$. The mapping $i : G \to \widetilde{G}$ given by

$g \mapsto (gH_\alpha)$ is the inverse limit of the canonical homomorphisms $G \to G/H_\alpha$; and is therefore a homomorphism of G into $\widetilde{G}$, and the inverse image under i of an element $(T_\alpha)_{\alpha\in I}$ is equal to $\bigcap_\alpha T_\alpha$. The kernel of i is therefore $\bigcap_\alpha H_\alpha$, and the image of i consists of all families (T_α) in $\widetilde{G}$ whose intersection is non-empty.

Now suppose that G is a topological group; if we give each $G_\alpha = G/H_\alpha$ the quotient topology, it is clear that $(G_\alpha, \pi_{\alpha\beta})$ is an inverse system of topological groups, and that $i : G \to \widetilde{G}$ is a continuous homomorphism.

Proposition 3.3.28. *Let G be a topological group and let $(H_\alpha)_{\alpha\in I}$ be a family of normal subgroups of G such that $H_\alpha \supseteq H_\beta$ whenever $\alpha \preceq \beta$, and which satisfy the following condition:*

(AP) For each $\alpha \in I$, H_α is closed in G and every neighbourhood of the identity element e in G contains one of the H_α (in other words, the filter base formed by the H_α converges to e).

Then the mapping $i : G \to \widetilde{G}$ is a strict morphism of G onto $i(G)$, $\widetilde{G}$ is Hausdorff and $i(G)$ is dense in G. Finally, the kernel of i is the closure of $\{e\}$ in G. If in addition one of the H_α is complete, then i is surjective.

Proof. Since H_α is closed, the $G_\alpha = G/H_\alpha$ are Hausdorff, hence so is G (since it is a subspace of $\prod G_\alpha$). The kernel H of i is the intersection of the H_α and is therefore a closed subgroup of G. Since each neighbourhood of e contains some H_α it contains H and therefore H is the closure of $\{e\}$. Let us next show that $i(G)$ is dense in $\widetilde{G}$. Let $\pi_\alpha : \widetilde{G} \to G_\alpha$ be the canonical mapping, which is the restriction to $\widetilde{G}$ of the projection. Then $\varphi_\alpha = \pi_\alpha \circ i$ is the canonical mapping $G \to G/H_\alpha$.

$$\begin{tikzcd} G \arrow[r, "i"] \arrow[dr, "\varphi_\alpha"'] & \widetilde{G} \arrow[d, "\pi_\alpha"] \\ & G/H_\alpha \end{tikzcd}$$

If U is any non-empty open set of $\widetilde{G}$, then there is an index $\alpha \in I$ and a non-empty open set V_α in G_α such that $\pi_\alpha^{-1}(V_\alpha) \subseteq U$; therefore $\varphi_\alpha^{-1}(U_\alpha) \subseteq i^{-1}(U)$. But since φ_α is surjective, $\varphi_\alpha^{-1}(U_\alpha)$ is not empty, and therefore $i(G) \cap U \neq \varnothing$.

To see that i is a strict morphism of G onto $i(G)$, consider a neighbourhood V of e in G. There is a neighbourhood W of e in G such that $W^2 \subseteq V$, and an index $\alpha \in I$ such that $H_\alpha \subseteq W$. It then follows that V contains $WH_\alpha = \varphi_\alpha^{-1}(\varphi_\alpha(W)) = i^{-1}(\pi_\alpha^{-1}(\pi_\alpha(W)))$. Since $\pi_\alpha^{-1}(\pi_\alpha(W))$ is a neighbourhood of the identity element in $\widetilde{G}$, the result follows.

Finally, suppose that there is an index $\gamma \in I$ such that H_γ is complete. To show that i is surjective it is enough to prove that every family $(T_\alpha) \in \widetilde{G}$ has a non-empty intersection. Since T_γ is obtained by translation from H_γ, it is a complete subspace of G (with respect to both the right and the left uniformities). Moreover, since every neighbourhood U of e in G contains one of the H_α, the corresponding set T_α is U_l- (or U_r-) small, and hence the set of T_α contained in T_γ is a Cauchy filter base; therefore it converges in T_γ, and since the T_α are closed in G (since they are translations of the H_α), their intersection is not empty. □

Corollary 3.3.29. *If the condition (AP) is satisfied and if in addition the groups G/H_α are complete, then the group G has a Hausdorff completion which can be identified with $\widetilde{G}$ and the mapping $i : G \to \widetilde{G}$ is then identified with the canonical mapping.*

Proof. For $\widetilde{G}$ is then complete, and Proposition 3.3.28 shows that $i(G)$ is isomorphic with the Hausdorff group associated with G; since it is dense in $\widetilde{G}$, the corollary follows. □

Corollary 3.3.30. *Let G be a group and let (H_α) be a family of normal subgroups of G directed with respect inclusion. If we endow G with the group topology for which the H_α form a fundamental system of neighbourhoods of the identity element e, then the Hausdorff group associated with G is isomorphic to $G' = G/(\bigcap_\alpha H_\alpha)$ and G' has a completion $\widetilde{G} = \varprojlim G/H_\alpha$. The canonical map $G \to G'$ extends to an isomorphism of $\widehat{G}$ onto $\widetilde{G}$.*

Proof. The subgroup H_α of G is open and therefore also closed, and G/H_α is discrete; hence the conditions of Corollary 3.3.29 are satisfied. □

For the remainder of this part we shall assume that G is Hausdorff and that (H_α) is a family of compact normal subgroups of G, which is directed with respect inclusion and which satisfies the condition (AP); by virtue of Proposition 3.3.28, the mapping

$$i : G \to \widetilde{G} = \varprojlim G/H_\alpha$$

is then an isomorphism of topological groups which permits us to identify G and $\widetilde{G}$. We denote by π_α the canonical mapping $G \to G/H_\alpha$.

Lemma 3.3.31. *Under the hypotheses of Proposition 3.3.28, if E is any closed subset of G we have $E = \bigcap_\alpha EH_\alpha$.*

Proof. For E is the intersection of the sets EV where V runs through the neighbourhood filter of e, and every neighbourhood of e contains an H_α; whence the result, since $E \subseteq EH_\alpha$. □

Proposition 3.3.32. *Suppose that G is Hausdorff and that the H_α are compact and satisfy (AP).*

(a) Let L be a closed subgroup of G; then, for each $\alpha \in I$, the subgroup $L_\alpha := \pi_\alpha(L)$ of $G_\alpha = G/H_\alpha$ is closed, and the isomorphism i of G onto $\lim G_\alpha$ gives by restriction an isomorphism of L onto $\varprojlim L_\alpha$. If also L is normal in G, then L_α is normal in G_α for each $\alpha \in I$, and by passing to the quotients, i induces an isomorphism of G/L onto $\varprojlim G/L_\alpha$.

(b) Conversely, for each $\alpha \in I$ let L_α be a closed subgroup of G_α such that $L_\alpha = \pi_{\alpha\beta}(L_\beta)$ whenever $\alpha \preceq \beta$. Then there is a unique closed subgroup L of G such that $L_\alpha = \pi_\alpha(L)$ for each $\alpha \in I$, and if in addition L_α is normal in G_α for each $\alpha \in I$, then L is normal in G.

Proof. First assume (a). Since H_α is compact, LH_α is closed in G by Proposition 3.1.11 and therefore L_α is closed in G_α. Since i identifies the topological groups G and $\varprojlim G_\alpha$ and since $\varprojlim L_\alpha$ may be identified with a (topological) subgroup of $\varprojlim G_\alpha$, i identifies the subgroup $\bigcap_\alpha LH_\alpha$ of G with $\varprojlim L_\alpha$, and to prove the first assertion it is enough to remark that $L = \bigcap_\alpha LH_\alpha$ by Lemma 3.3.31. On the other hand, if L is normal, then for each $\alpha \in I$ the mapping $\pi'_\alpha : G/L \to G_\alpha/L_\alpha$ induced by π_α is a surjective strict morphism (Example 3.1.42), whose kernel is the compact normal subgroup LH_α/L of G/L, the canonical image of the compact subgroup H_α of G. Since the subgroups LH_α/L of G/L satisfy condition (AP) (Proposition 3.1.43), and since G/L is Hausdorff, the last assertion of (a) is a consequence of Proposition 3.3.28.

Now we consider (b). Let $\pi'_{\alpha\beta}$ be the restriction of $\pi_{\alpha\beta}$ to L_α. Then $(L_\alpha, f'_{\alpha\beta})$ is an inverse system of topological groups, whose inverse limit L can be identified with the subgroup

$\bigcap_\alpha \pi_\alpha^{-1}(L_\alpha)$ of G. By hypothesis, $\pi'_{\alpha\beta}$ is surjective and its kernel is the compact subgroup $\pi_\beta(H_\beta) \cap L_\beta$ of L_α; consequently we have $L_\alpha = \pi_\alpha(L)$ for all $\alpha \in I$ (Proposition 1.8.23). If L' is another closed subgroup of G such that $\pi_\alpha(L') = L_\alpha$ for all $\alpha \in I$, then $L'H_\alpha = \pi_\alpha^{-1}(L_\alpha)$, whence

$$L' = \bigcap_\alpha L'H_\alpha = \bigcap_\alpha \pi_\alpha^{-1}(L_\alpha) = L.$$

Finally, the last assertion of (b) follows from the formula $L = \bigcap_\alpha \pi_\alpha^{-1}(L_\alpha)$, since the $\pi_\alpha^{-1}(L_\alpha)$ are now normal subgroups of G. □

Now we give an application of the previous results.

Proposition 3.3.33. *Let $(G_\alpha, \phi_{\alpha\beta})$ be an inverse system of Hausdorff topological groups such that the $\phi_{\alpha\beta}$ are surjective strict morphisms with compact kernels. Then for each $\alpha \in I$ the canonical mapping ϕ_α of $G = \varprojlim G_\alpha$ into G_α is a surjective strict morphism whose kernel is compact.*

Proof. The facts that ϕ_α is surjective and that its kernel is compact are consequences of Corollary 1.8.24. It remains to show that ϕ_α is a strict morphism. Let e (resp. e_α) denote the identity element of G (resp. G_α). Each neighbourhood V of e in G contains a set of the form $\phi_\beta^{-1}(V_\beta)$, where V_β is a neighbourhood of e_β in G_β, and we may suppose that $\beta \geq \alpha$. Since $\phi_{\beta\alpha}$ is a surjective strict morphism, $\phi_{\alpha\beta}(V_\beta)$ is a neighbourhood of e_α in G_α, and since ϕ_α is surjective, we have $V_\beta \subseteq \phi_\beta(V)$, whence

$$\phi_\alpha(V) = \phi_{\alpha\beta}(\phi_\beta(V)) \supseteq \phi_{\alpha\beta}(V_\beta)$$

This shows that $\phi_\alpha(V)$ is a neighbourhood of e_α in G_α. □

If $H_\alpha = \ker \phi_\alpha$, then each H_α is a compact normal subgroup of G. The H_α clearly satisfy the condition (AP) and G_α can be identified with G/H_α. In particular Proposition 3.3.32 apply to G and the H_α.

Corollary 3.3.34. *Let $(G_\alpha, \phi_{\alpha\beta})$ be an inverse system of topological groups which satisfies the hypotheses of Proposition 3.3.33. Let $(G'_\alpha, \phi'_{\alpha\beta})$ be an inverse system of topological groups, and for each α let $u_\alpha : G_\alpha \to G'_\alpha$ be a surjective strict morphism with compact kernel, such that the u_α from an inverse system of mappings. Then $u = \varprojlim u_\alpha$ is a strict morphism of $G = \varprojlim G_\alpha$ onto $G' = \varprojlim G'_\alpha$, and its kernel is compact.*

Proof. Let N_α be the kernel of u_α and H_α the kernel of ϕ_α. Then $L_\alpha = \phi_\alpha^{-1}(N_\alpha)$ is then the kernel of the surjective strict morphism $v_\alpha = u_\alpha \circ \phi_\alpha : G \to G'_\alpha$. Since L_α/H_α is isomorphic to N_α, L_α is a compact normal subgroup of G. The kernel L of u is the intersection of the L_α. Let π denote the canonical mapping $G \to G/L$; then we can write $v_\alpha = w_\alpha \circ \pi$, where w_α is a strict morphism of G/L onto G'_α, whose kernel is L_α/L. Since the intersection of the L_α/L is the identity element of G/L, and since the L_α/L form a filter base and are compact, this filter base converges to the identity element of G/L. Corollary 3.3.29 then shows that $w = \varprojlim w_\alpha$ is an isomorphism of G/L onto G'. It follows that $w \circ \pi$ is a strict morphism of G onto G', with kernel L. But it is clear that $u = w \circ \pi$, and thus the corollary is proved. □

Chapter 4

Topologies encountered in algebraic geometry

4.1 Irreducibility

4.1.1 Irredicible topological spaces

A topological space X is called **irreducible** if every finite intersection of non-empty open sets of X is non-empty. By considering the empty family of open sets of X it is seen that an irreducible space is non-empty. For a topological space X to be irreducible, it is necessary and sufficient that it be non-empty and that the intersection of two non-empty open sets of X be always non-empty (or, what amounts to the same thing, that the union of two closed sets distinct from X be always distinct from X).

Proposition 4.1.1. *Let X be a non-empty topological space. The following assertions are equivalent.*

(i) X is irreducible.

(ii) Any two non-empty open subsets of X have a non-empty intersection.

(iii) Every non-empty open subset is dense in X.

(iv) Every non-empty open subset is connected.

(v) Every non-empty open subset is irreducible.

Proof. It is clear that (i), (ii), and (iii) are equivalent. If there exist non-empty open subsets U_1 and U_2 that have an empty intersection, their union is a non-connected open subset. Conversely if U is a nonempty nonconnected subset we can write U as the disjoint union of two non-empty open subsets of U (and hence of X). This shows that (iv) and (i) are equivalent.

Obviously (v) implies (i). Let us show that (iii) implies (v). Let $U \subseteq X$ be open and non-empty, and V be an open subset of U. Then V is also open in X and therefore dense in X by (iii). But then V is certainly dense in U, so U is irreducible. □

Example 4.1.2. A Hausdorff space X is irreducible if and only if it consists of a single point.

A subset E of a topological space X is called an **irreducible** set if the subspace E of X is irreducible. For this to be so, it is necessary and sufficient that, for every pair of sets U, V

which are open in X and meet E, $U \cap V$ also meet E, or (what amounts to the same thing) that, for every pair of sets F, G which are closed in X and satisfy $E \subseteq F \cup G$, $E \subseteq F$ or $E \subseteq G$.

Proposition 4.1.3. *Let E be an irreducible set of X. If $(F_i)_{i \in I}$ is a finite family of closed sets of X such that $E \subseteq \bigcup_i F_i$, then there exists $i \in I$ such that $E \subseteq F_i$.*

Proof. This follows from the definition of irreducibility and induction on the cardinality of I. □

Proposition 4.1.4. *In a topological space X, for a set E to be irreducible, it is necessary and sufficient that its closure $\overline{E}$ be so.*

Proof. For an open set of X to meet E, it is necessary and sufficient that it meet E. Then the proposition follows from the above remarks. □

Proposition 4.1.5. *Let X be a topological space and let $(U_\alpha)_{\alpha \in A}$ be an open covering of X consists of irreducible open subsets such that $U_\alpha \cap U_\beta \neq \varnothing$ for $\alpha \neq \beta$. Then X is irreducible.*

Proof. Let us show that, for every non-empty open set V in X, $V \cap U_\alpha \neq \varnothing$ for all $\alpha \in A$; it then follows that $V \cap U_\alpha$ is dense in U_α by hypothesis, hence that V is dense in X and this proves that X is irreducible. Now there exists at least one index γ such that $V \cap U_\gamma \neq \varnothing$. As $U_\alpha \cap U_\gamma \neq \varnothing$ for all α and $V \cap U_\gamma$ is dense in U_γ, we see $V \cap U_\gamma \cap U_\alpha \neq \varnothing$ and a fortiori $V \cap U_\alpha \neq \varnothing$, which completes the proof of (b). □

Proposition 4.1.6. *Let X and Y be two topological spaces and $f : X \to Y$ a continuous map. For every irreducible subset E of X, $f(E)$ is an irreducible subset of Y.*

Proof. If U, V are two open sets of Y which meet $f(E)$, then $f^{-1}(U)$ and $f^{-1}(V)$ are open sets of X which meet E. Consequently, $f^{-1}(U) \cap f^{-1}(V) = f^{-1}(U \cap V)$ meets E, which implies that $U \cap V$ meets $f(E)$ and proves the proposition. □

Now let X be a topological space. Every maximal irreducible subset of a topological space X is called an **irreducible component** of X. It follows from Proposition 4.1.4 that every irreducible component of X is closed in X.

Proposition 4.1.7. *Let X be a topological space. Every irreducible subset of X is contained in an irreducible component of X and X is the union of its irreducible components.*

Proof. To prove the first assertion, it is sufficient, by virtue of Zorn's Lemma, to prove that the set $\mathcal{I}$ of irreducible subsets of X is inductive. Let $\mathcal{C}$ be a chain in $\mathcal{I}$. We show that the union E of the sets $F \in \mathcal{C}$ is irreducible. Let U, V be two open sets of X which meet E. As $\mathcal{C}$ is totally ordered, there exists a set $F \in \mathcal{I}$ meeting U and V. As F is irreducible, $U \cap V$ meets F and hence also E, which proves that E is irreducible and hence that $\mathcal{I}$ is inductive. The second assertion follows from the first, for every subset of X consisting of a single point is irreducible. □

Corollary 4.1.8. *Every connected component of a topological space X is a union of irreducible components of X.*

Proof. Every irreducible subspace of X is connected by Proposition 4.1.1 and hence is contained in a connected component of X. □

Proposition 4.1.9. *Let X be a topological space and $(Z_i)_{1\leq i\leq n}$ a finite closed covering of X consisting of irreducible sets. Then the irreducible components of X are the maximal elements (with respect to inclusion) of the set of Z_i.*

Proof. We may restrict ourselves to the case where no two Z_i are comparable. If E is an irreducible subset of X, then $E \subseteq \bigcup_i Z_i$, and hence E is contained in one of the closed sets Z_i (Proposition 4.1.3). This proves that the Z_i are the only maximal irreducible subsets of X. □

Corollary 4.1.10. *Let X be a topological space and E a subspace with only a finite number of distinct irreducible components $Q_1, \ldots, Q_n$. Then the irreducible components of the closure E in X are the closures $\overline{Q}_i$ of the Q_i and $\overline{Q}_i \neq \overline{Q}_j$ when $i \neq j$.*

Proof. The space $\overline{E}$ is the union of the $\overline{Q}_i$ which are irreducible (Proposition 4.1.4). As Q_i is closed in E, $\overline{Q}_i \cap E = Q_i$. As $Q_i \neq Q_j$, we see $\overline{Q}_i \neq \overline{Q}_j$ when $i \neq j$, whence the corollary by virtue of Proposition 4.1.9. □

Example 4.1.11. Suppose that X has only a finite number of distinct irreducible components $X_1, \ldots, X_n$. Then $U_i = (\bigcup_{j\neq i} X_j)^c$ is open in X and dense in X_i (since $X_i \not\subseteq \bigcup_{j\neq i} X_j$). The U_i are therefore non-empty open sets of X which are irreducible by Proposition 4.1.4, pairwise disjoint and with their union dense in X.

Proposition 4.1.12. *Let X be a topological space with finitely irreducible components $(X_i)_{1\leq i\leq r}$. Then any open dense subset U of X intersects each X_i.*

Proof. If $U \cap X_i = \varnothing$, then the open subset $X - \bigcup_{j\neq i} X_i$ of X is disjoint from U, contradicting to the fact that U is dense in X. □

Proposition 4.1.13. *Let U be an open subset of a topological space X. Then the map $C \mapsto \overline{C}$ (closure in X) gives a bijection between the set of irreducible closed subsets of U and the set of irreducible closed subsets of X meeting U, whose inverse is given by $Z \mapsto Z \cap U$. In particular, this bijection maps the set of irreducible components of U onto the set of irreducible components of X which meet U.*

Proof. If C is closed in U and irreducible, then $\overline{C}$ is irreducible and $C = \overline{V} \cap U$. Conversely, if Z is irreducible and closed in X and meets U, then $Z \cap U$ is a non-empty open subset of Z, hence irreducible and dense in Z and, as Z is closed, $Z = \overline{Z \cap U}$. This proves the proposition. □

4.1.2 Noetherian topological spaces

Definition 4.1.14. *A topological space is called **Noetherian** if the descending chain condition holds for closed subsets of X. A topological space is called **locally Noetherian** if every point has a neighbourhood which is Noetherian.*

Clearly, X is noetherian if and only if every non-empty set of closed subsets of X has a minimal element, if and only if every non-empty set of open subsets of X has a maximal element, or that every decreasing (resp. increasing) sequence of closed (resp. open) sets is stationary.

Proposition 4.1.15. *Any subspace of a Noetherian space is Noetherian. Let $(A_i)_{i\in I}$ be a finite covering of a topological space X. If the subspaces A_i of X are Noetherian, then X is Noetherian.*

Proof. Let X be a Noetherian space, A a subspace of X and (F_n) a decreasing sequence of subsets of A which are closed in A. Then $F_n = \overline{F}_n \cap A$ and the closures $\overline{F}_n$ of the F_n in X form a decreasing sequence of closed subsets of X. As this sequence is stationary, so is the sequence (F_n).

For (b), let (F_n) be a decreasing sequence of closed subsets of X. By hypothesis, each of the sequences $(E_n \cap A_i)_n$ is stationary. As I is finite, there is an integer n_0 such that, for $n \geq n_0$, $E_n \cap A_i = E_{n_0} \cap A_i$ for all $i \in I$. But

$$E_n = \bigcup_{i \in I} E_n \cap A_i$$

and hence the sequence (E_n) is stationary and X is Noetherian. □

Proposition 4.1.16. *For a topological space X to be Noetherian, it is necessary and sufficient that every open set in X be quasi-compact.*

Proof. To show the necessarity, it is sufficient, by virtue of Proposition 4.1.15, to prove that every Noetherian space X is quasi-compact. Let $(U_\alpha)_{\alpha \in A}$ be an open covering of X. The set of finite unions of sets U, is non-empty and hence admits a maximal element $V = \bigcup_{i \in H} U_i$ where H is a finite subset of I. By definition, $V \cup U_i = V$ for all $i \in I$ and hence $V = X$.

Conversely, suppose that every open set of X is quasi-compact and let (U_n) be an increasing sequence of open subsets of X. The union V of the U_n is open and hence quasi-compact. As (U_n) is an open covering of V, there is a finite subfamily of (U_n) which is a covering of V and hence $V = U_n$ for some index n, which proves that the sequence (U_n) is stationary. □

Lemma 4.1.17 (Principle of Noetherian Induction). *Let E be an ordered set such that any nonempty subset of E contains a minimal element. Let F be a subset of E with the following property: if $a \in E$ is such that the relation $x < a$ implies $x \in F$, then $a \in F$. Then $E = F$.*

Proof. Suppose $F \neq E$, then $E \setminus F$ would have a minimal element b. By definition, $x \in F$ for all $x < b$, which implies that $b \in F$, a contradiction. □

Proposition 4.1.18. *If X is a Noetherian space, the set of irreducible components of X (and a fortiori the set of connected components of X) is finite.*

Proof. It is sufficient to prove that X is a finite union of irreducible closed subsets (Corollary 4.1.10). Let us show that the principle of Noetherian induction can be applied taking E to be the set of closed subsets of X, ordered by inclusion, and F to be the set of finite unions of irreducible closed subsets. Let Y be a closed subset Of X such that every peroper closed subset of Y belongs to F. If Y is irreducible, then $Y \in F$ by definition. Otherwise, Y is the union of two closed subsets Y_1, Y_2 which are distinct from Y. Then $Y_1 \in F$ and $Y_2 \in F$ by hypothesis, whence $Y \in F$ by definition of F. □

Proposition 4.1.19. *Suppose X is a Noetherian topological space. Then every nonempty closed subset E can be expressed uniquely as a finite union $E = Z_1 \cup \cdots \cup Z_n$ of irreducible closed subsets, none contained in any other.*

Proof. Just take the irreducible component of E. □

Proposition 4.1.20. *Let $f : X \longrightarrow Y$ be a continuous map of topological spaces.*

(a) If X is Noetherian, then $f(X)$ is Noetherian

(b) If X is locally Noetherian and f is open, then $f(X)$ is locally Noetherian.

Proof. For (a), suppose that $(Z_i)_i$ is a descending chain of closed subsets of $f(X)$. Then $(f^{-1}(Z_i))_i$ is a descending chain of closed subsets of X. Hence this chain stabilizes. Since $f(f^{-1}(Z_i)) = Z_i$ we conclude that $(Z_i)_i$ also stabilizes. In case (b), let $y \in f(X)$. Choose $x \in X$ with $f(x) = y$. By assumption there exists a neighbourhood $E \subseteq X$ of x which is Noetherian. Then $f(E) \subseteq f(X)$ is a neighbourhood which is Noetherian by part (a). □

Proposition 4.1.21. *Let X be a locally Noetherian topological space. Then X is locally connected.*

Proof. Let $x \in X$ and V be a neighbourhood of x. We have to find a connected neighbourhood of x contained in V. By assumption there exists a neighbourhood U of x which is Noetherian. Then $U \cap V$ is Noetherian. Let $U \cap V = Z_1 \cup \cdots \cup Z_n$ be the decomposition into irreducible components, then $W = \bigcup_{x \in Z_i} Z_i$ is a connected subset of $U \cap V$ containing x (since each Z_i is connected). □

Proposition 4.1.22. *Let X be a locally Noetherian space, then the following are equivalent:*

(i) The irreducible components of X are open.

(ii) The irreducible components coincide with the connected components.

(iii) The connected components of X are irreducible.

(iv) The irreducible components of X are disjoint.

Proof. Since the irreducible components of X are closed and connected, clearly (i) implies (ii) and (ii) implies (iii). If (iii) holds, then the connected components are exactly the irreducible component since they are open and closed and disjoint. Thus (iii) implies (ii) and (iv).

Finally, we prove that (iv) implies (i). Let Z be an irreducible component of X and $x \in Z$ be arbitrary point. Choose a noetherian neirhborhood U of x. It is easy to see that the irreducible components of U are exactly the intersection of that of X with U. Since U is noetherian, there are finitely many such irreducible components: say $Z = Z_1, \ldots, Z_n$. Then since $Z_i \cap U$ are closed and disjoint, they are also open in U, hence in X. In particular, this means Z has an open neighborhood of x, which means it is open. □

4.1.3 Generic points

4.2 Krull dimension

4.2.1 Krull dimension of a topological space

Definition 4.2.1. *Let I be an ordered set. A non-empty and totally ordered finite subset of I is called a* ***chain*** *of I. Let C be a chain of I, the smallest and the most large element of C are called the* ***ends*** *of C. The integer $|C| - 1$ is called the* ***length*** *of C. The relation of inclusion in the set of subsets of I induces a order relation in the set of chains of I. A chain C of I is said to be* ***saturated*** *if it is maximal among the chains of I having the same endpoints as C.*

Let X be a topological space. We endow the set of irreducible closed subsets of X of the order relation defined by the inclusion. When we talk about a chain of closed irreducible subsets of X, it will always be a chain in the sense of this order relation.

Definition 4.2.2. *Let X be a topological space. The **dimension** or more precisely the **Krull dimension** of X, denoted by $\dim(X)$, is defined to be the supremum of chains of irreducible closed subsets of X. We set $\dim(X) = -\infty$ when X is the empty space. Let $x \in X$, the **Krull dimension of X at x**, denoted by $\dim_x(X)$, is defined to be the infimum of the dimensions of the open neighborhoods of x.*

Note that if X is Hausdorff then any irreducible closed subset of X reduces to a point. The definition of the Krull dimension is therefore devoid of interest for Hausdorff spaces, but it is specially adapted to the topological spaces encountered in commutative algebra. In this part, no confusion is to be feared with other notions of dimension of topological spaces, and we will simply say "dimension" for "Krul dimension".

Proposition 4.2.3. *Let X be a topological space.*

(a) Let Y be a subspace of X, then $\dim(Y) \leq \dim(X)$ and $\dim_y(Y) \leq \dim_y(X)$ for any point y of Y.

(b) Let x be a point of X and U a neighborhod of x. Then $\dim_x(X) = \dim_x(U)$.

Proof. Let Y be a subspace of X. If Z is an irreducible closed subset of Y, its closure $\overline{Z}$ in X is irreducible and $\overline{Z} \cap Y = Z$. Thus, any chain of irreducible closed subsets of Y defines, by passage to closure in X, a chain of irreducible closed subsets of X of the same length. This implies $\dim(Y) \leq \dim(X)$. If U is an open subset of X containing a point y of Y, we therefore have $\dim(U \cap Y) \leq \dim(U)$, whence $\dim_y(Y) \leq \dim_y(X)$. Now part (b) follows from (a). □

Proposition 4.2.4. *Let X be a topological space. Then $\dim(X) = \sup_{x \in X} \dim_x(X)$.*

Proof. First we have $\dim_x(X) \leq \dim(X)$ by Proposition 4.2.3(a). On the other hand, if $Z_0 \subset \cdots \subset Z_n$ is a chain of irreducible closed subsets and U a neighborhood of x_0 in X, where $x_0 \in Z_0$, then $Z_0 \cap U \subset \cdots \subset Z_n \cap U$ is a chain of irreducible closed subsets of U (Proposition 4.1.1). This shows $\dim_x(X) \geq n$, whence $\dim(X) \leq \sup_{x \in X} \dim_x(X)$. □

Corollary 4.2.5. *Let $(X_i)_{i \in I}$ be an open cover (or a locally finite closed cover) of a topological space X. Then*

$$\dim(X) = \sup_{i \in I} \dim(X_i), \quad \dim_x(X) = \sup_{i \in I_x} \dim_x(X_i)$$

where I_x is the set $i \in I$ such that $x \in U_i$.

Proof. The claim is immediate when (X_i) is an open cover, and we now deal with the case of a locally finite closed cover. First suppose that I is finite. Let $Z_0 \subset \cdots \subset Z_n$ be a chain of irreducible closed subsets of X. Then $Z_n = \bigcup_i Z_n \cap X_i$, and each $Z_n \cap X_i$ is closed in Z_n. Since I is finite, we see Z_n is contained in one of the X_i, whence $\dim(X) \leq \sup_i \dim(U_i)$, and the converse inequality follows from Proposition 4.2.3.

Now let $x \in X$ and for each $i \in I_x$ let U_i be a neighborhod of x such that $\dim(U_i \cap X_i) \leq n$, where $n = \sup_{i \in I_x} \dim_x(X_i)$, and let

$$U = \Big(\bigcap_{i \in I_x} U_i\Big) \cap \Big(\bigcap_{i \in I - I_x} X_i^c\Big).$$

Then U is open in X since I_x is finite, and since $(U \cap X_i)_{i \in I_x}$ is a finite closed cover of U, by the preceding argument we have

$$\dim(U) = \sup_{i \in I_x} \dim(U \cap X_i) \leq \sup_{i \in I_x} \dim(U_i \cap X_i) \leq n$$

whence $\dim_x(X) \leq n$ and the proof is finished in this case. The general case then follows from Proposition 4.2.4. □

Proposition 4.2.6. *Let $\mathcal{I}$ be the set of irreducible components of X. Then*

$$\dim(X) = \sup_{Y \in \mathcal{I}} \dim(Y).$$

Proof. It is clear that $\sup_{Y \in \mathcal{I}} \dim(Y) \leq \dim(X)$ according to Proposition 4.2.3. Now let $Z_0 \subset \cdots \subset Z_n$ be a chain of irreducible closed subsets in X. Then Z_n is contained in a irreducible component Y of X, and therefore $Z_0 \subset \cdots \subset Z_n$ is a chain of irreducible closed subsets in Y (since Y is closed), and we obtain $n \leq \sup_{Y \in \mathcal{I}} \dim(Y)$, whence the claim. □

Proposition 4.2.7. *Let X be an irreducible topological space and Y a proper closed subset of X. Then* $\dim(Y) < \dim(X)$.

Proof. Since X is irreducible and closed, any chain $Z_0 \subset \cdots \subset Z_n$ of irreducible closed subsets of Y can be extended by adding X at the end, whence $\dim(Y) \leq \dim(X) + 1$. □

Corollary 4.2.8. *If Y is a closed subset of an irreducible finite-dimensional topological space X, and if* $\dim Y = \dim X$, *then $Y = X$.*

4.2.2 Codimension of a closed subset

Let X be a topological space. For an irreducible closed subset Z of X, the **codimension** of Z in X is defined to be the supremum of the lengths of the chains of closed irreducible subsets of X containing Z. If Y is a closed subset of X, the **codimension** of Y in X is defined to be the infimum of the codimensions in X of the irreducible of components Y.

The codimension of a closed subset Y of X is therefore the infimum of the codimensions of the irreducible closed subsets of Y. We have $\operatorname{codim}(\varnothing, X) = +\infty$ and, if X is not empty, $\operatorname{codim}(X, X) = 0$. Since any nonempty closed subset of X contains an irreducible closed subset (for example the closure of a singleton), the codimension in X of a closed subset Y is always a positive integer or $+\infty$. It is zero if and only if Y contains an irreducible component of X. Note that by definition $\operatorname{codim}(Y, X) \leq \dim(X)$, and $\dim(X) = \sup_Y \operatorname{codim}(Y, X)$ where Y runs through all irreducible closed subsets of X. Also, if $Y' \subseteq Y$ are closed subsets of X, we have $\operatorname{codim}(Y, X) \leq \operatorname{codim}(Y, X)$.

Let Y be a closed subset of X and $(X_\alpha)_{\alpha \in A}$ (resp. $(Y_\beta)_{\beta \in B}$) be the family of irreducible components of X (resp. of Y). For each $\beta \in B$, let A_β be the subset $\alpha \in A$ such that $Y_\beta \subseteq X_\alpha$. Then since each irreducible closed subset of X is contained in one of X_α, it follows from definition that

$$\operatorname{codim}(Y, X) = \inf_{\beta \in B} \sup_{\alpha \in A_\beta} \operatorname{codim}(Y_\beta, X_\alpha).$$

In particular, if $(Y_i)_{i\in I}$ is a finite family of closed subsets of X and $Y = \bigcup_i Y_i$, then

$$\operatorname{codim}(Y, X) = \inf_{i\in I} \operatorname{codim}(Y_i, X)$$

since by Proposition 4.1.3 any irreducible component of Y is contained in one of the Y_i.

Proposition 4.2.9. *Let X be a topological space.*

(a) For any closed subset Y of X, we have

$$\dim(Y) + \operatorname{codim}(Y, X) \leq \dim(X).$$

(b) If $Y \subseteq Z \subseteq T$ are closed subsets of X, then

$$\operatorname{codim}(Y, Z) + \operatorname{codim}(Z, T) \leq \operatorname{codim}(Y, T).$$

Proof. To prove (a), we may assume that $\dim(X)$ is finite, whence $\dim(Y)$ and $\operatorname{codim}(Y, X)$ are both finite. If $Z_0 \subset \cdots \subset Z_n$ is a chain of irreducible closed subsets of Y such that $n = \dim(Y)$ and $Z_n \subset \cdots \subset Z_{n+p}$ is a chain of that of X such that $p \geq \operatorname{codim}(Y, X)$, then we get a chain $Z_0 \subset \cdots \subset Z_{n+p}$ in X, whence $\dim(X) \geq n + p$ and part (a) follows.

To prove (b), we may assume that Y is irreducible. Since $\operatorname{codim}(Y, Z) \leq \operatorname{codim}(Y, T)$, the claim is true if $\operatorname{codim}(Y, Z) = +\infty$. Otherwise, let Z_0 be an irreducible component of Z containing Y such that $\operatorname{codim}(Y, Z) = \operatorname{codim}(Y, Z_0)$. We have $\operatorname{codim}(Z, T) \leq \operatorname{codim}(Z_0, T)$, and we see, as the proof of (a), that $\operatorname{codim}(Y, Z_0) + \operatorname{codim}(Z_0, T) \leq \operatorname{codim}(Y, T)$, whence (b). □

Definition 4.2.10. *A topological space X is called **catenary** if for any pair (Y, Z) of irreducible closed subsets of X such that $Y \subseteq Z$, any saturated chain of subsets irreducible closed lines with ends Y and Z is of length* $\operatorname{codim}(Y, Z)$.

It amounts to the same thing to say that, for any pair (Y, Z) of closed irreducible subsets of X such that $\operatorname{codim}(Y, Z)$ is finite, all the saturated chains with ends Y and Z have the same length, and that, for any couple (Y, Z) such that $\operatorname{codim}(Y, Z) = +\infty$, there is no saturated chain with Y and Z ends.

Any closed subspace of a catenary space is catenary. For a space is catenary, it is necessary and sufficient that its irreducible components are catenary.

Proposition 4.2.11. *Let X be a topological space. For X be catenary, it is necessary and sufficient that, for every triple (Y, Z, T) of irreducible closed subsets of X such that $Y \subseteq Z \subseteq T$, we have*

$$\operatorname{codim}(Y, T) = \operatorname{codim}(Y, Z) + \operatorname{codim}(Z, T). \tag{2.2.1}$$

Proof. Suppose X is catenary. Concerning Proposition 4.2.9, it suffices to prove (2.2.1) when $\operatorname{codim}(Y, Z)$ and $\operatorname{codim}(Z, T)$ are finite. By putting end to end a saturated chain of irreducible closed subsets with endpoints Y and Z of length $\operatorname{codim}(Y, Z)$ and a saturated chain of irreducible closed subsets with end points Z and T of length $\operatorname{codim}(Z, T)$, we obtain a saturated chain with ends Y and T, of length $\operatorname{codim}(Y, Z) + \operatorname{codim}(Z, T)$. As X is catenary, this length is necessarily equal to $\operatorname{codim}(Y, T)$.

Conversely, suppose that (2.2.1) holds for every triple (Y, Z, T) of irreducible closed subset of X such that $Y \subseteq Z \subseteq T$, and we show that X is catenary. For this, we prove by induction that for every saturated chain $Z_0 \subset \cdots \subset Z_n$ we have $\operatorname{codim}(Z_0, Z_n) = n$. For $n = 0$ this is clear. Let $n > 0$, and suppose the property satisfied for chains of length smaller than $n - 1$. If $Z_0 \subset \cdots \subset Z_n$ is a maximal of length n, then $Z_0 \subseteq \cdots \subseteq Z_{n-1}$ is a saturated chain of length $n - 1$, so $\operatorname{codim}(Z_0, Z_{n-1}) = n - 1$. Given the assumption made on X, we have $\operatorname{codim}(Z_0, Z_n) = \operatorname{codim}(Z_0, Z_{n-1}) + \operatorname{codim}(Z_{n-1}, Z_n) = (n - 1) + 1 = n$. □

Corollary 4.2.12. *Let X be an irreducible topological space of finite dimension. For X to be catenary, it is necessary and sufficient that, for every pair (Y, Z) of irreducible closed subsets of X such that $Y \subseteq Z$, we have*

$$\operatorname{codim}(Y, Z) + \operatorname{codim}(Z, X) = \operatorname{codim}(Y, X).$$

Proof. The condition is necessary by Proposition 4.2.11. Conversely, suppose it is ture, and for each irreducible closed subset Z of X define $c(Z) = \operatorname{codim}(Z, X)$. Then for a triple triple (Y, Z, T) of irreducible closed subsets of X such that $Y \subseteq Z \subseteq T$,

$$\operatorname{codim}(Y, Z) + \operatorname{codim}(Z, T) = c(Y) - c(Z) + c(Z) - c(T) = c(Y) - c(T) = \operatorname{codim}(Y, T)$$

whence X is catenary by Proposition 4.2.11. □

Proposition 4.2.13. *Let X be a topological space of finite dimension. Suppose that all maximal chains of closed irreducible subsets of X have the same length. Then X is catenary, and for any irreducible closed subset Z of X, we have*

$$\operatorname{codim}(Z, X) = \dim(X) - \dim(Z).$$

Moreover, for any pair (Y, Z) of irreducible closed subsets of X such that $Y \subseteq Z$, we have

$$\operatorname{codim}(Y, Z) = \dim(Z) - \dim(Y).$$

Proof. Let Y and Z be irreducible closed subsets of X such that $Y \subseteq Z$. Let $Y_0 \subset \cdots \subset Y_p$ be a chain such that $Y_p = Y$ and $p = \dim(Y)$, $Z_0 \subset \cdots \subset Z_q$ a chain such that $Z_0 = Z$ and $q = \operatorname{codim}(Z, X)$. Then for any saturated chain $T_0 \subset \cdots \subset T_r$ with $T_0 = Y$, $T_r = Z$, the chain

$$Y_0 \subset \cdots \subset Y_{p-1} \subseteq T_0 \subset \cdots \subset T_r \subseteq Z_1 \subset \cdots \subset Z_q$$

is maximal with length $p + q + r$. The hypotheses on X then implies $p + q + r = \dim(X)$, whence $r = \dim(X) - \dim(Y) - \operatorname{codim}(Z, X)$. It follows that X is catenary and that, for Y and Z as above, we have

$$\dim(Y) + \operatorname{codim}(Y, Z) = \dim(X) - \operatorname{codim}(Z, X).$$

Put $Z = Y$, we see the second number is equal to $\dim(Z)$, whence the proposition. □

Chapter 5

Integral domains

5.1 Prime and irreducible elements

Two elements $a, b \in R$ are associates if and only if $(a) = (b)$,

Lemma 5.1.1. *Let a, b be nonzero elements of an integral domain R. Then a and b are associates if and only if $a = ub$, for u a unit in R.*

Proof. Assume a and b are associates. Then there are $u, v \in R$ such that

$$a = ub, \quad b = va.$$

Therfore $a = uva$, which means $uv = 1$, u is a unit. The converse is clear. □

Definition 5.1.2. *Let R an itegral domain and $a \in R$.*

- *a is **prime** if the ideal (a) is prime. That is, a is not a unit and*

$$a \mid bc \Rightarrow a \mid b \text{ or } a \mid c.$$

- *a is **irreducible** if a is not a unit and*

$$a = bc \Rightarrow b \text{ is a unit or } c \text{ is a unit}.$$

Proposition 5.1.3. *A nonunit $a \in R$ is irreducible if and only if*

(i) If $a = bc$ for some $b, c \in R$ then a is an associate of b or c.

(ii) If $a = bc$ for some $b, c \in R$ then $(a) = (b)$ or $(a) = (c)$.

(iii) The ideal (a) is maximal among proper principal ideals.

Proof. One only need to note that $b \mid a$ if and only if $(a) \subseteq (b)$. □

Lemma 5.1.4. *Let R be an integral domain. Then every prime element is irreducible.*

Proof. Let a be a prime element in R and assume that $a = bc$ for some $b, c \in R$, then we have $bc \in (a)$. Since a is prime, we conclude $b \in (a)$ or $c \in (a)$, say $b \in (a)$. But then $(b) \subseteq (a) = (bc) \subseteq (b)$, whence $(a) = (b)$. This proves a is irreducible. □

Example 5.1.5. The converse is not true in general. As an example, consider the ring $\mathbb{Z}[\sqrt{5}i]$. The element 2 is irreducible. However, $2 \mid 6 = (1+\sqrt{5}i)(1-\sqrt{5}i)$, but 2 does not divide $1+\sqrt{5}i$ and 2 does not divide $1-\sqrt{5}$.

5.2 Domains with factorizations

Definition 5.2.1. *Let R be an integral domain. An element $r \in R$ has a* ***factorization into irreducibles*** *if there exist irreducible elements $q_1, \ldots, q_n$ such that $r = q_1 \cdots q_n$. This factorization is* ***unique*** *if the elements q_i are determined by r up to order and associates.*

Definition 5.2.2. *An integral domain R is a* ***domain with factorizations*** *if every nonzero, nonunit element $r \in R$ has a factorization into irreducibles. It is a* ***unique factorization domain*** *if every nonzero, nonunit element $r \in R$ has a unique factorization into irreducibles.*

Proposition 5.2.3. *Let R be an integral domain, and r nonzero and nonunit. Assume that every ascending chain of principal ideals*

$$(r) \subseteq (r_1) \subseteq (r_3) \subseteq \cdots$$

stabilizes. Then r has a factorization into irreducibles.

Proof. Assume that r does not have a factorization into irreducible elements. In particular, r is itself not irreducible; thus $r_1, s_1 \in R$ such that $r = r_1 s_1$ and $(r) \subset (r_1), (r) \subset (s_1)$. If both r_1, s_1 have factorizations into irreducibles, the product of these factorizations gives a factorization of r; thus we may assume that (e.g.) r_1 does not have a factorization into irreducibles. Therefore we have a chain

$$(r) \subset (r_1) \subset (r_3) \subset \cdots$$

contradicting our hypothesis. □

Corollary 5.2.4. *Factorizations exist in Noetherian domains.*

Example 5.2.5. $\mathbb{Z}[X_1, X_2, \cdots]$ is not a Noetherian domain, but a.c.c holds for principle ideals in it, so it has factorizations.

Now we give a sufficient and necessary condition for a domain to be a UFD. First we prove some preparations.

Lemma 5.2.6. *Let R be a UFD, and let a, b, c be nonzero elements of R. Then*

(i) $(a) \subseteq (b)$ iff the multiset of irreducible factors of b is contained in the multiset of irreducible factors of a.

(ii) a and b are associates iff the two multisets coincide.

(iii) the irreducible factors of a product bc are the collection of all irreducible factors of b and of c.

Proposition 5.2.7. *In a domain in which factorization into irreducibles is possible, factorization is unique if and only if every irreducible is prime.*

Proof. Let's assume that we have two different decompositions

$$p_1 \cdots p_n = q_1 \cdots q_m$$

where all p_i and q_j are irreducible. Then $p_1 \cdots p_n \in (q_1)$, and (q_1) is a prime ideal (by hypothesis); thus $p_i \in (q_1)$ for some i, which we may assume to be 1 after changing the order of the factors. Therefore $p_1 = uq_1$ for some $u \in R$. Since p_1 is irreducible and q_1 is not a unit, necessarily u is a unit. Thus p_1 and q_1 are associates. Canceling p_1, q_1 and replacing p_2 by up_2, we find

$$p_2 \cdots p_n = q_2 \cdots q_m.$$

Repeating this process matches all factors one by one. It is clear that $m = n$, because otherwise we will obtain $1 =$ a product of irreducibles, contradicting the fact that irreducibles are not units.

Conversely, assume that factorization in R is unique, so that R is a UFD. Let $a \in R$ be irreducible. Then a is not a unit, by definition of irreducible. Assume $bc \in (a)$: thus $(bc) \subseteq (a)$, and the irreducible factors of a, that is, a itself, must be among the factors of b or of c. We have $b \in (a)$ in the first case and $c \in (a)$ in the second. This shows that (a) is a prime ideal, as needed. □

Theorem 5.2.8. *An integral domain R is a UFD if and only if*

- *The a.c.c. for principal ideals holds in R.*
- *Every irreducible element of R is prime.*

Proof. If these conditions are satisfied, then by Proposition 5.2.3 and Proposition 5.2.7 we know that R is a UFD. Conversely, if F is a UFD, then Proposition 5.2.7 shows that irreducible elements of R are prime. To prove that the a.c.c. for principal ideals holds, consider an ascending chain

$$(r_1) \subset (r_2) \subset (r_3) \subset \cdots$$

By lemma 5.2.6 this chain determines a corresponding descending chain of irreducible factors. A descending chain of finite multisets clearly stabilizes, and it follows that the original chain also stabilizes. □

5.3 Greatest common divisors and Bézout domains

Our next step is going to be: how do we prove that prime and irreducible are the same thing in a particular domain? The answer will be that if have GCDs and they behave well, then we can prove it. We are going to need to start by defining what a gcd is in general.

Definition 5.3.1. *Let $a, b \in R$. We say that $d \in R$ is a* ***greatest common divisor*** *of a and b if*

(1) *$d \mid a$ and $d \mid b$,*

(2) *If $c \in R$ is another element such that $c \mid a$ and $c \mid b$, then $c \mid d$.*

The following result is clear.

Lemma 5.3.2. *Let $a, b \in R$. Let $d \in R$.*

(1) *d is a common divisor of a and b iff $(a, b) \subseteq (d)$.*

(2) *d is a gcd of a and b iff (d) is a minimal element in the poset of principal ideals that contain (a, b) with respect to inclusion.*

Notice that based on the definition, the two elements a and b may in principle have one gcd, or various gcds, or none. It can be easily showed that if d' is another gcd of a, b, then d associates with d'. Thus in fact we define the gcd to be an associate class.

Lemma 5.3.3. *Let R be an integral domain. Let $a, b, c \in R - \{0\}$, then*

(1) $\gcd(a, b) = a$ *iff* $a \mid b$.

(2) $c \gcd(a, b) = \gcd(ca, cb)$.

(3) *If* $\gcd(ab, c) = 1$, *then* $\gcd(a, c) = \gcd(b, c) = 1$.

(4) *If* $\gcd(a, b) = 1$ *and* $\gcd(a, c) = 1$, *then* $(a, bc) = 1$.

(5) *If* $\gcd(a, b) = 1$ *and* $a \mid bc$, *then* $a \mid c$.

Proof. (1) One direction is obvious from the definition. So suppose $a \mid b$. Then since $a \mid a$, we have $a \mid \gcd(a, b)$. But $\gcd(a, b) \mid a$, thus $\gcd(a, b) = a$.

(2) Let $d_1 = \gcd(a, b)$ and $d_2 = \gcd(ca, cb)$. Then from $cd_1 \mid ca$ and $cd_1 \mid cb$ we conclude that $cd_1 \mid d_2$. Therefore

$$ca = x \cdot d_2 = x \cdot ucd_1,$$
$$cb = y \cdot d_2 = y \cdot ucd_1.$$

These then implies $ud_1 \mid a$, $ud_1 \mid b$, and therefore $ud \mid d$, so u is a unit.

(3) This follows from $(ab, c) \subseteq (a, c)$ and $(ab, c) \subseteq (b, c)$.

(4) Suppose that $d \mid a$ and $d \mid bc$. Then $d \mid ab$ and $d \mid bc$ and therefore $d \mid \gcd(ab, bc) = b \gcd(a, c) = b$. Since $\gcd(a, b) = 1$, we conclude that d is a unit.

(5) Now $a \mid bc$ and $a \mid ac$, thus $a \mid \gcd(ac, bc) = c \gcd(a, b) = c$. □

Definition 5.3.4. *Let R be an integral domain. Consider the following two properties:*

(1) *Given any non-zero elements $ab \in R$, there exists a gcd d of a and b.*

(2) *Moreover, d can be written as $d = xa + yb$ for some $x, y \in R$.*

We say that R is a ***GCD-domain*** *when it satisfies the first property. We say that R is a* ***Bézout domain*** *when it satisfies both properties.*

Proposition 5.3.5. *Let R be an integral domain. The the following conditions are equivalent:*

(1) *R is Bezout.*

(2) *For $a, b \in R$, the ideal (a, b) is principal.*

(3) *Every finitely generated ideal in R is principal.*

Proof. Clearly, if R is Bezout, then (2) holds. Also, an inductive argument implies that (2) and (3) are equivalent. Now assume (2), and let a, b be elements in R. Then since (a, b) is principal, by Lemma 5.3.2 we know that $\gcd(a, b)$ exists, and is a linear conbination of a, b. Thus R is Bezout. □

Proposition 5.3.6. *Every UFD is a GCD-domain.*

Proof. Let $a, b \in R$, we can write

$$a = uq_1^{\alpha_1} \cdots q_r^{\alpha_r}, \quad b = vq_1^{\beta_1} \cdots q_r^{\beta_r}$$

where u and v are units, the elements q_i are irreducible, q_i is not an associate of q_j for $i \neq j$, and $\alpha_i, \beta_i \geq 0$. We claim that

$$d = q_1^{\min(\alpha_1,\beta_1)} \cdots q_r^{\min(\alpha_r,\beta_r)}$$

is a gcd of a and b. Indeed, d is clearly a divisor of a and b; and if c also divides a and b, then the multiset of factors of c must be contained in both multisets of factors for a and b by Lemma 5.2.6; that is,

$$c = wq_1^{\gamma_1} \cdots q_r^{\gamma_r}.$$

with w a unit and $\gamma_i \leq \alpha_i, \beta_i$. This implies $c \mid d$ again by Lemma 5.2.6, as needed. □

Proposition 5.3.7. *Let R be a GCD domain. Then being prime is the same as being irreducible in R.*

Proof. We already know that every prime is irreducible in every domain. Let $p \in R$. Assume that p is irreducible and that $p \mid ab$ with $a, b \in R$. Let $d = \gcd(p, a)$. Since $d \mid p$, d must be either a unit or associate to p.

If d is associate to p, we have that $p \mid d$ and $d \mid a$, so that $p \mid a$ and we are done. If d is a unit, then we have

$$\gcd(p, a) = 1 \quad \text{and} \quad p \mid ab.$$

Thus by Lemma 5.3.3 we conclude $p \mid b$. □

Theorem 5.3.8. *An integral domain R is a UFD if and only if*

- *R is a GCD domain.*
- *The a.c.c. for principal ideals holds in R.*

Proof. By Proposition 5.3.7 and Theorem 5.2.8, the given conditions imply that R is a UFD. Conversely, if R is a UFD, then by Proposition 5.3.6 and Theorem 5.2.8, the conditions are satisfied. □

Theorem 5.3.9. *If R is a PID, then R is a Bézout domain and a UFD.*

Proof. Let $a, b \in R$, Then the ideal (a, b) is principal. Write $(a, b) = (d)$, then by Lemma 5.3.2 d is a gcd of a and b. Moreover, d is a linear combination of a and b. Thus R is a Bézout domain. Since R is Noetherian, R is a UFD by Theorem 5.3.8. □

5.4 Unique factorization in polynomial rings

Lemma 5.4.1. *Let R be a ring, and let I be an ideal of R. Then*

$$\frac{R[X]}{IR[X]} = \frac{R}{I}[X].$$

Therefore, if I is a prime ideal of R, then $IR[X]$ is prime in $R[X]$.

Definition 5.4.2. *Let R be a commutative ring, and let $f = \sum_{i=1}^{n} a_i X^i \in R[X]$ be a polynomial.*

- *f is **very primitive** if for all prime ideals $\mathfrak{p}$ of R, $f \notin \mathfrak{p}R[X]$.*
- *f is **primitive** if for all principal prime ideals $\mathfrak{p}$ of R, $f \notin \mathfrak{p}R[X]$.*

Lemma 5.4.3. *Let R be a commutative ring and $f \in R[X]$ as above.*

- *f is very primitive if and only if $(a_0, \dots, a_n) = 1$.*
- *If R is a UFD, then f is primitive if and only if $\gcd(a_0, \dots, a_n) = 1$.*

Proof. That f is very primitive means the coefficients of f are not all contained in any one prime ideal, thus is equivalent to $(a_0, \dots, a_n) = 1$.

For the second point note that, in a UFD, $\gcd(a_0, \dots, a_n) \neq 1$ if and only if there exists an irreducible element $q \in R$ such that $(a_0, \dots, a_n) \subseteq (q)$. As (q) is then prime, the second point follows as well. □

Lemma 5.4.4. *Let R be a commutative ring. Then for $f, g \in R[X]$,*

$$fg \text{ is primitive} \iff \text{both } f \text{ and } g \text{ are primitive}.$$

Proof. This is an easy consequence of Lemma 5.4.1:

$$\begin{aligned} fg \text{ is primitive} &\iff \forall \mathfrak{p} \text{ prime and principal in } R, fg \notin \mathfrak{p}R[X] \\ &\iff \forall \mathfrak{p} \text{ prime and principal in } R, f \notin \mathfrak{p}R[X] \text{ and } g \notin \mathfrak{p}R[X] \\ &\iff f \text{ is primitive and } g \text{ is primitive.} \end{aligned}$$

Thus the claim follows. □

Definition 5.4.5. *Let R be a UFD. The **content** of a nonzero polynomial $f \in R[X]$, denoted cont_f, is the* gcd *of its coefficients.*

The proof of the following remarks is immediate from the definition.

Lemma 5.4.6. *Let R be a UFD, and let $f \in R[X]$. Then*

- *$(f) = (\mathrm{cont}_f)(f_1)$ where f_1 is primitive.*
- *if $(f) = (c)(g)$, with $c \in R$ and g primitive, then $(c) = (\mathrm{cont}_f)$.*

Now we prove a useful result about primitive polynomials.

Proposition 5.4.7 (Gauss's lemma). *Let R be a UFD, and let $f, g \in R[X]$. Then*

$$(\mathrm{cont}_{fg}) = (\mathrm{cont}_f)(\mathrm{cont}_g).$$

Proof. This follows easily from our preparatory work. Write

$$(fg) = (\mathrm{cont}_f)(f_1)(\mathrm{cont}_g)(g_1) = (\mathrm{cont}_f)(\mathrm{cont}_g)(f_1 g_1)$$

with f_1, g_1 primitive. By Lemma 5.4.4 $f_1 g_1$ is primitive, thus $(\mathrm{cont}_f)(\mathrm{cont}_g)$ is the content of fg, as needed. □

Now we consider the field of fractions of R. We first prove some consequences of Gauss's lemma.

Proposition 5.4.8. *Let R be a UFD and $f \in R[X]$. Suppose that $f = gh$ where $g, h \in K[X]$. Then there exists $\lambda \in K^\times$ such that $\lambda g, \lambda^{-1} h \in R[X]$.*

Proof. Let $c, d \in K$ be such that

$$g = c g_1, \quad h = d h_1,$$

where $g_1, h_1 \in R[X]$ are primitive. Then $g_1 h_1$ is also primitive and from $c d g_1 h_1 \in R[X]$ we conclude that $u := cd \in R$. Set $\lambda = d$, we then get $\lambda g = c d g_1 \in R[X]$ and $\lambda^{-1} h = h_1 \in R[X]$. □

This result is also called Guass's lemma, and is used for example in algebraic number theory (the case $R = \mathbb{Z}$ and $K = \mathbb{Q}$).

Corollary 5.4.9. *Let R be an UFD with fraction field K. Let $f \in R[X]$ be a monic polynomial and suppose that f factors in $K[X]$ as gh with g and h monic. Then g and h have coefficients in R.*

Proof. By Proposition 5.4.8 there exists $\lambda \in K^\times$ such that $\lambda g, \lambda^{-1} h \in R[X]$. Since g, h are monic, it follows that $\lambda = 1$ and the claim holds. □

Before we preceed to give our main theorem, we prove a lemma that will be used later.

Lemma 5.4.10. *Let R be a UFD, and let K be its field of fractions. For nonzero $f, g \in R[X]$, denote by $(f)_K, (g)_K$ the principal ideals $fK[X]$, $gK[X]$ in $K[X]$. Then $(f) \subseteq (g)$ if and only if the following conditions are satisfied:*

- $(\mathrm{cont}_f) \subseteq (\mathrm{cont}_g)$.
- $(f)_K \subseteq (g)_K$.

The cliam still holds if we replace all the inclusions by equality.

Proof. The condition $(f) \subseteq (g)$ clearly implies $(f)_K \subseteq (g)_K$ and $(\mathrm{cont}_f) \subseteq (\mathrm{cont}_g)$. Thus we may assume the converse.

Since $(f)_K \subseteq (g)_K$ means $f = gh$, where $h \in K[X]$. Write $h = a/b \cdot h_1$ where $a, b \in R$ and h_1 is primitive, we then have

$$bf = agh_1.$$

Since h_1 is primitive, by Gauss's lemma we conclude

$$(b\,\mathrm{cont}_f) = (a\,\mathrm{cont}_g).$$

By hypothesis we have $(b\,\mathrm{cont}_f) \subseteq (b\,\mathrm{cont}_g)$, thus

$$(a\,\mathrm{cont}_g) \subseteq (b\,\mathrm{cont}_g).$$

Since R is an integral domain and $(\mathrm{cont}_g) \neq (0)$, this implies $a = bc$ for some $c \in R$. But then $h = ch_1 \in R[X]$, so that $(f) \subseteq (g)$. □

The first application is the following description of the irreducible elements of $R[X]$.

Proposition 5.4.11 (Irreducible crition for polynomials of UFDs). *Let R be a UFD, and let K be its field of fractions. Let $f \in R[X]$ be a nonconstant polynomial. Then f is irreducible in $R[X]$ if and only if it is irreducible in $K[X]$ and primitive in $R[X]$.*

Proof. Assume that f is irreducible in $R[X]$, then f is primitive, otherwise we could factor out its content. Next, assume that $f = gh$, with $g, h \in K[X]$; we have to prove that either g or h is a unit in $K[X]$. Let $c, d \in K$ be such that

$$g = cg_1, \quad h = dh_1,$$

where $g_1, h_1 \in R[X]$ are primitive. Then g_1h_1 is also primitive and we have $(\mathrm{cont}_{g_1h_1}) = (1) = (\mathrm{cont}_f)$. Further, we have $(f)_K = (gh_K) = (g_1h_1)_K$, thus by Lemma 5.4.10 we obtain $(f) = (g_1h_1)$. As f is irreducible in $R[X]$, this implies that either g_1 or h_1 is a unit in $R[X]$. But then g or h were units in $K[X]$, verifying that f is irreducible in $K[X]$.

Conversely, assume that f is irreducible in $K[X]$ and primitive. If $f = gh$ for $g, h \in R[X]$, then view this equation as in $K[X]$, we find tht g or h is a unit in $K[X]$. That is, $g \in K$ or $h \in K$. Assume that $g \in K$. Since $R[X] \cap K = R$ and f is primitive, g is then a unit in R. This implies that f is irreducible in $R[X]$. □

Theorem 5.4.12 (Gauss). *If R is a UFD, then $R[X]$ is a UFD.*

Proof. We begin by verifying the a.c.c. for principal ideals in $R[X]$. Let

$$(f_1) \subseteq (f_2) \subseteq (f_3) \subseteq \cdots$$

be an ascending chain of principal ideals of $R[X]$. By Lemma 5.4.10, this induces ascending chains of principal ideals

$$(\mathrm{cont}_{f_1}) \subseteq (\mathrm{cont}_{f_2}) \subseteq (\mathrm{cont}_{f_3}) \subseteq \cdots \quad \text{and} \quad (f_1)_K \subseteq (f_2)_K \subseteq (f_3)_K \subseteq \cdots.$$

Since R and $K[X]$ are both UFDs, these chains stabilizes. Thus by Lemma 5.4.10 again the original chain also stabilizes.

Next, we consider an irreducible element f of $R[X]$. By Corollary 5.4.9 f is primitive and irreducible in $K[X]$, thus is prime in $K[X]$. Consider the composition

$$\rho : R[X] \hookrightarrow K[X] \twoheadrightarrow \frac{K[X]}{(f)_K}.$$

We claim that $\ker \rho = (f)$. In fact, for $g \in R[X]$, $\rho(g) = 0$ is equivalent to $(g)_K \subseteq (f)_K$. Since we always have $(\mathrm{cont}_g) \subseteq (\mathrm{cont}_f) = 1$, by Lemma 5.4.10 this is exactly $(g) \subseteq (f)$. Since $\ker \rho = (f)$,

we find that ρ induces an injective homomorphism

$$\tilde{\rho} : \frac{R[X]}{(f)} \hookrightarrow \frac{K[X]}{(f)_K}.$$

Since the ring on the right is an integral domain, this implies $R[X]/(f)$ is also an integral domain. Thus (f) is prime in $R[X]$. □

Corollary 5.4.13. *If R is a UFD, then $R[X_1, \dots, X_n]$ is a UFD.*

Example 5.4.14. Let R be a UFD. Since every elements of $R[X_1, X_2, \cdots]$ can be embedded to $R[X_1, \dots, X_n]$ for some n, we find that $R[X_1, X_2, \cdots]$ is also a UFD. However, $R[X_1, X_2, \cdots]$ is not Noetherian, thus we get an example of a non-Noetherian UFD.

Irreducibility of a polynomial in several variables is more difficult to determine than irreducibility of a polynomial of one variable, but here is one criterion.

Proposition 5.4.15. *Let k be a field, and view $f(X_1, \dots, X_n) \in k[X_1, \dots, X_n]$ as a polynomial in $R[X_n]$, where $R = k[X_1, \dots, X_n]$:*

$$f(X_n) = a_0(X_1, \dots, X_{n-1}) + \cdots + a_m(X_1, \dots, X_{n-1})X_n^m.$$

If $f(X_n)$ is primitive and cannot be factored into two polynomials of lower degree in in $R[X_n]$, then $f(X_1, \dots, X_n)$ is irreducible in $k[X_1, \dots, X_n]$.

Proof. Suppose that $f(X_n) = g(X_n)h(X_n)$ in $R[X_n]$; by hypothesis, $\deg g = 0$ or $\deg h = 0$. It follows, because f is primitive, that g or h is a unit in R. Therefore, $f(X_1, \dots, X_n)$ is irreducible in $k[X_1, \dots, X_n]$. □

Corollary 5.4.16. *If $g(X_1, \dots, X_n)$ and $h(X_1, \dots, X_n)$ are relatively prime in $k[X_1, \dots, X_n]$, then $f(X_1, \dots, X_n, Y) = Yg(X_1, \dots, X_n) + h(X_1, \dots, X_n)$ is irreducible in $k[X_1, \dots, X_n, Y]$.*

Proof. Let $R = k[X_1, \dots, X_n]$. Note that f is primitive in $R[Y]$, because $(g, h) = 1$ forces any divisor of its coefficients g, h to be a unit. Since f is linear in Y, it is not the product of two polynomials in $R[Y]$ of smaller degree, and hence Proposition 5.4.15 shows that f is irreducible in $R[Y] = k[X_1, \dots, X_n, Y]$. □

As an application we consider irreducibility in $\mathbb{Z}[X]$.

Proposition 5.4.17. *Let $f \in \mathbb{Z}[X]$ be a primitive polynomial, and let p be a prime integer. Assume f mod p has the same degree as f and is irreducible in $\mathbb{Z}/p\mathbb{Z}[X]$. Then f is irreducible in $\mathbb{Z}[X]$.*

Proof. Argue contrapositively: if f is primitive and reducible in $\mathbb{Z}[X]$ and $\deg f = n$, then $f = gh$ with $\deg g = d, \deg h = e, d + e = n$. But then the same can be said of f mod p, so f mod p is also reducible. □

The hypothesis on degrees is necessary, precisely to take care of the special cases mentioned in the discussion preceding the statement. For example, $2X^3 + 3X^2 + 3X + 1$ equals $X^2 + X + 1$ mod 2, and the latter is irreducible in $\mathbb{Z}/2\mathbb{Z}[X]$; yet $2X + 1$ is a factor of the former. The point is of course that $2X + 1$ is a unit mod 2.

Remark 5.4.1. There are irreducible polynomials in $\mathbb{Z}[X]$ which are reducible modulo all primes! So Proposition 5.4.17 cannot be turned into a characterization of irreducibility in $\mathbb{Z}[X]$. It is however rather useful in producing examples.

Corollary 5.4.18. *There are irreducible polynomials in $\mathbb{Z}[X]$ and $\mathbb{Q}[X]$ of arbitrarily large degree.*

Proof. By Corollary 5.4.9, the statement for $\mathbb{Z}[X]$ implies the one for $\mathbb{Q}[X]$. By Proposition 5.4.17, it suffices to verify that there are irreducible polynomials in $\mathbb{Z}/p\mathbb{Z}[X]$ of arbitrarily large degree, for any prime integer p. This is a particular case of Corollary 9.3.28. □

The following result is commonly established in $\mathbb{Z}[X]$, but it holds for general rings.

Theorem 5.4.19 (Eisenstein's criterion). *Let R be a commutative ring, and let $\mathfrak{p}$ be a prime ideal of R. Let*

$$f = a_n X^n + \cdots + a_1 X + a_0 \in R[X]$$

be a polynomial, and assume that

- $a_n \notin \mathfrak{p}$.
- $a_i \in \mathfrak{p}$ *for* $0 \leq i \leq n-1$.
- $a_0 \notin \mathfrak{p}^2$.

Then f is not the product of polynomials of degree $< n$ in $R[X]$.

Proof. Argue by contradiction. Assume $f = gh$ in $R[X]$, with both $d = \deg g$ and $e = \deg h$ less than n; write

$$g = b_d X^d + \cdots + b_1 X + b_0, \quad h = c_e X^e + \cdots + c_1 X + c_0.$$

and note that necessarily $d > 0$ and $e > 0$. Consider f modulo $\mathfrak{p}$: thus

$$\overline{f} = \overline{gh} \text{ in } (R/\mathfrak{p})[X].$$

By hypothesis, $\overline{f} = a_n x^n$ modulo $\mathfrak{p}$, where $a + n \neq 0$ in $R/\mathfrak{p}$. Since $R/\mathfrak{p}$ is an integral domain, factors of $\overline{f}$ must also be monomials: that is, necessarily

$$\overline{g} = \overline{b_d} X^d, \quad \overline{h} = \overline{c_e} X^e.$$

Since $d, e > 0$, this implies $b_0 \in \mathfrak{p}$, $c_0 \in \mathfrak{p}$. But then $a_0 = b_0 c_0 \in \mathfrak{p}^2$, contradiction. □

Example 5.4.20. For all n and all primes p, the polynomial $x^n - p$ is irreducible in $\mathbb{Z}[X]$. This follows immediately from Eisenstein's criterion and gives an alternative proof of Corollary 5.4.18.

Proposition 5.4.21. *The polynomial*

$$\frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + 1$$

is irreducible over $\mathbb{Z}$ if and only if p is a prime.

Proof. If p is prime, plug into $X = X + 1$ yields

$$\frac{(X+1)^p - 1}{X} = X^{p-1} + \binom{p}{p-1} X^{p-2} + \cdots + \binom{p}{1}$$

thus we only need to show p divides $\binom{p}{k}$ for all $k = 1, \ldots, p-1$, and apply Eisenstein's criterion. But we have

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}$$

and p divides the numerator and does not divide the denominator; the claim follows as p is prime.

For p not a prime, we write $p = mn$, and note that

$$\frac{X^p - 1}{X - 1} = \frac{X^{mn} - 1}{X - 1} = \frac{X^{mn} - 1}{X^m - 1} \cdot \frac{X^m - 1}{X - 1}$$

so the polynomial is reducible. □

5.5 A prime ideal principle

We start with the two crucial definitions

Definition 5.5.1. *An ideal family $\mathcal{F}$ in a ring R with $R \in \mathcal{F}$ is said to be an* ***Oka family*** *if for $a \in R$ and $I \subseteq R$ an ideal,*

$$(I, a) \in \mathcal{F}, (I : a) \in \mathcal{F} \Rightarrow I \in \mathcal{F}.$$

It is a ***strongly Oka family*** *if for I, J ideals of R,*

$$(I, J) \in \mathcal{F}, (I : J) \in \mathcal{F} \Rightarrow I \in \mathcal{F}.$$

Definition 5.5.2. *An ideal family $\mathcal{F}$ in a ring R with $R \in \mathcal{F}$ is said to be an* ***Ako family*** *if for $a, b \in R$ and $I \subseteq R$ an ideal,*

$$(I, a) \in \mathcal{F}, (I, b) \in \mathcal{F} \Rightarrow (I : ab) \in \mathcal{F}.$$

It is a ***strongly Ako family*** *if for I, J ideals of R,*

$$(I, a) \in \mathcal{F}, (I, J) \in \mathcal{F} \Rightarrow (I, aJ) \in \mathcal{F}.$$

The following connections between the definitions are self-evident.

Proposition 5.5.3.

(1) *A strongly Oka family is Oka, and conversely if R is a principal ideal ring.*

(2) *A strongly Ako family is Ako, and conversely if R is a principal ideal ring.*

We will use $\mathcal{F}^c$ to denote the set of all ideals of R not belonging to $\mathcal{F}$, and $\mathrm{Max}(\mathcal{F}^c)$ for the set of maximal elements of $\mathcal{F}^c$ with respect to the partial ordering given by inclusion. We will say $\mathcal{F}^c$ is an **MP-family** if $\mathrm{Max}(\mathcal{F}^c) \subseteq \mathrm{Spec}(R)$.

With the notions of Oka and Ako families in place, we can now formulate the following general result.

Theorem 5.5.4. *If $\mathcal{F}$ is an Oka family or an Ako family, then $\mathcal{F}^c$ is an MP-family, that is,* $\mathrm{Max}(\mathcal{F}^c) \subseteq \mathrm{Spec}(R)$.

Proof. Suppose some $I \in \mathrm{Max}(F^c)$ is not prime. Since $I \neq R$, there exist $a, b \in R - I$ such that $ab \in I$. Then

$$(I, b), (I : a) \supset I, \quad (I, a), (I : b) \supset I.$$

Therefore, $(I, a), (I, b)$ and $(I : a), (I : b)$ all belong to $\mathcal{F}$. But $I = (I, ab) \notin \mathcal{F}$, so $\mathcal{F}$ is neither Oka nor Ako. □

Remark 5.5.1. The converse of Theorem 5.5.4 does not hold in general. For instance, let $(R, (t))$ be a DVR, and let $\mathcal{F} = \{(t)^i \mid i \neq 1, 4\}$. Then $\mathcal{F}^c = \{(0), (t), (t)^4\}$ is an MP-family since $\mathrm{Max}(\mathcal{F}^c) = \{\mathfrak{m}\} \subseteq \mathrm{Spec}(R)$. But $\mathcal{F}$ is not Oka since $I := (t)^4 \notin \mathcal{F}$, but $(I, t^2) = (I : t^2) = (t)^2 \in \mathcal{F}$. From $(I, t^4) = (t^4) = I \notin \mathcal{F}$, we see that $\mathcal{F}$ is also not Ako.

Proposition 5.5.5. *For an ideal family $\mathcal{F}$ in R with $R \in \mathcal{F}$, consider the following property, where I, J denote arbitrary ideals in R:*

(1) *$I \subseteq J$ and $J, (I : J) \in \mathcal{F} \Rightarrow I \in \mathcal{F}$ if J/I is cyclic.*

(2) *$I \subseteq J$ and $J, (I : J) \in \mathcal{F} \Rightarrow I \in \mathcal{F}$.*

Then the condition Oka is equivelent to (1)*, and strongly Oka to* (2)*.*

Proof. If $\mathcal{F}$ satisfies (2), then for $I, J \subseteq R$ with $(I, J) \in \mathcal{F}, (I : J) \in \mathcal{F}$, we have

$$I \subseteq (I, J) \quad \text{and} \quad (I : (I, J)) = (I : J)$$

Therefore by (2) we get $I \in \mathcal{F}$, hence $\mathcal{F}$ is strongly Oka. Conversely, if $\mathcal{F}$ is strongly Oka, since for ideals $I \subseteq J$ we have $(I, J) = J$, the condition (2) clearly holds. □

Theorem 5.5.6. *Let S be a multiplicative set in a ring R. An ideal $I \subseteq R$ that is maximal with respect to being disjoint from S is prime.*

Proof. Let $\mathcal{F} = \{I \subseteq R \mid I \cap S \neq \varnothing\}$ be the set of ideals touching S. We claim that $\mathcal{F}$ is an Ako family. In fact, if $(I, a) \in \mathcal{F}$ and $(I, b) \in \mathcal{F}$, then there are $k_1, k_2 \in R$ and $r_1, r_2 \in I$ such that

$$x = k_1 a + r_1 \in S, \quad y = k_2 b + r_2 \in S$$

Then since S is multiplicative, we have

$$S \ni xy = k_1 k_2 ab + k_1 a r_2 + k_2 b r_1 + r_1 r_2 \in (I, ab).$$

Therefore $(I, ab) \in \mathcal{F}$. □

Theorem 5.5.7. *Let I be an ideal in a ring R that is maximal with respect to not being finitely generated. Then I is prime.*

Proof. Let $\mathcal{F}$ be the set of all ideals of R that are finitely generated. If (I, x) and $(I : x)$ are finitely generated, we claim that I is also finitely generated. In fact, if

$$(I, x) = (p_1 + r_1 x, p_2 + r_2 x, \ldots, p_n + r_n x), \quad p_i \in I, r_i \in R.$$

Let $I_0 = (p_1, \dots, p_n)$, for $p \in I$ we have

$$p = \sum_{i=1}^{n} c_i(p_i + r_i x) = \sum_{i=1}^{n} c_i p_i + x \sum_{i=1}^{n} c_i r_i$$

Note that $x \sum c_i r_i = p - \sum c_i p_i \in I$, so it is in $x(I : x)$. Therefore we have proved that

$$I = I_0 + x(I : x)$$

Now $(I : x)$ is finitely generated, thus I is also finitely generated.

This means $\mathcal{F}$ is a Oka family, so the claim follows. □

Theorem 5.5.8. *Let I be an ideal in a ring R that is maximal with respect to being nonprincipal. Then I is prime.*

Proof. Let $\mathcal{F}$ be the set of all principal ideals of R. We show that $\mathcal{F}$ satisfies the condition (2) in Proposition 5.5.5, thus is strongly Oka. For $I \subseteq J$ ideals such that $J, (I : J) \in \mathcal{F}$, write $J = (x)$ then we observe that

$$I = x \cdot (I : x) \in \mathcal{F}$$

since $I \subseteq J = (x)$. Therefore the claim follows. □

5.6 Some results on UFDs and PIDs

5.6.0.0.1 On UFDs

Proposition 5.6.1 (Kaplansky's theorem). *An integral domain is a UFD iff every nonzero prime ideal contains a nonzero prime element.*

Proof. Let R be a UFD and $\mathfrak{p}$ a nonzero prime ideal of R. Choose $0 \neq x \in \mathfrak{p}$ and write $x = p_1 \cdots p_r$ into irreducibles. Then since $\mathfrak{p}$ is prime, one of the p_i's is in $\mathfrak{p}$. Since R is a UFD, p_i's are prime, so this gives one direction.

Conversely, assume the condition on prime ideals, if we can prove that every elements of R can be written into products of prime elements, then clearly R is a UFD. To show this, let

$$S = \{x \in R - \{0\} \mid x \text{ is a unit or } x \text{ can be written into prduct of prime elements}\}$$

Then clearly S is a multiplicative subset, so that a maximal element $I \subseteq R$ with respect to being disjoint from S is prime. If $I \neq 0$, then I contains a nonzero prime, which implies $I \cap S \neq \varnothing$, contradiction. Therefore $I = (0)$ and we get $S = R - \{0\}$, verifying our claim. □

Corollary 5.6.2. *If R is a UFD, then every prime ideal of height 1 in R is principal.*

Proof. Since R is an integral domain, a prime $\mathfrak{p}$ has height 1 means $\mathfrak{p}$ does not properly contains any prime idels. In particular $\mathfrak{p} \neq 0$, so by Proposition 5.6.1 $\mathfrak{p}$ contains a nonzero prime element p. Since (p) is then a prime ideal contained in $\mathfrak{p}$, we must have $\mathfrak{p} = (p)$. □

Proposition 5.6.3. *A Noetherian domain R is a UFD iff every prime ideal of height 1 in R is principal.*

Proof. One direction is showed in the previous corollary, so assume the later condition. Since the a.c.c. for principal ideals are satisfied, we only need to show that every irreducible element is prime. Let x be irreducible and $\mathfrak{p}$ be a minimal prime of (x), then since x is not a unit and not a zero-divisor, by Krull principal ideal theorem $\mathfrak{p}$ has height 1. By our assumption $\mathfrak{p}$ is principal, so write $\mathfrak{p} = (p)$. Clearly p is a prime element, and $(x) \subseteq (p)$. Since x is irreducible, we then conclude $(x) = (p) = \mathfrak{p}$, showing that x is prime. □

5.6.0.0.2 On PIDs

Theorem 5.6.4. *Let R be an integral domain. Then R is a PID iff every prime ideal of R is principal.*

Proof. This is a consequence of Theorem 5.5.8. □

Definition 5.6.5. *Let R be an integral domain, a function $v : R \to \mathbb{Z}^{\geq 0}$ is called a* ***Dedekind-Hasse norm*** *if it satisfies the following conditions:*

(1) $v(a) = 0$ *if and only if* $a = 0$.

(2) *For any nonzero elements a and b in R either $b \mid a$ or there exist elements x and y in R such that*

$$0 < v(xa - yb) < v(b).$$

Proposition 5.6.6. *An integral domain is a PID if and only if there is a Dedekind-Hasse norm on it.*

Proof. Assume the existence of the norm v, we prove that R is a PID. Let I be a nonzero ideal of R. We consider the set

$$S = \{x \mid x = v(a), 0 \neq a \in I\} \subseteq \mathbb{Z}^{\geq 0}$$

Then S has a minimal element, say x_0. If $v(a_0) = x_0$ is the least of the v-values of nonzero elements of I, then $0 < v(a_0) \leq v(a)$ if a_0 does not divide a.

For $0 \neq a \in I$, there exists a pair $x, y \in R$ such that

$$0 < v(ax - a_0 y) < v(a_0).$$

Since $ax - a_0 y \in I$, this contradicts the choice of a_0. Therefore, $a_0 \mid a$ for all $a \in I$, and I is principal.

Suppose that R is a PID. We define

$$v(a) = \begin{cases} 0 & \text{if } a = 0 \\ 2^n & \text{if } a \neq 0 \text{ and } n \text{ is the number of irreducible factors of } a \end{cases}$$

Then $v(a) = 0$ iff $a = 0$ by our definition. For nonzero elements $a, b \in R$ with $b \nmid a$, we write $I = (a, b)$. Since I is principal, $I = (d)$ for some $d \in R$. Then there exists a pair $x, y \in R$ such that $ax + by = d$, and from $d \mid b$ we get

$$0 < v(ax + by) = v(d) < v(b).$$

Thus v is a Dedekind-Hasse norm for R. □

Proposition 5.6.7. *An integral domain is a PID iff it is Bezout and satisfies the a.c.c. for principal ideals.*

Proof. One direction is clear, assume the other. By Theorem 5.3.8 we know that R is a UFD, so we can define a norm as in Proposition 5.6.6. The Bezout condition implies that this norm is a Dedekind-Hasse norm, thus R is a PID. □

5.6.0.0.3 On UFD into PID

Proposition 5.6.8. *Let R be a UFD. Then R is a PID iff* $\dim R = 1$.

Proof. If R is a PID, then prime ideals are maximal in R, so $\dim R = 1$. Conversely, if $\dim R = 1$, then every nonzero prime ideal has height 1. By Corollary 5.6.2 they are principal. Now apply Theorem 5.6.4. □

Proposition 5.6.9. *Let R be a UFD. Then R is a PID iff maximal ideals of R are principal.*

Proof. Let $\mathfrak{p}$ be a nonzero prime ideal of R. Then $\mathfrak{p}$ is contained in a maximal ideal $\mathfrak{m}$, which by assumption is principal: $\mathfrak{m} = (x)$. Since R is a UFD, by Proposition 5.6.1, $\mathfrak{p}$ contains a nonzero prime element p. Then we have $(p) \subseteq (x) = \mathfrak{m}$. As p is irreducible, (p) is maximal among principal ideals, thus $(p) = (x) = \mathfrak{m}$. We then get $\mathfrak{p} = \mathfrak{m}$ is principal, and therefore R is a PID by Theorem 5.6.4. □

5.6.0.0.4 Fermat's Last Theorem for Polynomials

Theorem 5.6.10. *Let $f, g, h \in \mathbb{C}[X]$ be nonconstant polynomials such that no irreducible divides all of f, g, h. If*

$$f^n + g^n = h^n.$$

then $n \leq 2$.

Note that we cannot improve on this bound of $n \leq 2$. Indeed, if $f \in \mathbb{C}[X]$ then it is always true that

$$(1 - f^2)^2 + (2f)^2 = (1 + f^2)^2.$$

We present two proofs.

***Proof* 1*: Induction and Roots of Unity*.** Because we are working over $\mathbb{C}$ we have all roots of unity. Thus we can factor

$$h^n = f^n + g^n = (f + g)(f + \zeta g) \cdots (f + \zeta^{n-1} g) = \prod_{i=0}^{n-1} (f + \zeta^i g)$$

where $\zeta = e^{2\pi i/n}$. Note that for $i \neq j$, $f + \zeta^i g$ and $f + \zeta^j g$ are coprime. Indeed

$$f + \zeta^i g - (f + \zeta^j g) = (\zeta^i - \zeta^j) g, \quad f + \zeta^i g - (\zeta^i - \zeta^j) \frac{\zeta^i}{\zeta^i - \zeta^j} g = f.$$

so that $\gcd(f + \zeta^i g, f + \zeta^j g) = \gcd(f, g) = 1$. Now we are prepared for the first proof.

Let $\deg f + \deg g = d$ and $n \geq 3$. By above,

$$h^n = \prod_{i=0}^{n-1}(f + \zeta^i g)$$

These are pairwise coprime polynomials. Since h^n factors into n-th powers, each $f + \zeta^i g$ is also a n-th power.

We proceed by inducting on d. If $d = 2$, then f, g are linear and this is clearly impossible by degree considerations. Now supppose the theorem holds for all degrees less than d where $d > 2$. We have $f + g = a^n, f + \zeta g = b^n, f + \zeta^2 g = c^n$ (this is where the $n > 2$ hypothesis enters). Then

$$-\zeta a^n + (1 + \zeta)b^n = -\zeta f - \zeta g + (1 + \zeta)(f + \zeta g) = f + \zeta^2 g = c^n$$

Thus we obtain a relation $(\lambda a)^n + (\mu b)^n = (\nu c)^n$, where $\lambda, \mu, \nu \in \mathbb{C}$. Since a, b, c has degree strictly small that f, g, we get the claim. □

Theorem 5.6.11 (Mason's theorem). *Let F be any field. Suppose $f, g, h \in F[X]$ are nonzero and that f, g, h are coprime. If f, g, h satisfy the equation $f + g = h$, then either $D(f) = D(g) = D(h) = 0$, or*

$$\max\{\deg f, \deg g, \deg h\} \leq \deg \sqrt{fgh} - 1.$$

Proof 2: Computations of Degrees. Suppose there exist $f, g, h \in \mathbb{C}[X]$ nonconstant, coprime such that

$$f^n + g^n = h^n.$$

Then by Mason's Theorem we have

$$\max\{\deg f^n, \deg g^n, \deg h^n\} \leq \deg \sqrt{fgh} - 1 \leq \deg f + \deg g + \deg h - 1.$$

The maximum of a finite set is at least the mean, so the left side is at least

$$\frac{\deg f^n + \deg g^n + \deg h^n}{3} = \frac{n}{3}(\deg f + \deg g + \deg h) \geq \deg f + \deg g + \deg h$$

contradiction. □

5.7 Exercise

Exercise 5.7.1. Prove that the inclusion $i : \mathbb{Z} \to \mathbb{Q}$ is an epimorphism of rings, through it is not surjective.

Proof. If there are two ring homomorphism α_1, α_2 such that $\alpha_a|\mathbb{Z} = \alpha_2|\mathbb{Z} := \alpha$, then

$$\alpha_i\left(\frac{p}{q}\right) = \alpha_i(p)\alpha_i(q^{-1}) = \alpha(p)\big(\alpha(q)\big)^{-1}$$

so they coincide on $\mathbb{Q}$, which show that i is an epimorphism of rings. □

Exercise 5.7.2. Prove that the polynomial $(x-1)(x-2)\cdots(x-n) - 1$ is irreducible in $\mathbb{Q}[X]$ for all $n \geq 1$.

Proof. Suppose $h = fg$ is a nontrivial factorization of h where h is the polynomial above, then we see $f(i)g(i) = -1$ for $i = 1, \dots, n$. So $f(i), g(i) = \pm 1$ and $f(i) = -g(i)$. Now the polynomial $f(x) + g(x)$ has n roots with its degree strictly less than n, hence is identically zero. So we conclude $f(x) = -g(x)$ and $h = -f^2$. But $h(x)$ also takes positive values, which is a contradiction. □

Exercise 5.7.3. Prove that the polynomial $(x-1)(x-2)\cdots(x-n)+1$ is irreducible in $\mathbb{Q}[X]$ for all $n \geq 1, n \neq 4$.

Proof. Suppose $h = fg$ is a nontrivial factorization of h where h is the polynomial above, then we see $f(i)g(i) = 1$ for $i = 1, \dots, n$. Similar to the exercise above, we get $h = f^2$, so n must be even, let $n = 2k$.

The cases $n = 2$ and $n = 4$ are easy to varify, so we assume $n \geq 6$. Now $f(x)$ takes the value ± 1 on the set $\{1, \dots, 2k\}$, let denotes I, J the subset on which $f(x) = 1$, $f(x) = -1$ respectively, and assume $1 \in I$. Since $k \geq 3$, J has at least 3 distinct elements greater than 1, so there exists an elment u in J such that $u - 1 \geq 3$. But we must have $u - 1 \mid f(u) - f(a) = -2$, contradiction. (We have $a - b \mid f(a) - f(b)$ since $a - b | a^n - b^n$ is true for every n.) □

Exercise 5.7.4. Let R be a ring. The opposite ring R° is obtained from R by reversing the multiplication: that is, the product $a \bullet b$ in R° is defined to be $ba \in R$. Prove that the identity map $R \to R^\circ$ is an isomorphism if and only if R is commutative. Prove that $\mathcal{M}_n(R)$ is isomorphic to its opposite (not via the identity map!). Explain how to turn right-R-modules into left-R-modules and conversely, if $R \simeq R^\circ$. (by this exercise, we can identify left and right module if we are considering commutative rings)

Proof. The first claim is clear, for the second, suppose $\rho : R \times M \to M$ is a left action on M. Now we define a new action σ on M by R° through:

$$\sigma : M \times R \to M, \quad (m, r) \mapsto \rho(r, m)$$

We verify that

$$\begin{aligned}
&\sigma(m, r+s) = \rho(r+s, m) = \rho(r, m) + \rho(s, m) = \sigma(m, r) + \sigma(m, s) \\
&\sigma(m+n, r) = \rho(r, m+n) = \rho(r, m) + \rho(r, n) = \sigma(m, r) + \sigma(n, r) \\
&\sigma(m, r \bullet s) = \rho(r \bullet s, m) = \rho(sr, m) = \rho(s, \rho(r, m)) = \rho(s, \sigma(m, r)) = \sigma(\sigma(m, r), s) \\
&\sigma(m, 1) = \rho(1, m) = m
\end{aligned}$$

this shows that σ is a right action. □

Exercise 5.7.5. Let G be an abelian group. Prove that if G has a structure of $\mathbb{Q}$-vector space, then it has only one such structure.

Proof. For any $g \in G, g \neq 0$, we know g has infinite order since $ng = 0$ implies $g = 0$. Since the map ng and $\frac{1}{n}g$ are uniquely determined, G can only have one $\mathbb{Q}$-vector space structure. □

Exercise 5.7.6. An abelian group A is a vector space over $\mathbb{Q}$ if and only if it torsion free and is divisible.

Exercise 5.7.7. Let R be a commutative ring, and let I, J be ideals of R. Prove that $I \cdot (R/J) \simeq (I+J)/J$ as R-modules.

Proof. Since we have

$$\frac{I+J}{J} \simeq \frac{I}{I \cap J}$$

we only need to show $I/(I \cap J) \simeq I \cdot (R/J)$. Define a homomorphism:

$$\psi : I \to I \cdot (\frac{R}{J}), \quad i \mapsto i(1+J) = i + J$$

the kernel of ψ is exactly $I \cap J$. Every element in $I \cdot (R/J)$ has the form

$$ir + J \quad \text{for} \quad i \in I, r \in R.$$

Since I is an ideal, $ir \in I$, so $\psi(ir) = ir + J$, which gives the surjectivity of ψ. So we find

$$\frac{I}{I \cap J} \simeq I \cdot (\frac{R}{J})$$

as desired. □

Exercise 5.7.8. Let I, J be ideals in a ring R, such that $I + J = (1)$. Prove that $IJ = I \cap J$.

Proof. Since $I + J = (1)$, there is elements $x \in I$, $y \in J$ such that $x + y = 1$. Then for $a \in I \cap J$, we have

$$a = a \cdot 1 = a(x+y) = ax + ay$$

Since $a \in I, a \in J$, we have $ax \in IJ$ and $ay \in IJ$. Thus $I \cap J \subseteq IJ$. Hence the claim follows. □

Exercise 5.7.9. Let I, J be ideals in a ring R. Assume that $R/(IJ)$ is reduced (that is, it has no nonzero nilpotent elements). Prove that $IJ = I \cap J$.

Proof. For $a \in I \cap J$, we have $a^2 \in IJ$. Hence $(a + IJ)^2 = 0$ in $R/(IJ)$ and $a + IJ = 0$ since it is reduced. This means $a \in IJ$. Hence the claim follows. □

Chapter 6

Chain conditions

6.1 General properties

Let Σ be a set partially ordered by a relation $\leq$.

Proposition 6.1.1. *The following conditions on Σ are equivalent:*

(a) Every increasing sequence $x_1 \leq x_2 \leq \cdots$ in Σ is stationary.

(b) Every non-empty subset of Σ has a maximal element.

Proof. If (b) is false there is a non-empty subset T of Σ with no maximal element, and we can construct inductively a non-terminating strictly increasing sequence in T. The converse is easy to see. □

If Σ is the set of submodules of a module M, ordered by the relation $\subseteq$, then (a) is called the **ascending chain condition** (a.c.c. for short) and (b) the **maximal condition**. A module M satisfying either of these equivalent conditions is said to be **Noetherian**.

If Σ is ordered by $\supseteq$, then (a) is the **descending chain condition** (d.c.c. for short) and (b) the **minimal condition**. A module M satisfying these is said to be **Artinian**.

Example 6.1.2 (Examples of Noetherian and Artinian rings).

(a) A finite abelian group (as $\mathbb{Z}$-module) satisfies both a.c.c. and d.c.c.

(b) The ring $\mathbb{Z}$ satisfies a.c.c. but not d.c.c. For if $a \in \mathbb{Z}$ and $a \neq 0$ we have $(a) \supseteq (a^2) \supseteq (a^n) \supseteq \cdots$ (strict inclusions).

(c) Let G be the subgroup of $\mathbb{Q}/\mathbb{Z}$ consisting of all elements whose order is a power of p, where p is a fixed prime. Then G has exactly one subgroup G_n of order p^n for each $n \geq 0$, and $G_0 \subseteq G_1 \subseteq \cdots$ (strict inclusions) so that G does not satisfy the a.c.c. On the other hand the only proper subgroups of G are the G_m so that G does satisfy d.c.c.

(d) The group H of all rational numbers of the form m/p^n $(m, n \in \mathbb{Z}, n \geq 0)$ satisfies neither chain condition. For we have an exact sequence

$$0 \longrightarrow \mathbb{Z} \longrightarrow H \longrightarrow G \longrightarrow 0$$

so that H doesn't satisfy d.c.c. because $\mathbb{Z}$ doesn't; and H doesn't satisfy a.c.c. because G doesn't.

(e) The ring $k[X]$ where k is a field satisfies a.c.c. but not d.c.c. on ideals.

(f) The polynomial ring $k[X_1, X_2, \cdots]$ in an infinite number of indeterminates satisfies neither chain condition on ideals: for the sequence $(X_1) \subseteq (X_1, X_2) \subseteq \cdots$ is strictly increasing, and the sequence $(X_1) \supseteq (X_1^2) \supseteq \cdots$ is strictly decreasing.

(g) We shall see later that a ring which satisfies d.c.c. **on ideals** must also satisfy a.c.c. **on ideals**. (This is not true in general for modules.)

Proposition 6.1.3. *A module M is a Noetherian A-module if and only if every submodule of M is finitely generated.*

Proof. Assume that M is Noetherian and let N be a submodule of M, and let Σ be the set of all finitely generated submodules of N. Then Σ is not empty (since $0 \in \Sigma$) and therefore has a maximal element, say N_0. If $N_0 = N$, consider the submodule $N_0 + Ax$ where $x \in N$, $x \notin N_0$; this is finitely generated and strictly contains N_0, so we have a contradiction. Hence $N = N_0$ and therefore N is finitely generated.

Conversely, assume that every submodule of M is finitely generateed. Let $M_1 \subseteq M_2 \subseteq \cdots$ be an ascending chain of submodules of M. Then $N = \bigcup_n M_n$ is a submodule of M, hence is finitely generated, say by $x_1, \ldots, x_r$. Say $x_i \in M_{n_i}$, and let $n = \max_i n_i$, then each $x_i \in M_n$ hence $M_n = M$ and therefore the chain is stationary. □

Because of Proposition 6.1.3, Noetherian modules are more important than Artinian modules: the Noetherian condition is just the right finiteness condition to make a lot of theorems work. However, many of the elementary formal properties apply equally to Noetherian and Artinian modules.

Proposition 6.1.4. *Let*

$$0 \longrightarrow L \xrightarrow{\alpha} M \xrightarrow{\beta} N \longrightarrow 0$$

be an exact sequence of A-modules. Then

(a) M is Noetherian if and only if L and N are Noetherian.

(b) M is Artinian if and only if L and N are Artinian.

Proof. An ascending chain of submodules of L (or N) gives rise to a chain in M, hence is stationary if M is Noetherian. Conversely, let (M_n) be an ascending chain of submodules of M; then $(\alpha^{-1}(M_n))$ is a chain in L, and $(\beta(M_n))$ is a chain in N. If L and N are Noetherian, then for large enough n both these chains are stationary, and it follows that the chain (M_n) is stationary. □

Proposition 6.1.5. *If $M_1, \ldots, M_n$ are Noetherian (resp. Artinian) A-modules, so is $\bigoplus_{i=1}^n M_i$.*

Proof. Apply induction and Proposition 6.1.4 to the exact sequence

$$0 \longrightarrow M_n \longrightarrow \bigoplus_{i=1}^n M_i \longrightarrow \bigoplus_{i=1}^{n-1} M_i \longrightarrow 0$$

we get the claim. □

A ring A is said to be **Noetherian** (resp. **Artinian**) if it is so as an A-module, i.e., if it satisfies a.c.c. (resp. d.c.c.) on ideals.

Example 6.1.6.

(a) Any field is both Artinian and Noetherian; so is the ring $Z/n\mathbb{Z}$ ($n \neq 0$). The ring $\mathbb{Z}$ is Noetherian, but not Artinian.

(b) Any principal ideal domain is Noetherian.

(c) The ring $k[X_1, X_2, \cdots]$ is not Noetherian. But it is an integral domain, hence has a field of fractions. Thus a subring of a Noetherian ring need not be Noetherian.

(d) Let X be a compact infinite Hausdorff space, $C(X)$ the ring of realvalued continuous functions on X. Take a strictly decreasing sequence $F_1 \supseteq F_2 \supseteq \cdots$ of closed sets in X, and let $I_n = \{f \in C(X) : f(F_n) = 0\}$ Then the I_n form a strictly increasing sequence of ideals in $C(X)$: so $C(X)$ is not a Noetherian ring.

Proposition 6.1.7. *Let A be a Noetherian (resp. Artinian) ring, M a finitely generated A-module. Then M is Noetherian (resp. Artinian).*

Proof. Since M is a quotient of A^n for some n, the result follows by applying Proposition 6.1.5 and Proposition 6.1.4. □

Proposition 6.1.8. *Let A be Noetherian (resp. Artinian), I an ideal of A. Then A/I is a Noetherian (resp. Artinian) ring.*

Proof. By Proposition 6.1.4 A/I is Noetherian (resp. Artinian) as an A-module, hence also as an A/I-module. □

A **chain** of submodules of a module M is a sequence $(M_i)_{i=0}^n$ of submodules of M such that

$$M = M_0 \supset M_1 \supset \cdots \supset M_n = 0$$

The **length** of the chain is defined to be n (the number of links). A **module composition series exist iff acc dcc** of M is a maximal chain, that is, each M_{i-1}/M_i is simple.

Proposition 6.1.9. *Suppose that M has a composition series of length n. Then every composition series of M has length n, and every chain in M can be extended to a composition series.*

Proof. Let $\ell(M)$ denote the least length of a composition series of a module M. We first note that if $N \subset M$ then $\ell(N) \leq \ell(M)$: Let (M_i) be a composition series of M of minimum length, and consider the submodules $N_i = N \cap M_i$ of N. Since $N_{i-1}/N_i \subseteq M_{i-1}/M_i$ and the latter is a simple module, we have either $N_{i-1}/N_i = M_{i-1}/M_i$ or else $N_{i-1} = N_i$; hence, removing repeated terms, we have a composition series of N, so that $\ell(N) \leq \ell(M)$. If $\ell(N) = \ell(M) = n$, then $N_{i-1}/N_i = M_{i-1}/M_i$ for each $1 \leq i \leq n$. This implies $M_{n-1} = N_{n-1}$, $M_{n-2} = N_{n-2}$, and finally $M = N$.

On the other hand, any chain in M has length smaller than $\ell(M)$. In fact, let

$$M = M_0 \supset M_1 \supset \cdots \supset M_k = 0$$

be a chain of length k. Then by the preceeding argument we have $\ell(M) > \ell(M_1) > \cdots > \ell(M_k) = 0$, hence $\ell(M) \geq k$.

Now consider any composition series of M. If it has length k, then we must have $k \leq \ell(M)$, and therefore $k = \ell(M)$ by the definition of $\ell(M)$. This proves all composition series of M have the same length.

Finally, consider any chain of M. If its length is $\ell(M)$ it must be a composition series; if its length is strictly smaller than $\ell(M)$, then it is not a composition series, hence not maximal, and therefore new terms can be inserted until the length is $\ell(M)$. □

Proposition 6.1.10. *M has a composition series if and only if M satisfies both chain conditions.*

Proof. One direction is clear: if M has a composition series, then every chain in M are of bounded length, hence both a.c.c. and d.c.c. hold. Conversely, if M satisfies both a.c.c. and d.c.c., we construct a composition series of M as follows. Since $M = M_0$ satisfies the maximum condition by Proposition 6.1.1, it has a maximal submodule $M_1 \subseteq M_0$. Similarly M_1 has a maximal submodule $M_2 \subseteq M_1$ and so on. Thus we have a strictly descending chain

$$M_0 \supset M_1 \supset M_3 \supset \cdots$$

which by d.c.c. must be finite, and hence is a composition series of M. □

A module satisfying both a.c.c. and d.c.c. is therefore called a **module of finite length**. By Proposition 6.1.9 all composition series of M have the same length $l(M)$, called the length of M. The **Jordan-Hölder theorem** applies to modules of finite length: if (M_i) and (M'_i) are any two composition series of M, there is a one-to-one correspondence between the set of quotients (M_{i-1}/M_i) and the set of quotients (M'_{i-1}/M'_i), such that corresponding quotients are isomorphic. The proof is the same as for finite groups.

Proposition 6.1.11. *The length $\ell(M)$ is an additive function on the class of all A-modules of finite length.*

Proof. We have to show that if

$$0 \longrightarrow L \xrightarrow{\alpha} M \xrightarrow{\beta} N \longrightarrow 0$$

is an exact sequence, then $\ell(M) = \ell(L) + \ell(N)$. Take the image under α of any composition series of L and the inverse image under β of any composition series of N; these fit together to give a composition series of M, hence the result. □

Example 6.1.12. If A is a field, then A-modules are just vector spaces, and the notation of length coincides with dimension. In particular, a vector space M is of finite length if and only if it is finite-dimensional.

To conclude, we give a condition when Noetherian is equivalent to Artinian. This result will be used latter when we discuss Artianian rings.

Corollary 6.1.13. *Let A be a ring in which the zero ideal is a product $\mathfrak{m}_1 \cdots \mathfrak{m}_n$ of maximal ideals. Then A is Noetherian if and only if A is Artinian.*

Proof. Consider the chain of ideals

$$A \supset \mathfrak{m}_1 \supset \mathfrak{m}_1\mathfrak{m}_2 \supset \mathfrak{m}_1 \cdots \mathfrak{m}_n = 0.$$

Each factor $\mathfrak{m}_1 \cdots \mathfrak{m}_{i-1}/\mathfrak{m}_1 \cdots \mathfrak{m}_i$ is a vector space over the field $A/\mathfrak{m}_i$. Hence a.c.c. if and only if d.c.c. for each factor. But a.c.c. (resp. d.c.c.) holds for each factor if and only if it holds for A, by repeated application of Proposition 6.1.4. Hence a.c.c. if and only if d.c.c. for A. □

6.2 Noetherian rings

Proposition 6.2.1. *If A is Noetherian and ϕ is a homomorphism of A onto a ring B, then B is Noetherian.*

Proof. This follows from the exact sequence of ϕ. □

Proposition 6.2.2. *Let A be a subring of B; suppose that A is Noetherian and that B is finitely generated as an A-module. Then B is Noetherian.*

Proof. By Proposition 6.1.7 B is Noetherian as an A-module, hence also as a B-module. □

Proposition 6.2.3. *In a noetherian ring A, every ideal $\mathfrak{a}$ contains a power of its radical.*

Proof. If $a_1, \ldots, a_n$ generate $\sqrt{\mathfrak{a}}$, then there exists an integer k such that for $a_n^k \in \mathfrak{a}$ for all i. Let $m = n(k-1)+1$, then $(\sqrt{\mathfrak{a}})^m$ is generated by the power products $\prod_i a_i^{\alpha_i}$, where $\sum_i \alpha_i = m$. Since $m > n(k-1)$, at least one of the exponents α_i is not less than k, and this proves that these products are in $\mathfrak{a}$, and therefore $\mathfrak{a}$ contains $(\sqrt{\mathfrak{a}})^m$. □

Corollary 6.2.4. *In a Noetherian ring A the nilradical $\mathfrak{n}(A)$ is nilpotent.*

Proposition 6.2.5. *If A is Noetherian and S is any multiplicatively closed subset of A, then $S^{-1}A$ is Noetherian.*

Proof. By Proposition 10.2.36 the ideals of $S^{-1}A$ are in one-to-one order-preserving correspondence with the contracted ideals of A, hence satisfy the maximal condition. □

Corollary 6.2.6. *If A is Noetherian and $\mathfrak{p}$ is a prime ideal of A, then $A_\mathfrak{p}$ is Noetherian.*

Now we prove the most important therorem concerning Noetherian rings.

Theorem 6.2.7 (Hilbert's Basis Theorem). *If A is Noetherian, then the polynomial ring $A[X]$ is Noetherian.*

Proof. We show that any ideal $I \subseteq A[X]$ is finitely generated. We inductively produce a set of generators f_i as follows.

For $n > 0$, if $I \neq (f_1, \ldots, f_{n-1})$, let f_n be any nonzero element of $I - (f_1, \ldots, f_{n-1})$ of lowest degree. Thus f_1 is any element of I of lowest degree, assuming $I \neq (0)$. If this procedure terminates, we are done. Otherwise, let $a_n \in A$ be the initial coefficient of f_n for $n > 0$. Then as A is Noetherian, there exists $N > 0$ such that $(a_1, \ldots, a_n) = (a_1, \ldots, a_{n+1})$ for all $n \geq N$. Say $a_{N+1} = \sum_{i=1}^N c_i a_i$. Then

$$f_{N+1} - \sum_{i=1}^N c_i f_i x^{\deg f_{N+1} - \deg f_N}$$

is an element of I that is nonzero (as $f_{N+1} \notin (f_1, \ldots, f_N)$), and of lower degree than f_{N+1}, yielding a contradiction. □

Corollary 6.2.8. *If A is Noetherian so is $A[X_1, \dots, X_n]$.*

Corollary 6.2.9. *Let B be a finitely-generated A-algebra. If A is Noetherian, then so is B.*

Proposition 6.2.10. *Let A be a Noetherian ring, then $A[[X]]$ is Noetherian.*

Proof. Set $B = A[[X]]$ and let $\mathfrak{a}$ be an ideal of B, we will prove that $\mathfrak{a}$ is finitely generated. Write $\mathfrak{a}(r)$ for the ideal of A formed by the leading coefficients a_r of $f = \sum_{i \geq r} a_i X^i$ as f runs through in $\mathfrak{a} \cap X^r B$, then we have

$$\mathfrak{a}(0) \subseteq \mathfrak{a}(1) \subseteq \mathfrak{a}(2) \subseteq \cdots$$

Since A is Noetherian, there exists $s > 0$ such that $\mathfrak{a}(i+1) = \mathfrak{a}(i)$ for $i \geq s$; moreover, each $\mathfrak{a}(i)$ is finitely generated. For each $0 \leq i \leq s$ we take finitely many elements $a_{i\nu} \in A$ generating $\mathfrak{a}(i)$, and choose $g_{i\nu} \in \mathfrak{b} \cap X^i B$ having $a_{i\nu}$ as the coefficient of X^i. These $g_{i\nu}$ then generate $\mathfrak{a}$. Indeed, for $f \in \mathfrak{a}$ we can take a linear combination g_0 of the $g_{0\nu}$ with coefficients in A such that $f - g_0 \in \mathfrak{a} \cap XB$, then proceed by induction to get

$$f - g_0 - g_1 - \cdots - g_s \in \mathfrak{a} \cap X^{s+1} B$$

Now $\mathfrak{a}(i+1) = \mathfrak{a}(i)$ for $i \geq s$, so we can take linear combinations $g_{s+i} \in X^i g_{s\nu}$ with coefficients in A such that

$$f - g_0 - g_1 - \cdots - g_s - g_{s+1} - \cdots - g_{s+i} \in \mathfrak{a} \cap X^{s+i+1} B.$$

Letting i tends to infinity, we then see f can be generated by the $g_{i\nu}$, whence the claim. □

6.3 Artin rings

Proposition 6.3.1. *An Artinian integral domain is a field.*

Proof. Let $x \neq 0$ in A, then we have a descending chain

$$(x) \supseteq (x^2) \supseteq \cdots$$

By the d.c.c. there is $n > 0$ such that $(x^n) = (x^{n+1})$, in particular we have $x^n = ax^{n+1}$ for some $a \in A$. Since A is an integral domain, we get $ax = 1$, so x is a unit. Hence A is a field. □

Proposition 6.3.2. *In an Artin ring A every prime ideal is maximal.*

Proof. Let $\mathfrak{p}$ be a prime ideal of A. Then $B = A/\mathfrak{p}$ is an Artinian integral domain, hence a field. □

Corollary 6.3.3. *In an Artin ring the nilradical is equal to the Jacobson radical.*

Proposition 6.3.4. *An Artin ring has only a finite number of maximal ideals.*

Proof. Consider the set of all finite intersections $\bigcap_{i=1}^n \mathfrak{m}_i$, where the $\mathfrak{m}_i$ are maximal ideals. This set has a minimal element, say $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$; hence for any maximal ideal $\mathfrak{m}$ we have

$$\mathfrak{m} \cap \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$$

, and therefore $\mathfrak{m} \supseteq \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$. By Proposition 10.1.5 $\mathfrak{m} \subseteq \mathfrak{m}_i$ for some i, hence $\mathfrak{m} = \mathfrak{m}_i$ since $\mathfrak{m}_i$ is maximal. □

Proposition 6.3.5. *In an Artin ring the nilradical is nilpotent.*

Proof. By d.c.c. we have $\mathfrak{n}(A)^k = I$ for k large enough. Suppose that $I \neq 0$, and let Σ denote the set of all ideals J such that $IJ \neq 0$. Then Σ is not empty, since $I \in \Sigma$. Let J_0 be a minimal element of Σ. Then we have $J_0 = (x)$, by the minimality of J_0. But

$$(xI)I = xI^2 = xI \neq 0$$

and $xI \subseteq (x)$, hence $xI = (x)$ (again by minimality). Hence $x = xy$ for some $y \in I$, and therefore

$$x = xy = \cdots = xy^n = \cdots = 0$$

since $y \in I = \mathfrak{n}(A)^k \subseteq \mathfrak{n}(A)$ is nilpotent. This contradicts the choice of x, so $I = 0$. □

By a **chain of prime ideals** of a ring A we mean a finite strictly increasing sequence

$$\mathfrak{p}_0 \supset \mathfrak{p}_1 \supset \cdots \supset \mathfrak{p}_n$$

the **length** of the chain is n. We define the dimension of A to be the supremum of the lengths of all chains of prime ideals in A: it is an integer ≥ 0, or $+\infty$ (assuming $A \neq 0$). A field has dimension 0; the ring $\mathbb{Z}$ has dimension 1.

Theorem 6.3.6. *A ring A is Artin if and only if A is Noetherian and* $\dim A = 0$.

Proof. Assume that A is Artinian. By Proposition 6.3.2, we have $\dim A = 0$. Let $\mathfrak{m}_i$ $(1 \leq i \leq n)$ be the distinct maximal ideals of A by Proposition 6.3.4. Then $\prod_{i=1}^n \mathfrak{m}_i^k \subseteq (\bigcap_{i=1}^n \mathfrak{m}_i)^k = \mathfrak{n}(A)^k = 0$. Hence by Corollary 6.1.13 A is Noetherian.

Conversely, assume that A is Noetherian and $\dim A = 0$. Then A has only a finite number of minimal prime ideals, and these are all maximal since $\dim A = 0$. Hence $\mathfrak{n}(A) = \bigcap_{i=1}^n \mathfrak{m}_i$ say; we have $\mathfrak{n}(A)^k = 0$ by Corollary 6.2.4, hence $\prod_{i=1}^n \mathfrak{m}_i^k = 0$ as in the previous part of the proof. Now by Corollary 6.1.13, A is an Artin ring. □

If A is an Artin local ring with maximal ideal $\mathfrak{m}$, then $\mathfrak{m}$ is the only prime ideal of A and therefore $\mathfrak{m}$ is the nilradical of A. Hence every element of $\mathfrak{m}$ is nilpotent, and $\mathfrak{m}$ itself is nilpotent. Every element of A is either a unit or is nilpotent. An example of such a ring is $\mathbb{Z}/p^n\mathbb{Z}$, where p is prime and $n \geq 1$.

Proposition 6.3.7. *Let A be a Noetherian local ring, $\mathfrak{m}$ its maximal ideal. Then exactly one of the following two statements is true:*

(a) $\mathfrak{m}^n \neq \mathfrak{m}^{n+1}$ *for all n.*

(b) $\mathfrak{m}^n = 0$ *for some n, in which case A is an Artin local ring.*

Proof. Suppose $\mathfrak{m}^n = \mathfrak{m}^{n+1}$ for some n. By Nakayama's lemma we have $\mathfrak{m}^n = 0$. Let $\mathfrak{p}$ be any prime ideal of A. Then $\mathfrak{m}^n \subseteq \mathfrak{p}$, hence (taking radicals) $\mathfrak{m} = \mathfrak{p}$. Hence $\mathfrak{m}$ is the only prime ideal of A and therefore A is Artinian. □

Theorem 6.3.8 (Structure theorem for Artin rings). *An Artin ring A is uniquely a finite direct product of Artin local rings.*

Proof. Let $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ be a complete list of distinct maximal ideals of A. From the proof of Theorem 6.3.6, we see $\prod_{i=1}^n \mathfrak{m}_i^k = \bigcap_{i=1}^n \mathfrak{m}_i^k = 0$ for some $k > 0$. By Proposition 10.1.24 the ideals $\mathfrak{m}_i^k$ are coprime in pairs, hence $\bigcap_{i=1}^n \mathfrak{m}_i^k = \prod_{i=1}^n \mathfrak{m}_i^k$ by Proposition 10.1.13. Consequently by Proposition 10.1.13 again the natural mapping $A \to \prod_{i=1}^n (A/\mathfrak{m}_i^k)$ is an isomorphism. Each $A/\mathfrak{m}_i^k$ is an Artin local ring, hence A is a direct product of Artin local rings.

Conversely, suppose $A \cong \prod_{i=1}^n A_i$, where the A_i are Artin local rings. Then for each i we have a natural surjective homomorphism (projection on the i-th factor) $\phi_i : A \to A_i$. Let $I_i = \ker \phi_i$. By Proposition 10.1.13 the I_i are pairwise coprime, and $\bigcap_{i=1}^n I_i = 0$. Let $\mathfrak{q}_i$ be the unique prime ideal of A_i, and let $\mathfrak{p}_i$ be its contraction $\mathfrak{p}_i = \phi_i^{-1}(\mathfrak{q}_i)$. The ideal $\mathfrak{p}_i$ is prime and therefore maximal by Proposition 6.3.2. Since $\mathfrak{q}_i$ is nilpotent it follows that I_i is $\mathfrak{p}_i$-primary, and hence $\bigcap_i I_i = (0)$ is a primary decomposition of the zero ideal in A. Since the I_i are pairwise coprime, so are the $\mathfrak{p}_i$, and they are therefore isolated prime ideals of (0). Hence all the primary components I_i are isolated, and therefore uniquely determined by A, by the second uniqueness theorem. Hence the rings $A_i \cong A/I_i$ are uniquely determined by A. □

Example 6.3.9. A ring with only one prime ideal need not be Noetherian (and hence not an Artin ring). Consider the ring

$$A = k[X_1, X_2, \cdots]/(X_1, X_2^2, \cdots)$$

it has only one prime ideal, namely the image of $(X_1, X_2, \cdots)$, hence is a local ring of dimension 0. But A is not Noetherian, for it is not difficult to see that its prime ideal is not finitely generated.

If A is a local ring, $\mathfrak{m}$ its maximal ideal, $k = A/\mathfrak{m}$ its residue field, the A-module $\mathfrak{m}/\mathfrak{m}^2$ is annihilated by $\mathfrak{m}$ and therefore has the structure of a k-vector space. If $\mathfrak{m}$ is finitely generated (e.g., if A is Noetherian), the images in $\mathfrak{m}/\mathfrak{m}^2$ of a set of generators of $\mathfrak{m}$ will span $\mathfrak{m}/\mathfrak{m}^2$ as a vector space. and therefore $\dim_k(\mathfrak{m}/\mathfrak{m}^2)$ is finite.

Proposition 6.3.10. *Let A be an Artin local ring. Then the following are equivalent:*

(a) every ideal in A is principal.

(b) the maximal ideal $\mathfrak{m}$ is principal.

(c) $\dim_k(\mathfrak{m}/\mathfrak{m}^2) \leq 1$.

Proof. The implications $(a) \Rightarrow (b) \Rightarrow (c)$ are clear. Now we show $(c) \Rightarrow (a)$. If $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 0$, then $\mathfrak{m} = \mathfrak{m}^2$, hence $\mathfrak{m} = 0$ by Nakayama's lemma, and therefore A is a field and there is nothing to prove. If $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 1$, then $\mathfrak{m}$ is a principal ideal by Proposition 7.1.5 (take $M = \mathfrak{m}$ there), say $\mathfrak{m} = (x)$. Let I be an ideal of A, other than (0) or (a). We have $\mathfrak{m} = J(A)$ hence $\mathfrak{m}$ is nilpotent by Proposition 6.3.5 and therefore there exists an integer r such that $I \subseteq \mathfrak{m}^r$, $I \not\subseteq \mathfrak{m}^{r+1}$; hence there exists $y \in I$ such that $y = ax^r$, $y \notin (x^{r+1})$; consequently $a \notin (x)$ and thus a is a unit in A. Hence $x^r \in I$, therefore $\mathfrak{m}^r = (x^r) \subseteq I$ and hence $I = \mathfrak{m}^r = (x^r)$. Hence I is principal. □

Example 6.3.11. The rings $\mathbb{Z}/(p^n)$ (p prime), $k[X]/(f^n)$ (f irreducible) satisfy the conditions of Proposition 6.3.10. On the other hand, the Artin local ring $k[X^2, X^3]/(X^4)$ does not: here $\mathfrak{m}$ is generated by X^2 and X^3 (mod X^4), so that $\mathfrak{m}^2 = 0$ and $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 2$.

6.4 Exercise

Exercise 6.4.1. Let A be a Noetherian ring and let $f = \sum_{n=1}^{\infty} a_n X^n \in A[[X]]$. Prove that f is nilpotent if and only if each a_n is nilpotent.

Proof. One direction is verified in Exercise 10.1.4. For the other, assume each a_n is nilpotent. Then by Corollary 6.2.4, there is $m > 0$ such that $(J(A))^m = 0$. This means the product $a_I = \prod_{i=1}^{m} a_{n_i} = 0$. In f^m, the coefficient of each term is divisible by some a_I, so $f^m = 0$. □

Exercise 6.4.2. Let A be a ring such that

(a) for each maximal ideal $\mathfrak{m}$ of A, the local ring $A_{\mathfrak{m}}$ is Noetherian.

(b) for each $x \neq 0$ in A, the set of maximal ideals of A which contain x is finite.

Show that A is Noetherian.

Proof. Let $I \subseteq A$ be an ideal. By (b) the set M of maximal ideals containing I is finite, say $M = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_r\}$. For each $\mathfrak{m}_i \in M$, the extension $A_{\mathfrak{m}_i} I$ of I in $A_{\mathfrak{m}_i}$ is finitely generated since (a) says $A_{\mathfrak{m}}$ is Noetherian. We may take $x_1, \ldots, x_t$ such that their image in each $A_{\mathfrak{m}_i}$ generate $A_{\mathfrak{m}_i} I$. Let $z \neq 0$ in I, and $M_z = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_{r+s}\}$ be the maximal ideals containing z. Then for each $\mathfrak{m}_{r+j}$, there is $y_j \in I$ such that $y_j \notin \mathfrak{m}_{r+j}$. Now let

$$I_0 = (z, x_1, \ldots, x_t, y_1, \ldots, y_j)$$

Now for any maximal ideal $\mathfrak{m}$,

- If $\mathfrak{m} \in M$, by construction we have $S^{-1} I_0 = S^{-1} I$.
- If $\mathfrak{m} \notin M_z$, we have $z \in A - \mathfrak{m}$, so $S^{-1} I = S^{-1} I_0 = (a)$.
- If $\mathfrak{n} \in M_z - M$, then there is $y_j \in A - \mathfrak{n}$, hence $S^{-1} I_0$. Also, $\mathfrak{m} \notin M$, so $I \cap A - \mathfrak{m} \neq \varnothing$ so $S^{-1} I = (a)$.

Hence I and I_0 have the same extension in $A_{\mathfrak{m}}$ for every maximal ideal $\mathfrak{m}$, by Corollary 10.3.20 the map $I_0 \to I$ is surjective, so I is finitely generated. □

Exercise 6.4.3. Let A be a Noetherian local ring, $\mathfrak{m}$ its maximal ideal and k its residue field, and let M be a finitely generated A-module. Then the following are equivalent:

(a) M is free.

(b) M is flat.

(c) The mapping of $\mathfrak{m} \otimes_A M$ into $A \otimes_A M$ is injective.

(d) $\mathrm{Tor}_1^A(k, M) = 0$.

Proof. To see the implication $(b) \Rightarrow (c)$, consider the exact sequence

$$0 \longrightarrow \mathfrak{m} \longrightarrow A \longrightarrow k \longrightarrow 0$$

Tensoring with M gives a short exact sequence, if M is flat.

Now the equivalence $(c) \Leftrightarrow (d)$ comes from the exact sequence

$$0 \longrightarrow \mathrm{Tor}_1^A(k, M) \longrightarrow \mathfrak{m} \otimes_A M \longrightarrow A \otimes_A M \longrightarrow k \otimes_A M \longrightarrow 0$$

Hence we only need to show $(d) \Rightarrow (a)$. Since M is finitely generated, there are $x_1, \ldots, x_n \in M$ whose image in $M/\mathfrak{m}M$ forms a basis. By Proposition 7.1.5, they also generate M. Now consider the exact sequence

$$0 \longrightarrow K \longrightarrow A^n \xrightarrow{\phi} M \longrightarrow 0$$

where $K := \ker \phi$. Tensoring with k gives

$$0 \longrightarrow k \otimes_A K \longrightarrow k \otimes_A A^n \longrightarrow k \otimes M \longrightarrow 0$$

since $\mathrm{Tor}_1^A(k, M) = 0$. Then since $x_1, \ldots, x_n$ is a basis, the map $1 \otimes \phi$ is an isomorphism, so $k \otimes_A K = 0$. Since A is Noetherian, K is finitely generated. Also, $k \otimes_A K = K/\mathfrak{m}K = 0$, and by Nakayama's lemma we conclude $K = 0$, so M is free. □

Exercise 6.4.4. Let A be a Noetherian ring, M a finitely generated A-module. Then the following are equivalent:

(a) M is a free A-module.

(b) $M_{\mathfrak{p}}$ is a free $A_{\mathfrak{p}}$-module, for all prime ideals $\mathfrak{p}$.

(c) $M_{\mathfrak{m}}$ is a free $A_{\mathfrak{m}}$-module, for all maximal ideals $\mathfrak{m}$.

In other words, flat = locally free.

Proof. By Proposition 10.3.24, and note that $A_{\mathfrak{p}}$ is a Noetherian ocal ring by Proposition 6.2.5. Hence the claim follows from Exercise 6.4.3. □

Exercise 6.4.5. Let $(0) = \bigcap_{i=1}^n \mathfrak{q}_i$ be a reduced primary decomposition of the zero ideal in a Noetherian ring, and let $\mathfrak{q}_i$ be $\mathfrak{p}_i$-primary. Let $\mathfrak{p}_i^{(r)}$ be the r-th **symbolic power** of $\mathfrak{p}_i$ (that is, the saturation of $\mathfrak{p}_i^r$ with respect to $\mathfrak{p}_i$). Show that for each $1 \le i \le n$ there exists an integer r_i such that $\mathfrak{p}_i^{(r_i)} \subseteq \mathfrak{q}_i$.

Suppose $\mathfrak{q}_i$ is an isolated primary component. Then $A_{\mathfrak{p}_i}$ is an Artin local ring, hence if $\mathfrak{m}$ is its maximal ideal we have $\mathfrak{m}^r = 0$ for all sufficiently large r, hence $\mathfrak{q}_i = \mathfrak{p}_i^{(r)}$ for all large r.

If $\mathfrak{q}_i$ is an embedded primary component, then $A_{\mathfrak{p}_i}$ is not Artinian, hence the powers $\mathfrak{m}^r$ are all distinct, and so the $\mathfrak{p}_i^{(r)}$ are all distinct. Hence in the given primary decomposition we can replace $\mathfrak{q}_i$ by any of the infinite set of $\mathfrak{p}_i$-primary ideals $\mathfrak{p}_i^{(r_i)}$ where $r \ge r_i$ and so there are infinitely many reduced primary decompositions of 0 which differ only in the $\mathfrak{p}_i$-component.

Proof. By Proposition 6.2.3 for each $\mathfrak{p}_i$ there is r_i such that $\mathfrak{p}_i^{r_i} \subseteq \mathfrak{q}_i \subseteq \mathfrak{p}_i$. Then

$$\mathfrak{p}_i^{(r_i)} = S_{\mathfrak{p}_i}(\mathfrak{p}_i^{r_i}) \subseteq S_{\mathfrak{p}_i}(\mathfrak{q}_i) = \mathfrak{q}_i$$

where we use $S_{\mathfrak{p}_i}(\mathfrak{q}_i) = \mathfrak{q}_i$ by Proposition 12.2.4. This proves the first claim.

If $\mathfrak{p}_i$ is isolated, since the isolated ideal of (0) is minimal in A, $A_{\mathfrak{p}_i}$ contains exactly one prime ideal $\mathfrak{m}$, hence is an Artin local ring. Since $\mathfrak{m} = \mathfrak{n}(A_{\mathfrak{p}_i})$, by Proposition 6.3.5 $\mathfrak{m}^k = 0$ for some $k > 0$. Also, for $r \geq r_i$ the intersection

$$\mathfrak{p}_i^{(r)} \cap \bigcap_{j \neq i} \mathfrak{q}_j \subseteq \mathfrak{p}_i^{(r_i)} \cap \bigcap_{j \neq i} \mathfrak{q}_j \subseteq \bigcap_{i=1}^{n} \mathfrak{q}_i = (0)$$

gives another primary decomposition of (0), since by Proposition 12.2.10 the isolated primary component is unique, we conclude $\mathfrak{p}_i^{(r)} = \mathfrak{q}_i$ for $r \geq r_i$.

If $\mathfrak{p}_i$ is embedded, we have $\mathfrak{p}_j \subset \mathfrak{p}_i$ for another $j \neq i$, hence we have the chain $\mathfrak{p}_j A_{\mathfrak{p}_i} \subseteq \mathfrak{p}_i A_{\mathfrak{p}_i}$ in $A_{\mathfrak{p}_i}$. It follows that $A_{\mathfrak{p}_i}$ is not an Artin ring, hence by Proposition 6.3.7 the powers $\mathfrak{m}^r$ are all distinct. Now if $\mathfrak{p}_i^r = \mathfrak{p}_i^s$ for $r \neq s$, then $\mathfrak{p}_i^r A_{\mathfrak{p}_i} = \mathfrak{m}^r = \mathfrak{p}_i^s A_{\mathfrak{p}_i} = \mathfrak{m}^s$, contradiction. Hence the powers $\mathfrak{p}_i^r$ are also distince. Also, note that

$$(\mathfrak{p}_i^{(r)})^e = (\mathfrak{p}_i^r)^{ece} = (\mathfrak{p}_i^r)^e = \mathfrak{m}^r$$

so if $\mathfrak{p}_i^{(r)} = \mathfrak{p}_i^{(s)}$, then $\mathfrak{m}^r = \mathfrak{m}^s$ and hence $r = s$. This implies all $\mathfrak{p}_i^{(r)}$ are distinct. If $r \geq r_i$, then the intersection

$$\mathfrak{p}_i^{(r_i)} \cap \bigcap_{j \neq i} \mathfrak{q}_j \subseteq \bigcap_{i=1}^{n} \mathfrak{q}_i = (0)$$

gives another primary decomposition of (0). Since $\mathfrak{p}_i^{(r)}$ are distinct, these are distince primary decomposition of (0), infinitely many, all minimal. □

Exercise 6.4.6. Let A be a Noetherian ring. Prove that the following are equivalent:

(a) A is Artinian.

(b) $\operatorname{Spec}(A)$ is discrete and finite.

(c) $\operatorname{Spec}(A)$ is discrete.

Proof. If A is Artinian, then every prime ideal is maximal, so $\operatorname{Spec}(A)$ is discrete. If $\operatorname{Spec}(A)$ is discrete, then $\dim A = 0$, hence A is Artinian. □

Exercise 6.4.7. Let k be a field and A a finitely generated k-algebra. Prove that the following are equivalent:

(a) A is Artinian.

(b) A is a finite k-algebra.

Proof. Assume A is Artin, then A is a direct product of Artin local rings, hence we can assume A is an Artin local ring. Let $\mathfrak{m}$ be the maximal ideal in A, then $A/\mathfrak{m}$ is a field, hence is finite by Zariski's Lemma. Now A is Noetherian and Artinain, so A has a composition series

$$A = M_0 \supset M_1 \supset \cdots \supset M_n = 0$$

where each quotient $M_{i-1}/M_i \cong A/\mathfrak{p}$ for a prime ideal in A. Since A is local, $M_{i-1}/M_i \cong A/\mathfrak{m}$ is finite, hence by induction A is finite.

If A is finite, observe that the ideals of A are k-vector subspaces and therefore satisfy d.c.c. □

Exercise 6.4.8. Let $\rho : A \to B$ be a ring homomorphism of finite type. Consider the following statements:

(a) ρ is finite.

(b) the fibres of ${}^a\rho$ are discrete subspaces of $\mathrm{Spec}(B)$.

(c) for each prime ideal $\mathfrak{p}$ of A, the ring $B \otimes_A k(\mathfrak{p})$ is a finite $k(\mathfrak{p})$-algebra.

(d) the fibres of ${}^a\rho$ are finite.

Prove that (a)⇒(b)⇔(c)⇒(d).

Proof. We first observe that

$$C := B \otimes_A k(\mathfrak{p}) = B \otimes_A (A_\mathfrak{p} \otimes_{A_\mathfrak{p}} k(\mathfrak{p})) = (B \otimes_A A_\mathfrak{p}) \otimes_{A_\mathfrak{p}} k(\mathfrak{p})$$

and that $\rho^{*-1}(\mathfrak{p}) = \mathrm{Spec}(B \otimes_A k(\mathfrak{p}))$. Therefore, in view of Exercise 6.4.7 and Exercise 6.4.6, we see (b) is equivalent to (c).

Now if ρ is finite, then B is a finite algebra. Thus C is a finite dimensional $k(\mathfrak{p})$-vector space. Finally, by Exercise 6.4.7, C is Artinian iff it is finite, and Exercise 6.4.6 says $\mathrm{Spec}(C)$ is finite if this holds. □

Exercise 6.4.9. Let A be a Noetherian ring and $\mathfrak{q}$ a $\mathfrak{p}$-primary ideal in A. Consider chains of primary ideals from $\mathfrak{q}$ to $\mathfrak{p}$. Show that all such chains are of finite bounded length, and that all maximal chains have the same length.

Proof. Since we are interested in ideals between $\mathfrak{q}$ and $\mathfrak{p}$, let $B = (A/\mathfrak{q})_{\mathfrak{p}/\mathfrak{q}}$. Then ideals in B are those in between, while extension and contradction preserves primarity. Also, note that since A is Noetherian, there is $n > 0$ such that $\mathfrak{p}^n \subseteq \mathfrak{q}$, hence $\mathfrak{m}^r = 0$ in B where $\mathfrak{m}$ is the unique maximal ideal in B. Thus, by Proposition 6.3.7 B is an Artin local ring. Also, for any ideal $\mathfrak{b}$ in B we have $\mathfrak{m}^n \subseteq \mathfrak{b} \subseteq \mathfrak{m}$, so $\mathfrak{b}$ is $\mathfrak{m}$-primary.

Thus our question boils down to arbitrary chains of ideals in an Artinian ring B. By the a.c.c. and d.c.c., these must all have finite length. A maximal chain is a composition series, and these all have the same length. □

Chapter 7

Linear algebras

In this section all rings are assumed to be commutative with unit. Let M be an A-module and let $(M_i)_{i\in I}$ be a family of submodules of M. Their sum $\sum M_i$ is the set of all (finite) sums $\sum_i x_i$ where $x_i \in M_i$ for all $i \in I$, and almost all the x. (that is, all but a finite number) are zero. $\sum_i M_i$ is the smallest submodule of M which contains all the M_i.

The intersection $\bigcap_i M_i$ is again a submodule of M. Thus the submodules of M form a complete lattice with respect to inclusion. We cannot in general define the **product** of two submodules, but we can define the product IM, where I is an ideal and M an A-module; it is the set of all finite sums $\sum_i a_i x_i$ with $a_i \in I$, $x_i \in M$, and is a submodule of M.

If N, P are submodules of M, we define $(N : P)$ to be the set of all $a \in A$ such that $aP \subseteq N$; it is an ideal of A. In particular, $(0 : M)$ is the set of all $a \in A$ such that $aM = 0$; this ideal is called the **annihilator** of M and is also denoted by $\mathrm{Ann}(M)$.

If $I \subseteq \mathrm{Ann}(M)$, we may regard M as an A/I-module, as follows: if $\bar{x} \in A/I$ is represented by $x \in A$, define $\bar{x} \cdot m$ to be xm $(m \in M)$: this is independent of the choice of the representative x of $\bar{x}$, since $IM = 0$.

An A-module is **faithful** if $\mathrm{Ann}(M) = 0$. If $\mathrm{Ann}(M) = I$, then M is faithful as an A/I-module. If x is an element of M, the set of all multiples $ax (a \in A)$ is a submodule of M, denoted by Ax or (x). If $M = \sum_{i\in I} Ax_i$ then x_i are said to be a set of generators of M; this means that every element of M can be expressed (not necessarily uniquely) as a finite linear combination of the x_i with coefficients in A. An A-module M is said to be finitely generated if it has a finite set of generators.

7.1 Modules and diagrams

7.1.1 Finitely generated modules

Proposition 7.1.1. *Let M be a finitely generated A-module, let I be an ideal of A, and let ϕ be an A-module endomorphism of M such that $\phi(M) \subseteq IM$. Then ϕ satisfies an equation of the form*

$$\phi^n + a_1\phi^{n-1} + \cdots + a_n = 0$$

where $a_i \in I$.

Proof. Let $x_1, \ldots, x_n$ be a set of generators of M. Then each $\phi(x_i) \in IM$, so that we have say

$$\phi(x_i) = \sum_{i=1}^{n} a_i^j x_j$$

where $a_i^j \in I$. Then let $T = [a_j^i]$, we see

$$\phi(x) = Tx.$$

Let $f(\lambda)$ be the characteristic polynomial of T, we see $f(\phi) = 0$. □

Corollary 7.1.2. *Let M be a finitely generated A-module and let I be an ideal of A such that $IM = M$. Then there exists $x \equiv 1$ mod I such that $xM = 0$.*

Proof. Take $\phi =$ identity, $x = 1 + a_1 + \cdots + a_n$ in Proposition 7.1.1. □

Proposition 7.1.3 (Nakayama's lemma). *Let M be a finitely generated A-module and I an ideal of A contained in the Jacobson radical of A. Then $IM = M$ if and only if $M = 0$.*

Proof. First Proof. By Corollary 7.1.2 we have $xM = 0$ for some $x \equiv 1$ mod $\mathfrak{r}(A)$. By Proposition 10.1.10 x is a unit in A, hence $M = x^{-1}xM = 0$.

Second Proof. Suppose $M \neq 0$, and let $u_1, \ldots, u_n$ be a minimal set of generators of M. Then $u_n \in IM$, hence we have an equation of the form

$$u_n = a_1 u_1 + \cdots + a_n u_n$$

with the $a_i \in I$. Hence

$$(1 - a_n)u_n = a_1 u_1 + \cdots + a_{n-1} u_{n-1}$$

since $a_n \in \mathfrak{r}(A)$, it follows that $1 - a_n$ is a unit in A. Hence u_n belongs to the submodule of M generated by $u_1, \ldots, u_{n-1}$, contradiction. □

Corollary 7.1.4. *Let M be a finitely generated A-module, N a submodule of M, I an ideal of A contained in the Jacobson radical of A. Then $M = IM + N$ if and only if $M = N$.*

Proof. Apply Proposition 7.1.3 to M/N, observing that $I(M/N) = M/N$. □

Let A be a local ring, $\mathfrak{m}$ its maximal ideal, $k = A/\mathfrak{m}$ its residue field. Let M be a finitely generated A-module. $M/\mathfrak{m}M$ is annihilated by $\mathfrak{m}$, hence is naturally an $A/\mathfrak{m}$-module, i.e., a k-vector space, and as such is finite-dimensional.

Proposition 7.1.5. *Let $x_1, \ldots, x_n$ be elements of M whose images in $M/\mathfrak{m}M$ form a basis of this vector space. Then the x_i generate M.*

Proof. Let N be the submodule of M generated by the x_i. Then the composite map

$$N \to M \to M/\mathfrak{m}M$$

maps N onto $M/\mathfrak{m}M$, hence $N + \mathfrak{m}M = M$, hence $N = M$ by Corollary 7.1.4. □

Proposition 7.1.6. *Let A be a local ring, and let M be a* ***direct summand*** *of a finitely generated free A-module: that is, there exists an A-module N such that $M \oplus N$ is a free A-module. Then M is free.*

Proof. Choose elements $m_1, \ldots, m_r \in M$ whose cosets mod $\mathfrak{m}M$ are a basis of $M/\mathfrak{m}M$ as a vector space over the field $A/\mathfrak{m}$. By Nakayama's lemma, M is generated by $m_1, \ldots, m_r$. Since M is a direct summand of a free module, it is projective. For the epimorphism $\pi : A^r \to M$ induced by the m_i, we get an lift $\psi : M \to A^r$ such that $\pi \circ \psi = \mathrm{id}_M$. This means π splits, so $A^r \cong M \oplus K$, where $K := \ker \pi$. Tensoring this with $A/\mathfrak{m}$, we get $K/\mathfrak{m}K = 0$. On the other hand, K is a quotient of A^r, hence is finitely generated. Then by Nakayama's lemma, $K = 0$. Hence M is free. □

7.1.2 Exact sequence and the snake lemma

Proposition 7.1.7. *Let* $L \xrightarrow{\alpha} M \xrightarrow{\beta} N \longrightarrow 0$ *be a sequence of A-modules. Then this sequence is exact if and only if for all A-modules Q, the sequence*

$$0 \longrightarrow \mathrm{Hom}(N, Q) \xrightarrow{\beta^*} \mathrm{Hom}(M, Q) \xrightarrow{\alpha^*} \mathrm{Hom}(L, Q)$$

is exact.

Proof. The nontrivial case is the only if part. So suppose that the second sequence

$$0 \longrightarrow \mathrm{Hom}(N, Q) \xrightarrow{\beta^*} \mathrm{Hom}(M, Q) \xrightarrow{\alpha^*} \mathrm{Hom}(L, Q)$$

is exact for all Q. We need to show the following is exact:

$$L \xrightarrow{\alpha} M \xrightarrow{\beta} N \longrightarrow 0$$

First of all, to show β is surjective. Let $Q = N/\mathrm{im}\,\beta$, and consider the projection $\phi : N \to N/\mathrm{im}\,\beta$. Note that

$$\beta^*(\phi) = \phi \circ \beta = 0.$$

Since β^* is injective, $\phi = 0$ must be the case, and hence $\mathrm{im}\,\beta = N$, β is surjective.

For $\alpha^* \circ \beta^* = (\beta \circ \alpha)^* = 0$. Let $Q = N$ and choose $id : N \to N$. Then we can see

$$\alpha^* \circ \beta^*(id) = id \circ \beta \circ \alpha = 0.$$

so $\beta \circ \alpha = 0$, $\mathrm{im}\,\alpha \subseteq \ker \beta$.

Now take $Q = M/\mathrm{im}\,\alpha$, and let $\phi : M \to N$ be the projection. Then $\alpha^*(\phi) = \phi \circ \alpha = 0$, hence by the exactness, $\phi = \beta^*(\psi) = \psi \circ \beta$ for some $\psi : N \to M/\mathrm{im}\,\alpha$. Consequenctly $\mathrm{im}\,\alpha = \ker \phi \supseteq \ker \beta$. Hence we are done. □

Similarly, we can get the following result for the functor $\mathrm{Hom}(Q, -)$.

Proposition 7.1.8. *Let* $0 \longrightarrow L \xrightarrow{\alpha} M \xrightarrow{\beta} N$ *be a sequence of A-modules and homomorphisms. Then this sequence is exact if and only if for all A-modules M, the sequence*

$$0 \longrightarrow \mathrm{Hom}(Q, L) \xrightarrow{\alpha_*} \mathrm{Hom}(Q, M) \xrightarrow{\beta_*} \mathrm{Hom}(Q, N)$$

is exact.

A particular case of short exact sequence arises by considering the second projection from a direct sum: $M_1 \oplus M_2 \to M_2$; there is then an exact sequence

$$0 \longrightarrow M_1 \longrightarrow M_1 \oplus M_2 \longrightarrow M_2 \longrightarrow 0$$

These short exact sequences are said to **split**; more generally, a short exact sequence

$$0 \longrightarrow M_1 \longrightarrow N \longrightarrow M_2 \longrightarrow 0$$

is said to be exact if it is isomorphic to one of these sequences in the sense that there is a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & M_1 \arrow[r] \arrow[d, "\sim"] & N \arrow[r] \arrow[d, "\sim"] & M_2 \arrow[r] \arrow[d, "\sim"] & 0 \\
0 \arrow[r] & M_1' \arrow[r] & M_1' \oplus M_2' \arrow[r] & M_2' \arrow[r] & 0
\end{tikzcd}$$

Theorem 7.1.9. *Let $\varphi : M \to N$ be an A-module homomorphism. Then*

- *φ has a left-inverse if and only if the sequence*

$$0 \longrightarrow M \xrightarrow{\varphi} N \longrightarrow \operatorname{coker} \varphi \longrightarrow 0$$

  splits.

- *φ has a right-inverse if and only if the sequence*

$$0 \longrightarrow \ker \varphi \longrightarrow M \xrightarrow{\varphi} N \longrightarrow 0$$

  splits.

Proof. If the sequence splits, then φ may be identified with the embedding of M into a direct sum $M \oplus M'$, and the projection $M \oplus M' \to M$ gives a left-inverse of φ. Conversely, assume that φ has a left-inverse ψ:

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r, "\varphi"] \arrow[dr, "\mathrm{id}"'] & N \arrow[d, "\psi"] \\
 & & M
\end{tikzcd}$$

Then we claim that N is isomorphic to $M \oplus \ker \psi$ and that φ corresponds to the identification of M with the first factor: $M \to M \oplus \ker \psi \simeq N$. The isomorphism $M \oplus \ker \psi \to N$ is given by

$$(m, k) \mapsto \varphi(m) + k$$

its inverse $N \to M \oplus \ker \psi$ is

$$n \mapsto (\psi(n), n - \varphi \circ \psi(n))$$

The element $n - \varphi \circ \psi(n)$ is in $\ker \psi$ as it should be, since

$$\psi(n - \varphi \circ \psi(n)) = \psi(n) - \psi \circ \varphi \circ \psi(n) = \psi(n) - \psi(n) = 0.$$

However, if φ has an right-inverse

$$\begin{tikzcd} M \arrow[r, "\varphi"] & N \arrow[r] & 0 \\ N \arrow[u, "\psi"] \arrow[ur, "\mathrm{id}"'] & & \end{tikzcd}$$

Then the isomorphism $N \times \ker \varphi \to M$ becomes

$$(n, k) \mapsto \psi(n) + k$$

with the inverse $M \to N \times \ker \varphi$ being

$$m \mapsto (\varphi(m), m - \psi \circ \varphi(m))$$

This completes the proof. □

Lemma 7.1.10 (snake lemma). *If given a **snake diagram** as follows*

$$\begin{tikzcd} & A \arrow[r, "f"] \arrow[d, "\alpha"] & B \arrow[r, "g"] \arrow[d, "\beta"] & C \arrow[r] \arrow[d, "\gamma"] & 0 \\ 0 \arrow[r] & A' \arrow[r, "f'"'] & B' \arrow[r, "g'"'] & C' & \end{tikzcd}$$

where the two rows are exact. Then there is an homomorphism $\delta : \ker \gamma \to \operatorname{coker} \alpha$ such that the follows diagram commutes

$$\begin{tikzcd} 0 \arrow[r] & \ker f \arrow[r] & \ker \alpha \arrow[r] \arrow[d] & \ker \beta \arrow[r] \arrow[d] & \ker \gamma \arrow[d] \arrow[dddll, red, "\delta"] & & \\ & & A \arrow[r, blue, "f"] \arrow[d, blue, "\alpha"] & B \arrow[r, blue, "g"] \arrow[d, blue, "\beta"] & C \arrow[r, blue] \arrow[d, blue, "\gamma"] & 0 & \\ & 0 \arrow[r, blue] & A' \arrow[r, blue, "f'"'] \arrow[d] & B' \arrow[r, blue, "g'"'] \arrow[d] & C' \arrow[d] & & \\ & & \operatorname{coker} \alpha \arrow[r] & \operatorname{coker} \beta \arrow[r] & \operatorname{coker} \gamma \arrow[r] & \operatorname{coker} g' \arrow[r] & 0 \end{tikzcd}$$

*the homomorphism δ is called the **connection homomorphism**.*

Proof. First, let $c \in \ker \gamma$, We can construct elements of A' as follows. Since g is surjective, there exists an element $b \in B$ such that $g(b) = c$. We now move vertically down by β, and take $\beta(b)$. The commutativity $\gamma \circ g = g' \circ \beta$ shows that

$$g'(\beta(b)) = \gamma(g(b)) = \gamma(c) = 0$$

whence $\beta(b)$ is in the kernel of g' in B'. By exactness, there exists an element $a' \in A'$ such that $f'(a) = \beta(b)$. We map a into $\operatorname{coker} \alpha$ by the canonical projection, and still denote it by a.

In brief, we write

$$\delta(c) = a = f'^{-1} \circ \beta \circ g^{-1}(c)$$

$$\begin{tikzcd}
 & & c \arrow[d] \\
 & b \arrow[r, "g"] \arrow[d, "\beta"] & c \arrow[d, dashed, "\gamma"] \\
a \arrow[r, "f'"] \arrow[d] & \beta(b) \arrow[r, dashed, "g'"] & 0 \\
a & &
\end{tikzcd}$$

We now verify that δ is well defined. First, f' is injective by exactness, a is uniquely determined by $\beta(b)$, hence by b. So the only verification is for b.

Suppose we choose a different b' mapping to the same c: $g(b') = c = g(b)$. Then $b' - b \in \ker g$, and by exactness, $\operatorname{im} f = \ker g$, so there is $\ell \in A$ such that $\alpha(\ell) = b' - b$. It follows from the commutativity that

$$\beta(b' - b) = \beta(f(b' - b)) = f'(\alpha(\ell))$$

Following our construction, $f'^{-1}(\beta(b' - b)) = \alpha(\ell)$. But since the column is exact, the projection into $\operatorname{coker} \alpha$ kills $\alpha(\ell)$, hence taking b' makes no difference to $\delta(c)$, that is, δ is well defined.

$$\begin{tikzcd}
\ell \arrow[r, "f"] \arrow[d, "\alpha"] & b' - b \arrow[r, "g"] \arrow[d, "\beta"] & 0 \\
\alpha(\ell) \arrow[r, "f'"] \arrow[d] & \beta(b' - b) & \\
0 & &
\end{tikzcd}$$

Now we need to verify the exactness of the sequence. First we give the morphisms in the sequence

$$0 \to \ker f \xrightarrow{i} \ker \alpha \xrightarrow{f_*} \ker \beta \xrightarrow{g_*} \ker \gamma \xrightarrow{\delta} \operatorname{coker} \alpha \xrightarrow{f'_*} \operatorname{coker} \beta \xrightarrow{g'_*} \operatorname{coker} \gamma \xrightarrow{j} \operatorname{coker} g' \to 0$$

We just define $f_* := f|_{\ker \alpha}$, and similar for g_*, f'_*, g'_*. If $a \in \ker f$, then $f'(\alpha(a)) = 0$ by commutativity, and $\alpha(a) = 0$ by injectvity of f'. This gives an inclusion $\ker f \to \ker \alpha$, which is our i. Similarly, if $c \in \operatorname{im} \gamma$, then there is an element $b \in B$ such that $\gamma(g(b)) = c$ by the surjectivity of g. Then we see $c = g'(\beta(b))$ by commutativity, hence $c \in \operatorname{im} g'$. This gives $\operatorname{im} \gamma \subseteq \operatorname{im} g'$, and we have an induced quotient map $\operatorname{coker} \gamma \to \operatorname{coker} g'$. This is our j. By our definition, the exactness of two ends follows, now we begin to verify the rest.

Since $\ker f \subseteq \ker \alpha$, by our definition of f_*, the exactness at $\ker \alpha$ follows. Similar for the exactness of $\operatorname{coker} \gamma$. Since the top row is exact, $\operatorname{im}(f) = \ker(g)$. Ii follows that $g_* \circ f_* = 0$, so $\operatorname{im} f_* \subseteq \ker g_*$. To verify the converse, assume $b \in \ker g_*$, that is, $b \in \ker \beta$ and $g(b) = 0$. By exactness of B, there is $a \in A$ such that $f(a) = b$. We show that $a \in \ker \alpha$: in fact,

$$f'(\alpha(a)) = \beta(f(a)) = \beta(b) = 0$$

Since f' is injective, this means $\alpha(a) = 0$, so $a \in \ker \alpha$. Thus $\ker g_* = \operatorname{im} f_*$, giving the exactness

at $\ker\beta$.

The exactness at $\operatorname{coker}\beta$ arises similarly. Assume $b' + \operatorname{im}\beta \in \ker g'_*$, then $g'(b') \in \operatorname{im}\gamma$. By the surjectivity of g, $\exists b \in B$ such that $g'(b') = \gamma(g(b)) = g'(\beta(b))$. Then $b' = \beta(b) + x$ with $x \in \ker g'$. By exactness, $x = f'(a')$ for some $a' \in A'$. Then it follows

$$b' + \operatorname{im}\gamma = \beta(b) + f'(a') + \operatorname{im}\beta = f'(a')$$

this shows $\ker g'_* \subseteq \operatorname{im} f'_*$, and the claim.

We verify the exactness about δ. First, let $c = g(b)$ for some $b \in \ker\beta$. Since $\beta(b) = 0$, by our definition of δ, $\delta(c) = f'^{-1}(\beta(b)) + \operatorname{im}\alpha = \operatorname{im}\alpha$. This gives $\operatorname{im} g_* \subseteq \ker\delta$. Conversely, if $\delta(c + \operatorname{im}\alpha) = \operatorname{im}\alpha$ for some $c \in C$, we get $\delta(c) \in \operatorname{im}\alpha$, hence $\delta(c) = \alpha(a)$ by some $a \in A$. By the construction of δ, choose some $b \in B$ such that $g(b) = c$, then $f'^{-1}(\beta(b)) = \delta(c) = \alpha(a)$. It follows that

$$\beta(b) = f'(\alpha(a)) = \beta(f(a))$$

and $b = f(a) + x$ for $x \in \ker\beta$. Applying g we get $c = g(b) = g(f(a)) + g(x) = g(x)$ since $g \circ f = 0$. Since $x \in \ker\beta$, $g_*(x) = g(x) = c$. This gives $\ker\delta \subseteq \operatorname{im} g_*$, giving the exactness at $\ker\gamma$. Finally, we deal with the exactness at $\operatorname{coker}\alpha$. Choose $a' + \operatorname{im}\alpha = \delta(c)$ for $c \in \ker\gamma$. Agian the definition of δ: $f'(a') = f'(\delta(c)) = \beta(b)$ for some $g(b) = c, b \in B$. This already gives

$$f'_*(a' + \operatorname{im}\alpha) = f'(\delta(c)) + \operatorname{im}\beta = \beta(b) + \operatorname{im}\beta = \operatorname{im}\beta$$

For the other direction, let $a' + \operatorname{im}\beta \in \ker f'_*$, that is, $f'(a') \in \operatorname{im}\beta$. So let $f'(a') = \beta(b), b \in B$, we observe that $a' = f'^{-1} \circ \beta(b) = f'^{-1} \circ \beta \circ g^{-1}(g(b)) = \delta(g(b))$. This gives $\ker f'_* \subseteq \operatorname{im}\delta$, finishing the proof. □

7.1.3 Exercise

Exercise 7.1.1. Let A be a local ring, and $f_1, \ldots, f_r \in A$ be elements in A generating a non-trivial ideal I of A. Suppose I is principal, show that $I = (f_i)$ for some f_i.

Proof. Let $I = (a)$ with $a \neq 0$ and $\mathfrak{m}$ the unique maximal ideal of A. Then for every f_i we have $f_i = k_i a$ for $k_i \in A$. Now consider the module $\mathfrak{m}I$: we have $\mathfrak{m}I \subseteq I$. If one of k_i is a unit, then $I = (a_i)$ and we are done. So we assume this is not the case. Then, each k_i is contained in $\mathfrak{m}$, and hence $f_i = k_i a$ is in $\mathfrak{m}I$, hence $I \subseteq \mathfrak{m}I$. Now we have $\mathfrak{m}I = I$, and by Nakayame's lemma we have $I = 0$, which is contradiction. □

Exercise 7.1.2. Let $A[X]$ be the ring of polynomials in one indeterminate over a ring A. Prove that $A[X]$ is a flat A-algebra.

Proof. We have

$$A[X] = \bigoplus_{i \in \mathbb{N}} (x^n)$$

Each (x^n) is free, hence flat, so $A[X]$ is flat. □

Exercise 7.1.3. For any A-module, let $M[X]$ denote the set of all polynomials in x with coefficients in M, prove that

$$A[X] \otimes_A M \cong (A \otimes_A M)[X] \cong M[X].$$

Exercise 7.1.4. Let

$$0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$$

be an exact sequence of A-modules. If L and N are finitely generated, then so is M.

Proof. We have $M \subseteq L + N$ if we identify this sequence as a projection. □

Exercise 7.1.5. If M is a finitely generated A-module and $f : M \to M$ is a surjective homomorphism, then f is an isomorphism.

Proof. Define a $A[X]$-module structure on M via $x \cdot m := f(m)$. Let $I := (x)$, we claim that $IM = M$: In fact, since f is surjective, for each $m \in M$ there is $n \in M$ such that $x \cdot n = f(n) = m$, so $m \in IM$. Now by Corollary 7.1.2 there exists $g \in I$ such that $(1 + g)M = 0$. By the definition of I, we can write $g(x) = xh(x)$.

Now we prove f is injective. Let $m \in M$ be such that $f(m) = 0$. Then

$$0 = (1 + xh(x)) \cdot m = m + h(x) \cdot f(m) = m + 0 = m.$$

This finishes the proof. □

Exercise 7.1.6. Let $\mathcal{M} = (M_i, \mu_i)$ be a directed system directed by some set I. We shall construct an A-module M called the direct limit of the direct system M. Let C be the direct sum of the M_i and identify each module M_i with its canonical image in C. Let D be the submodule of C generated by all elements of the form $x_i - \mu_{ij}(x_i)$ where $i \leq j$ and $x_i \in M_i$. Let $M = C/D$, let $\mu : C \to M$ be the projection and let μ_i be the restriction of μ to M_i. Then clearly $\mu_j = \mu_{ij}\mu_i$. Show that every element of $M = \varinjlim M_i$ can be written in the form $\mu_i(x_i)$ for some $i \in I$ and some $x_i \in M_i$. Show also that if $\mu_i(x_i) = 0$ then there exists $j \geq i$ such that $\mu_{ij}(x_i) = 0$ in M_j.

Proof. For the first claim, $x \in C$ has a representative of the form $x = \sum_{j \in J} x_j$ for some finite subset J. Then we can get $i \in I$ such that $i \geq j$ for all $j \in J$. So

$$x = \mu\Big(\sum_{j \in J} x_j\Big) = \sum_{j \in J} \mu_j(x_j) = \sum_{j \in J} \mu_i \mu_{ji}(x_j) = \mu_i\Big(\sum_{j \in J} \mu_{ji}(x_j)\Big)$$

Let $x_i = \sum \mu_{ji}(x_j)$ we get the claim.

For the second claim, suppose $\mu_i(x_i) = 0$ for some $i \in I$. Then, $x_i \in M_i \cap D$ is a finite sum

$$x_i = \sum_{\ell} (y_{j_\ell} - \mu_{j_\ell k_\ell}(y_{j_\ell}))$$

for some finite subset J of I, and $y_{j_\ell} \in M_{j_\ell}$ for each $j \in J$ with $j_\ell \leq k_\ell$. Now, there exists $l \in I$ such that $l \geq k_\ell$ for all $k_\ell \in J \cup \{i\}$. Let $\pi_a : x \to M_a$ be the projectin, then we have

$$\pi_a = \sum_{j_\ell = a} y_{j_\ell} - \sum_{k_\ell = a} \mu_{j_\ell k_\ell}(y_{j_\ell}).$$

Hence

$$\mu_{al}(\pi_a(x_i)) = \sum_{j_\ell = a} \mu_{al}(y_{j_\ell}) - \sum_{k_\ell = a} \mu_{j_\ell l}(y_{j_\ell})$$

It follows that

$$\begin{aligned}\sum_a \mu_{al}\pi_a(x_i) &= \sum_a \Big(\sum_{j_\ell=a} \mu_{al}(y_{j_\ell}) - \sum_{k_\ell=a} \mu_{j_\ell l}(y_{j_\ell})\Big) \\ &= \sum_\ell \sum_{a=j_\ell} \mu_{al}(y_{j_\ell}) - \sum_\ell \sum_{a=k_\ell} \mu_{j_\ell l}(y_{j_\ell}) \\ &= \sum_\ell \mu_{j_\ell l}(y_{j_\ell}) - \sum_\ell \mu_{j_\ell l}(y_{j_\ell}) = 0\end{aligned}$$

Since $x_i \in M_i$, the left sum is $\mu_{il}(x_i)$, and we get $\mu_{il}(x_i) = 0$. □

Exercise 7.1.7. Let I be a directed set, and let (A_i, α_{ij}), (B_i, β_{ij}), and (C_i, γ_{ij}) be direct systems of A-modules over I. If $r_i : A_i \to B_i$ and $s_i : B_i \to C_i$ are morphisms of direct systems, and if

$$0 \longrightarrow A_i \xrightarrow{r_i} B_i \xrightarrow{s_i} C_i \longrightarrow 0$$

is exact for each $i \in I$, then there is an exact sequence

$$0 \longrightarrow \varinjlim A_i \xrightarrow{r} \varinjlim B_i \xrightarrow{s} \varinjlim C_i \longrightarrow 0$$

where $r = \vec{r}_i$, $s = \vec{s}_i$. Consequently, filtered colimits commute with homology in A-Mod.

Proof. Since direct limit is a left adjoint functor, it is right-exact. Hence we only need to prove r is injective. Suppose that $r(x) = 0$, where $x \in \varinjlim A_i$. Since the index set I is directed, allows us to write $x = \alpha_i(a_i)$, where $\alpha_i : A_i \to \bigoplus A_i$ is projection, similar for β_i. Now, be definition we have

$$r(x) = \beta_i r_i(a_i).$$

so $\beta_i r_i(a_i) = 0$. By Exercise 7.1.6, there is a $j \geq i$ such that $\beta_i r_i(a_i) = \beta_{ij} r_i(a_i) = 0$. Since r_i is a map of direct systems, we have

$$r_j \alpha_{ij} = \beta_{ij} r_i$$

Thus $r_j \alpha_{ij}(a_i) = 0$, and by the injectivity of r_j, we conclude $\alpha_{ij}(a_i) = 0$, since we have

$$x = \alpha_i(a_i) = \alpha_j \alpha_{ij}(a_i)$$

we conclude $x = 0$. □

Exercise 7.1.8. Let $(M_i)_{i\in I}$ be a family of submodules of an A-module, such that for each pair of indices i, j in I there exists $k \in I$ such that $M_i + M_j \subseteq M_k$. Define $i \leq j$ to mean $M_i \subseteq M_j$ and let $\mu_{ij} : M_i \to M_j$ be the embedding of M_i in M_j. Show that

$$\varinjlim M_i = \sum M_i = \bigcup_i M_i.$$

In particular, any A-module is the direct limit of its finitely generated submodules.

Proof. We can easily check that $\bigcup_i M_i$ is a module and satisfies that universal property of $\varinjlim M_i$. And since it has the same discription as $\sum M_i$, we get the equality. □

Exercise 7.1.9. Let $\mathcal{M} = (M_i, \mu_{ij})$, $\mathcal{N} = (N_i, \nu_{ij})$ be direct systems of A-modules over the same directed set. Let M, N be the direct limits and $\mu_i : M \to M$, $\nu_i : N_i \to N$ the associated homomorphisms.

A homomorphism $\Phi : \mathcal{M} \to \mathcal{N}$ is by definition a family of A-module homomorphisms $\phi_i : M_i \to N_i$, such that $\phi_i \circ \mu_{ij} = \nu_{ij}$ whenever $i \leq j$. Show that Φ defines a unique homomorphism $\phi = \varinjlim \phi_i : M \to N$ such that $\phi \circ \mu_i = \nu_i$ for all $i \in I$.

Exercise 7.1.10. Consider a direct limit of rings $A = \varinjlim A_i$, prove that $\varinjlim A = 0$ if and only if $A_i = 0$ for some i.

Proof. If $A = 0$, then in particular $0 = 1$. By exercise 7.1.6, for fixed i, there exists $j \in I$ such that $\mu_{ij}(a) = 0$. Since μ_{ij} is also a ring homomorphism from A_i to A_j, this implies that $1 = 0$ in A_j and hence $A_j = 0$. □

Exercise 7.1.11. Let (A_i, μ_i) be a direct system of rings and let $\mathfrak{n}(A_i)$ be the nilradical of A_i. Show that $\varinjlim \mathfrak{n}(A_i)$ is the nilradical of $\varinjlim A_i$. If each A_i is an integral domain, then $\varinjlim A_i$ is an integral domain.

Proof. Let a be a nilpotent element of A. Then $\exists n \in \mathbb{N}$ such that $a^n = 0$. By Exercise 7.1.6, $a = \mu_i(x)$ thus $0 = a^n = \mu_i(x^n)$. By Exercise 7.1.6, $\mu_i(x^n) = 0$ implies $\exists j \geq i$ such that $\mu_{ij}(x^n) = 0$. Hence, $\mu_{ij}(x)$ is in the nilradical of A_j, and

$$\mu_j(\mu_{ij}(x)) = \mu_i(x) = a$$

Hence $a \in \varinjlim \mathfrak{n}(A_i)$.

Conversely, if $a \in \varinjlim \mathfrak{n}(A_i)$, then by Exercise 7.1.6, there is $x_i \in M_i$ such that $\mu_i(x_i) = a$. Then

$$a^n = \mu_i(x_i^n) = 0$$

so there is $j \geq i$ such that $\mu_{ij}(x_i^n) = 0 = \mu_{ij}(x_i)^n$. This means $\mu_{ij}(x_i)$ is in $\mathfrak{n}(A_j)$. Since

$$\mu_j(\mu_{ij}(x_i)) = \mu_i(x) = a,$$

we see a is nilpotent in A. □

7.2 Flat modules

7.2.1 M-flat modules

Let A be a ring, E and M A-modules. Then E is said to be **flat for M** (or **M-flat**) if, for every A-module N and every injective homomorphism $\phi : M' \to M$, the homomorphism $1 \otimes v : E \otimes_A M' \to E \otimes_A M$ is injective.

Lemma 7.2.1. *For an A-module E to be M-flat, it is necessary and sufficient that for every finitely generated submodule N of M the canonical homomorphism $1 \otimes v : E \otimes_A N \to E \otimes_A M$ is injective.*

Proof. Suppose that this condition holds and let N be any submodule of M. Suppose that the canonical image in $E \otimes_A M$ of an element $z = \sum_i x_i \otimes y_i \in E \otimes M$ is zero and let M' be the finitely

generated submodule of N generated by the y_i. As by hypothesis the composition map

$$E \otimes_A M' \to E \otimes_A N \to E \otimes_A M$$

is injective, the sum $z' = \sum_i x_i \otimes y_i$ considered as an element of $E \otimes_A M'$, is zero. Since z is the image of z', we have $z = 0$, whence the lemma. □

Lemma 7.2.2. *Let E be an A-module and M an A-module such that E is M-flat. If N is either a submodule or a quotient module of M, then E is N-flat.*

Proof. The case in which N is a submodule is easy, as, if N' is a submodule of N, the composite homomorphism

$$E \otimes_A N' \to E \otimes_A N \to E \otimes_A M$$

is injective, hence so is $E \otimes_A N' \to E \otimes_A N$. Suppose then that N is a quotient module of M, that is there exists an exact sequence

$$0 \longrightarrow R \xrightarrow{i} M \xrightarrow{\pi} N \longrightarrow 0$$

Let N' be a submodule of N and $M' = \pi^{-1}(N')$. Let ι' denote the mapping of R to M' with the same graph as ι, π' the surjection $M' \to N'$ with the same graph as the restriction of π to M', and ϕ, ψ, γ the canonical injections. The the folloiwng diagram

$$\begin{tikzcd}
0 \arrow[r] & R \arrow[r, "\iota'"] \arrow[d, "\phi"] & M' \arrow[r, "\pi'"] \arrow[d, "\psi"] & N' \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & R \arrow[r, "\iota"] & M \arrow[r, "\pi"] & N \arrow[r] & 0
\end{tikzcd}$$

is commutative and its rows are exact. Tensoring with E, since E is M-flat, we get the following diagram

$$\begin{tikzcd}
 & E \otimes_A R \arrow[r, "1\otimes\iota'"] \arrow[d, "1\otimes\phi"] & E \otimes_A M' \arrow[r, "1\otimes\pi'"] \arrow[d, "1\otimes\psi"] & E \otimes_A N' \arrow[r] \arrow[d, "1\otimes\gamma"] & 0 \\
0 \arrow[r] & E \otimes_A R \arrow[r, "1\otimes\iota"] & E \otimes_A M \arrow[r, "1\otimes\pi"] & E \otimes_A N \arrow[r] & 0
\end{tikzcd}$$

with row exact. Now since $1 \otimes \phi$ is surjective and $1 \otimes \psi$ is injective, by snake lemma we see $1 \otimes \gamma$ is injective, whence the claim. □

Lemma 7.2.3. *Let $(M_i)_{i\in I}$ be a family of A-modules, $M = \bigoplus_i M_i$ their direct sum and E an A-module. If, for all $i \in I$, E is flat for M_i, then E is flat for M.*

Proof. Suppose first that $I = \{1, 2\}$, and let M' be a submodule of $M = M_1 \oplus M_2$, M_1 and M_2 being canonically identified with submodules of M. Denote by M_1' the intersection $M' \cap M_1$ and by M_2' the image of M' in M_2 under the canonical projection π of M onto M_2. We have a diagram

$$\begin{tikzcd}
0 \arrow[r] & M_1' \arrow[r, "\iota'"] \arrow[d, "\phi"] & M' \arrow[r, "\pi'"] \arrow[d, "\psi"] & M_2' \arrow[r] \arrow[d, "\eta"] & 0 \\
0 \arrow[r] & M_1 \arrow[r, "\iota"] & M \arrow[r, "\pi"] & M_2 \arrow[r] & 0
\end{tikzcd}$$

where ι, ι' are the canonical injections and π' is the mapping with the same graph as the restriction of π to M', which is surjective. It is immediately verified that this diagram is commutative

and that its rows are exact.

$$\begin{tikzcd}
 & E \otimes_A M_1' \arrow[r, "1\otimes\iota'"] \arrow[d, "1\otimes\phi"] & E \otimes_A M' \arrow[r, "1\otimes\pi'"] \arrow[d, "1\otimes\psi"] & E \otimes_A M_2' \arrow[r] \arrow[d, "1\otimes\eta"] & 0 \\
0 \arrow[r] & E \otimes_A M_1 \arrow[r, "1\otimes\iota"] & E \otimes_A M \arrow[r, "1\otimes\pi"] & E \otimes_A M_2 \arrow[r] & 0
\end{tikzcd}$$

By hypotheses the two rows of this diagram are exact. As E is flat for M_1 and M_2, $1 \otimes \phi$ and $1 \otimes \eta$ are injective. The snake lemma then shows that $1 \otimes \psi$ is injective and consequently E is M-flat.

If I is a finite set with n elements, the lemma follows by induction on n. In the general case, let M' be a finitely generated submodule of M. Then there exists a finite subset J of the indexing set I such that M' is contained in the direct sum $M^J = \bigoplus_{i \in J} M_j$. By the finite case E is flat for M^J. The canonical homomorphism $E \otimes_A M' \to E \otimes_A M^J$ is therefore injective. On the other hand, as M^J is a direct factor of M, the canonical homomorphism $E \otimes_A M^J \to E \otimes_A M$ is injective. Taking the composition, it follows that $E \otimes_A M^J \to E \otimes_A M$ is injective and E is flat for M by Lemma 7.2.1. □

7.2.2 Flat modules

Proposition 7.2.4. *Let E be an A-module. The following three properties are equivalent:*

(i) E is flat for A (in other words, for every ideal $\mathfrak{a}$ of A, the canonical homomorphism $E \otimes_A \mathfrak{a} \to E \otimes_A A$ is injective).

(ii) E is M-flat for every A-module M.

(iii) The functor $\otimes_A E$ is exact, that is, E is flat.

Proof. It is immediate that (ii) is equivalent to (iii) and (ii) implies (i). Conversely, if (i) holds, then by Lemma 7.2.3, E is fiat for every flee left A-module. As every A-module is isomorphic to a quotient of a free module, it follows from Lemma 7.2.2 that E is flat for M. □

Remark 7.2.1. By Lemma 7.2.1, for an A-module E to be flat, it is necessary and sufficient that, for every finitely generated ideal $\mathfrak{a}$ of A, the canonical mapping $E \otimes_A \mathfrak{a}$ with image $E\mathfrak{a}$ be injective.

Proposition 7.2.5. *Let $(E_i)_{i \in I}$ be a family of A-modules. For $E = \bigoplus_i E_i$ to be flat, it is necessary and sufficient that each of the E_i be flat.*

Proof. Let $M' \to M$ be an injective A-module homomorphism. For the direct sum homomorphism

$$\bigoplus_{i \in I} (E_i \otimes_A M) \to \bigoplus_{i \in I} (E_i \otimes_A M)$$

to be exact, it is necessary and sufficient that each of the homomorphisms $E_i \otimes_A M' \to E_i \otimes_A M$ be so, which proves the claim since $\bigoplus_{i \in I} (E_i \otimes_A M)$ is canonically identified with $E \otimes_A M$. □

Proposition 7.2.6. *Let I be an ordered set and $(E_\alpha, f_{\beta\alpha})$ a direct system of A-modules. If each of the E_α is flat, then $E = \varinjlim E_\alpha$ is flat.*

Proof. By hypothesis each of the sequences $0 \to E_\alpha \otimes_A M' \to E_\alpha \otimes_A M$ is exact; so then is the sequence $0 \to E \otimes_A M' \to E \otimes_A M$ since taking the direct limit commutes with tensor products and preserves exactness. □

Example 7.2.7.

(a) For any ring A, A is clearly a flat A-module. Then it follows from Proposition 7.2.5 that every free A-module, and more generally every projective A-module, is a flat A-module.

(b) If A is a semisimple ring, every A-module E is semisimple and hence a direct sum of simple modules. As each of these latter is isomorphic to a direct factor of A, E is projective and therefore flat.

(c) Let $a \in A$ be such that the map $a_A : x \mapsto ax$ on A is injective (a is not a zero divisor). If E is a flat A-module, then the homothety a_E is injective. In particular, if A is integral, any flat A-module is torsion free. Conversely, if A is a PID, then any torsion free A-module is flat: infact, if the A-module E is torsion-free, any finitely generated submodule of E is free, and E is the union of these flat submodules, hence flat (Proposition 7.2.6).

Proposition 7.2.8. *Let A be a ring and E an A-module.*

(a) Suppose that E is flat. For every element a of A which is not a divisor of 0, the relations $x \in E$, $ax = 0$ imply $x = 0$.

(b) Suppose that A is an integral domain in which every finitely generated ideal is principal. Then for E to be flat it is necessary and sufficient that E be torsion-free.

Proof. We prove (a). Let $v : A \to A$ be the A-module homomorphism $t \mapsto at$. The hypothesis implies that v is injective. As E is flat, the homomorphism $1_E \otimes v : E \otimes_A A \to E \otimes_A A$ is also injective. When $E \otimes_A A$ is canonically identified with E, $1_E \otimes v$ becomes the endomorphism $x \mapsto ax$ of E. Thus the relation $ax = 0$ implies $x = 0$.

We prove (b). By (a), if E is flat, E is torsion-free. Conversely, let E be a torsion-free A-module and let $\mathfrak{a}$ be a nonzero finitely generated ideal of A. By hypothesis $\mathfrak{a} = Aa$ for some nonzero $a \in A$ and $t \mapsto at$ is then an isomorphism v of A onto $\mathfrak{a}$. Using i to denote the canonical injection $\mathfrak{a} \to A$, $i \circ v$ is the homothety with ratio a on E and is injective since E is assumed to be torsion-free. Then $1_E \otimes (i \circ v) = (1_E \otimes i) \circ (1_E \otimes v)$. As $1_E \otimes v$ is an isomorphism, $1_E \otimes i$ is injective, which completes the proof. □

Proposition 7.2.9. *Let E be an A-module. The three following properties are equivalent:*

(i) E is flat.

(ii) For every exact sequence of A-modules of the form

$$0 \longrightarrow G \xrightarrow{\phi} H \xrightarrow{\psi} E \longrightarrow 0 \tag{2.2.1}$$

and every A-module F, the sequence

$$0 \longrightarrow G \otimes_A F \xrightarrow{\phi\otimes 1} H \xrightarrow{\psi\otimes 1} E \otimes_A F \longrightarrow 0 \tag{2.2.2}$$

sexact.

(iii) There exists an exact sequence (2.2.1), where H is flat, such that the sequence (2.2.2) is is exact for every A-module F of the form $A/\mathfrak{a}$, where $\mathfrak{a}$ is a finitely generated ideal of A.

Proof. The A-module F is isomorphic to a quotient of a free module. In other words, we have an exact sequence $0 \longrightarrow R \xrightarrow{\iota} L \xrightarrow{\pi} F \longrightarrow 0$ where L is free. Consider the diagram

$$\begin{tikzcd}
 & G \otimes_A R \arrow[r, "\phi\otimes 1_R"] \arrow[d, "1_G\otimes\iota"] & H \otimes_A R \arrow[r, "\psi\otimes 1_R"] \arrow[d, "1_H\otimes\iota"] & E \otimes_A R \arrow[r] \arrow[d, "1_E\otimes\iota"] & 0 \\
0 \arrow[r] & G \otimes_A L \arrow[r, "\phi\otimes 1_L"] \arrow[d, "1_G\otimes\pi"] & H \otimes_A L \arrow[r, "\psi\otimes 1_L"] \arrow[d, "1_H\otimes\pi"] & E \otimes_A L \arrow[r] \arrow[d, "1_F\otimes\pi"] & 0 \\
 & G \otimes_A F \arrow[r, "\phi\otimes 1_F"] \arrow[d] & H \otimes_A F \arrow[r, "\phi\otimes 1_F"] \arrow[d] & E \otimes_A F \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd} \tag{2.2.3}$$

It follows immediately that this diagram is commutative, and its rows and columns are exact. Apply the snake lemma to the first two rows, we get the following exact sequence

$$\ker(1_H \otimes \iota) \longrightarrow \ker(1_E \otimes \iota) \xrightarrow{\delta} G \otimes_A F \xrightarrow{\phi\otimes 1_F} H \otimes_A F \tag{2.2.4}$$

Now if E is flat, then $1_E \otimes \iota$ is injective, and the exact sequence shows that $\phi \otimes 1_F$ is injective, hence the sequence (2.2.2) is exact.

As (ii) obviously implies (iii), it remains to prove that (iii) implies (i). Consider the diagram (2.2.3) in the case $R = \mathfrak{a}$, $L = A$, $F = A/\mathfrak{a}$ and apply the exact sequence (2.2.4). By hypothesis $\phi \otimes 1_F$ is injective, so $\operatorname{im}\delta = 0$. Moreover, as H is exact, we see $\ker(1_H \otimes \iota) = 0$, whence $\ker(1_E \otimes \iota) = 0$ and E is flat. □

Proposition 7.2.10. *Let $0 \longrightarrow E_1 \xrightarrow{\phi} E_2 \xrightarrow{\psi} E_3 \longrightarrow 0$ be an exact sequence of A-modules. Suppose E_3 is flat. Then, for E_2 to be flat it is necessary and sufficient that E_1 be flat.*

Proof. Let $\eta : F' \to F$ be an injective homomorphism of A-modules. Consider the diagram

$$\begin{tikzcd}
0 \arrow[r] & E_1 \otimes_A F' \arrow[r, "\phi\otimes 1_{F'}"] \arrow[d, "1_{E_1}\otimes\eta"] & E_2 \otimes_A F' \arrow[r, "\psi\otimes 1_{F'}"] \arrow[d, "1_{E_2}\otimes\eta"] & E_3 \otimes_A F' \arrow[r] \arrow[d, "1_{E_3}\otimes\eta"] & 0 \\
0 \arrow[r] & E_1 \otimes_A F \arrow[r, "\phi\otimes 1_F"] & E_2 \otimes_A F \arrow[r, "\psi\otimes 1_F"] & E_3 \otimes_A F \arrow[r] & 0
\end{tikzcd}$$

It is commutative and its rows are exact by Proposition 7.2.9. Since E_3 is flat, we know $1_{E_3} \otimes \eta$ is injective. Now snake lemma gives the claim. □

Let E and F be A-modules. Every element of $E \otimes_A F$ can be written in at least one way in the form $z = \sum_{i=1}^n e_i \otimes f_i$ where $e_i \in E$ and $f_i \in F$. The following lemma gives a condition under which this sum is zero:

Lemma 7.2.11. *Let $(f_i)_{i\in I}$ be a family of generators of F and $(e_i)_{i\in I}$ a family of elements of E of finite support. For $\sum_{i\in I} e_i \otimes f_i = 0$, it is necessary and sufficient that there exist a finite set J, a family $(x_j)_{j\in J}$ of elements of E and a family $(a_{ji})_{j\in J, i\in I}$ of elements of A with the following properties:*

(a) the family (a_{ji}) has finite support;

(b) $\sum_{i\in I} a_{ji} f_i = 0$ *for all* $j \in J$*;*

(c) $e_i = \sum_{j\in J} a_{ji} x_j$ *for all* $i \in I$*.*

Proof. Consider the free A-module $A^{\oplus I}$, its canonical basis (u_i) and the homomorphism $g : A^{\oplus I} \to F$ such that $g(u_i) = f_i$ for all $i \in I$. Denoting by R the kernel of g, we have (since the f_i generate F) an exact sequence

$$R \xrightarrow{\iota} A^{\oplus I} \xrightarrow{g} F \longrightarrow 0$$

wherc ι denotes the canonical injection. We derive from this the exact sequence

$$E \otimes_A R \longrightarrow E \otimes_A A^{\oplus I} \xrightarrow{1\otimes g} E \otimes_A F \longrightarrow 0 \tag{2.2.5}$$

Now, $E \otimes_A A^{\oplus I}$ is canonically identified with $E^{\oplus I}$ a family $e = (e_i) \in E^{\oplus I}$ being identified with $\sum_{i\in I} e_i \otimes u_i$. For such a family to belong to the kernel of $1_E \otimes g$, it is necessary and sufficient that $\sum_{i\in I} e_i \otimes f_i = 0$ in $E \otimes_A F$. Taking account of the exact sequence (2.2.5), this is equivalent to saying that e belongs to the image of $1_E \otimes \iota$, in other words there is a relation of the form

$$\sum_{i\in I} e_i \otimes u_i = \sum_{j\in J} x_j \otimes \iota(r_j) \tag{2.2.6}$$

where $x_i \in E$, $r_i \in R$ and J is finite. Writing $\iota(r_i) = \sum_{i\in I} a_{ji} u_i$, the hypothesis $r_j \in R$ implies the relation $\sum_{i\in I} a_{ji} f_i = 0$ for all $j \in J$. On the other hand the relation (2.2.6) implies $e_i = \sum_{j\in J} a_{ji} x_j$ for all $i \in I$ (**??**), which completes the proof. □

Proposition 7.2.12. *For E to be F-flat, it it necessary and sufficient that the following condition be satisfied:*

(R) If $(e_i)_{i\in I}$ and $(f_i)_{i\in I}$ are two finite families of elements of E and F respectively such that $\sum_{i\in I} e_i \otimes f_i = 0$ in $E \otimes_A F$, there exists a finite set J, a family $(x_j)_{j\in J}$ of elements of E and a family $(a_{ji})_{j\in J, i\in I}$ of elements of A, with the following properties:

(a) $\sum_{i\in I} a_{ji} f_i = 0$ *for all* $j \in J$*.*

(b) $e_i = \sum_{j\in J} a_{ji} x_j$ *for all* $i \in I$*.*

Proof. Suppose that E is F-flat. Let (e_i) and (f_i) be finite families of elements such that $\sum_{i\in I} e_i \otimes f_i = 0$ in $E \otimes_A F$, and let F' be the submodule of F generated by the f_i. Since the canonical mapping $E \otimes_A F' \to E \otimes_A F$ is injective, we have also $\sum_{i\in I} e_i \otimes f_i = 0$ in $E \otimes_A F'$ and Lemma 7.2.11 can then be applied to E and F'. Thus families (x_j) and (a_{ji}) are obtained satisfying the conditions of (R).

Conversely, suppose that condition (R) holds. Let F' be a submodule of F and let $y = \sum_{i\in I} e_i \otimes f_i$ be an element of the kernel of the canonical mapping $E \otimes_A F' \to E \otimes_A F$. Since (R) holds, there exist families (x_j) and (a_{ji}) satisfying conditions (a) and (b). We conclude that, in $E \otimes_A F$,

$$y = \sum_{i,j} a_{ji} x_j \otimes f_i = \sum_{j\in J} (x_j \otimes \sum_{i\in I} a_{ji} f_i) = 0$$

hence the map $E \otimes F' \to E \otimes F$ is injective. □

Corollary 7.2.13. *For an A-module E to be flat, it is necessary and sufficient that the following condition hold:*

(RP) Every solution $\boldsymbol{y} \in M^n$ of a linear equation $P\boldsymbol{y} = 0$ with $P \in \mathcal{M}_{mn}(A)$ is a linear combination $\boldsymbol{y} = Q\boldsymbol{x}$, where $Q \in \mathcal{M}_{nk}(A)$, $\boldsymbol{x} \in M^k$ and $PQ = 0$.

7.2.3 Intersection properties

Lemma 7.2.14. *Let E be an A-module, F an A-module and F_1, F_2 two submodule of F such that $F = F_1 + F_2$. Then the intersection of the canonical images of $E \otimes F_1$ and $E \otimes F_2$ in $E \otimes F$ is equal to the canonical image of $E \otimes (F_1 \cap F_2)$.*

Proof. Consider the diagram

$$\begin{tikzcd}
0 \arrow[r] & F_1 \cap F_2 \arrow[r] \arrow[d] & F_1 \arrow[r] \arrow[d] & F_1/(F_1 \cap F_2) \arrow[r] \arrow[d, "\eta"] & 0 \\
0 \arrow[r] & F_2 \arrow[r] & F_1 + F_2 \arrow[r] & (F_1 + F_2)/F_2 \arrow[r] & 0
\end{tikzcd}$$

where the unspecified arrows are the canonical injections and surjections and η is the canonical isomorphism. This diagram is commutative and its rows are exact. We derive (since $F = F_1 + F_2$) a commutative diagram

$$\begin{tikzcd}
E \otimes (F_1 \cap F_2) \arrow[r] \arrow[d] & E \otimes F_1 \arrow[r] \arrow[d] & E \otimes (F_1/(F_1 \cap F_2)) \arrow[r] \arrow[d, "1_E \otimes \eta"] & 0 \\
E \otimes F_2 \arrow[r] & E \otimes F \arrow[r] & E \otimes ((F_1 + F_2)/F_2) \arrow[r] & 0
\end{tikzcd}$$

The rows of this diagram are exact and $1_E \otimes \eta$ is an isomorphism. A simple diagram chasing shows the claim. □

Proposition 7.2.15. *Let E be an A-module and F an A-module such that E is F-flat. Then, if F_1, F_2 are two submodules of F, we have*

$$E \otimes (F_1 \cap F_2) = (E \otimes F_1) \cap (E \otimes F_2).$$

Proof. As E is F-flat, $(E \otimes F_1) + (E \otimes F_2)$ is identified with $E \otimes (F_1 + F_2)$, which is a submodule of $E \otimes F$. The assertion then follows from Lemma 7.2.14. □

Example 7.2.16. Let k be a field, and consider the subring $A = k[X^2, X^3]$ of the polynomial ring $B = k[X]$ in an indeterminate x. Then $X^2A \cap X^3A$ is the set of polynomials made up of terms of degree ≥ 5 in X, so that $(X^2A \cap X^3A)B = X^5B$; but on the other hand $X^2B \cap X^3B = X^3B$. Therefore by the above proposition B is not flat over A.

Proposition 7.2.17. *Let E be an A-module, E' a submodule of E, F an A-module and F' a submodule of F. Suppose that E/E' or F/F' is flat. Then we have*

$$E' \otimes F' = (E' \otimes F) \cap (E \otimes F').$$

Proof. Suppose for example that E/E' is flat and consider the diagram

$$\begin{tikzcd} E' \otimes F' \arrow[r] \arrow[d] & E \otimes F' \arrow[r] \arrow[d] & (E/E') \otimes F \arrow[r] \arrow[d, "\eta"] & 0 \\ E' \otimes F \arrow[r] & E \otimes F \arrow[r] & (E/E') \otimes F \arrow[r] & 0 \end{tikzcd}$$

where the arrows are the canonical homomorphisms. This diagram is commutative and its rows are exact. As E/E' is flat, η is injective. Then our assertion then follows from a diagram chasing as in Lemma 7.2.14. □

Corollary 7.2.18. *Let E be an A-module and E' a submodule of E.*

(a) Suppose that E/E' is flat. Then, for every ideal $\mathfrak{a}$ of A, we have $\mathfrak{a}E' = \mathfrak{a}E \cap E'$.

(b) Conversely, suppose that E is flat and, for every finitely generated ideal $\mathfrak{a}$ of A we have $\mathfrak{a}E' = \mathfrak{a}E \cap E'$. Then E/E' is flat.

Proof. For (a), it is sufficient to apply Proposition 7.2.17 to the case $F = A$ and $F' = \mathfrak{a}$. Conversely, to prove that E/E' is flat, apply criterion (iii) of Proposition 7.2.9. It is then necessary to establish that the sequence

$$0 \longrightarrow E'/\mathfrak{a}E' \longrightarrow E/\mathfrak{a}E \longrightarrow E/(E' + \mathfrak{a}E) \longrightarrow 0$$

is exact for every finitely generated ideal $\mathfrak{a}$ of A. Now this is precisely what relation $\mathfrak{a}E' = \mathfrak{a}E \cap E'$ expresses. □

7.2.4 Extension of scalars and flatness

Proposition 7.2.19. *Let R, S be two rings, E an R-module and F an (R, S)-bimodule. Suppose that E is flat and that F is flat as an S-module. Then the S-module $E \otimes_R F$ is flat.*

Proof. Let M be a left S-module and M' a submodule of M. Since F is flat as a S-module, the canonical homomorphism $F \otimes_S M' \to F \otimes_S M$ is injective. Since E is flat, the canonical homomorphism

$$E \otimes_R (F \otimes_S M') \to E \otimes_R (F \otimes_S M)$$

is injective. As $E \otimes_R (F \otimes_S M')$ and $E \otimes_R (F \otimes_S M)$ are canonically identified with $(E \otimes_R F) \otimes_S M'$ and $(E \otimes_R F) \otimes_S M$ respectively, the canonical homomorphism

$$(E \otimes_R F) \otimes_S M' \to (E \otimes_R F) \otimes_S M$$

is injective, which proves that $E \otimes_R F$ is a flat S-module. □

Corollary 7.2.20. *Let A be a ring, E, F two flat A-modules. Then $E \otimes_A F$ is a flat A-module.*

Proof. We see F is a (A, A)-bimodule and it is sufficient to apply Proposition 7.2.19 with $R = S = A$. □

Corollary 7.2.21. *Let $\rho : A \to B$ be a ring homomorphism. If E is a flat A-module, the B-module $\rho_*(E) = E \otimes_A B$ is flat.*

Proof. The B-module B is flat, so the result follows from Proposition 7.2.19. □

Corollary 7.2.22. *Let $\rho : A \to B$ be a ring homomorphism. If M is a flat A-module and B is a flat A-module, then $\rho^*(M)$ is a flat A-module.*

Proof. Apply Proposition 7.2.19 with $R = B$, $S = A$, $E = M$ and $F = B$, B having a (B, A)-bimodule structure defined by f, the A-module $M \otimes_B B$ is then $\rho^*(M)$. □

Example 7.2.23. Suppose that $A = K[X, Y]$ where K is a field. The maximal ideal $\mathfrak{m}$ generated by X and Y is a torsion-free A-module, but not flat. In fact, consider the ring $B = A/(Y)$, which is isomorphic to $K[X]$, hence integral. The B-module $\mathfrak{m} \otimes_A B$ is isomorphic to $\mathfrak{m}/Y\mathfrak{m} = (X, Y)/(XY, Y^2)$, in which the class of Y is torsion (killed by X). Therefore, $\mathfrak{m} \otimes_A B$ is not a flat B-module, so $\mathfrak{m}$ is not flat (Corollary 7.2.21).

Proposition 7.2.24. *Let $\rho : R \to S$ be a ring homomorphism and F an R-module. The following two properties are equivalent:*

(i) $\mathrm{Tor}_1^R(\rho^*(E), F) = 0$ *for every S-module E.*

(ii) $\mathrm{Tor}_1^S(E, \rho_*(F)) = 0$ *for every S-module E and* $\mathrm{Tor}_1^R(\rho^*(S), F) = 0$.

Proof. Suppose that (i) holds. Taking $E = S$, we see that $\mathrm{Tor}_1^R(\rho^*(S), F) = 0$. We show also that $\rho_*(F)$ is a flat S-module. For that, we note that, if E is an S-module, the additive group $E \otimes_S \rho_*(F) = E \otimes_S (S \otimes_R F)$ is identified with $\rho_*(E) \otimes_R F$. Then if there is an exact sequence of S-modules

$$0 \longrightarrow E_1 \longrightarrow E_2 \longrightarrow E_3 \longrightarrow 0$$

we obtain, using (i), an exact sequence

$$0 \longrightarrow \rho^*(E_1) \otimes_R F \longrightarrow \rho^*(E_2) \otimes_R F \longrightarrow \rho^*(E_3) \otimes_R F \longrightarrow 0$$

or also

$$0 \longrightarrow E_1 \otimes_S \rho_*(F) \longrightarrow \rho_*(E_2) \otimes_S \rho_*(F) \longrightarrow \rho_*(E_3) \otimes_S \rho_*(F) \longrightarrow 0$$

which proves that $\rho_*(F)$ is flat. Conversely, if (ii) holds, we have first of all, for every free right S-module $L = S^{\oplus I}$, $\mathrm{Tor}_1^R(\rho^*(L), F) = \mathrm{Tor}_1^R(\rho^*(S), F)^{\oplus I} = 0$. Every right S-module E can be written in the form $E = L/H$ for a suitable free S-module L, then we have the exact sequence

$$0 = \mathrm{Tor}_1^R(\rho^*(L), F) \longrightarrow \mathrm{Tor}_1^R(\rho^*(E), F) \longrightarrow \rho^*(H) \otimes_R F \longrightarrow \rho^*(L) \otimes_R F \tag{2.4.1}$$

But as $\rho_*(F)$ is flat, the homomorphism $H \otimes_S \rho_*(F) \to L \otimes_S \rho_*(F)$ is injective and is identified with the homomorphism $\rho^*(H) \otimes_R F \to \rho^*(L) \otimes_R F$. Then it follows from (2.4.1) that $\mathrm{Tor}_1^R(\rho^*(E), F) = 0$. □

7.2.5 Finitely presented modules

Let A be a ring. An exact sequence

$$L_1 \longrightarrow L_0 \longrightarrow E \longrightarrow 0$$

of A-modules, where L_0 and L_1 are free, is called a **presentation** of an A-module E. Every A-module E admits a presentation: we know there exists a surjective homomorphism $\phi : L_0 \to E$, where L_0 is free. If R is the kernel of ϕ, there exists similarly a surjective homomorphism $\psi : L_1 \to R$, where L_1 is free. If ψ is considered as a homomorphism of L_1 to L_0, the sequence

$$L_1 \xrightarrow{\psi} L_0 \xrightarrow{\phi} E \longrightarrow 0$$

is exact by definition, whence our assertion. A presentation of a module E is called **finite** if the free modules L_0 and L_1 have finite bases. E is called a **finitely presented** A-module if it admits a finite presentation.

Proposition 7.2.25. *Let A be a ring.*

(a) Every module admitting a finite presentation is finitely generated.

(b) If A is a Noetherian ring, every finitely generated A-module admits a finite presentation.

(c) Every finitely generated projective module admits a finite presentation.

Proof. Assertion (a) follows trivially from the definitions. If A is Noetherian and there exists a surjective homomorphism $\phi : L_0 \to E$, where L_0 is a free A-module with a finite basis, the kernel R of ϕ is finitely generated, hence there is a surjective homomorphism $\psi : L_1 \to R$, where L_1 is free and has a finite basis, and the exact sequence

$$L_1 \xrightarrow{\psi} L_0 \xrightarrow{\phi} E \longrightarrow 0$$

is a finite presentation of E; whence (b).

Finally, suppose that E is a finitely generated projective module; then it is a direct factor of a finitely generated free module L_0. The kernel R of the surjective homomorphism $L_0 \to E$ is then isomorphic to a quotient of L_0 and hence finitely generated and the proof is completed as for (b). □

Proposition 7.2.26. *Let A be a ring and E a finitely presented A-module. For every exact sequence*

$$0 \longrightarrow F \xrightarrow{\iota} G \xrightarrow{\pi} E \longrightarrow 0$$

where G is finitely generated, the module F is finitely generated.

Proof. Let $L_1 \xrightarrow{\psi} L_0 \xrightarrow{\phi} E \to 0$ be a finite presentation. If (e_i) is a basis of L_0, there exists for each i an element $g_i \in G$ such that $\pi(g_i) = \phi(e_i)$. the homomorphism $\eta : L_0 \to G$ such that $\eta(e_i) = g_i$ for all i then satisfies $\phi = \pi \circ \eta$. As $\phi \circ \psi = 0$, we have $\mathrm{im}(\eta \circ \phi) \subseteq \ker \pi$, and as $\ker \pi$ is isomorphic to F, it can be seen that there is a homomorphism $\gamma : L_1 \to F$ such that the diagram

$$\begin{tikzcd}
 & L_1 \arrow[r, "\psi"] \arrow[d, "\gamma"] & L_0 \arrow[r, "\phi"] \arrow[d, "\eta"] & E \arrow[r] \arrow[d, "1_E"] & 0 \\
0 \arrow[r] & F \arrow[r, "\iota"] & G \arrow[r, "\pi"] & E \arrow[r] & 0
\end{tikzcd}$$

is commutative. As ι is injective and ψ surjective, we can apply the snake lemma, in other words there is an exact sequence

$$0 = \ker 1_E \longrightarrow \operatorname{coker}\gamma \longrightarrow \operatorname{coker}\eta \longrightarrow \operatorname{coker} 1_E = 0$$

This shows that $\operatorname{coker}\gamma$ is isomorphic to $G/\eta(L_0)$, which is finitely generated by hypothesis. Moreover we have the exact sequence

$$0 \longrightarrow \gamma(L_1) \longrightarrow F \longrightarrow \operatorname{coker}\gamma \longrightarrow 0$$

and as $\gamma(L_1)$ and $\operatorname{coker}\gamma$ are finitely generated, so is F. □

Proposition 7.2.27. *Let M be an A-module. There exist a direct system $(M_\alpha, \varphi_{\beta\alpha})$ of finitely presented A-modules such that M is isomorphic to $\varinjlim M_\alpha$. If M is generated by n elements, then we may suppose that M_α is generated by n elements.*

Proof. Consider a presentation

$$A^{\oplus K} \xrightarrow{\psi} A^{\oplus L} \xrightarrow{\phi} M \longrightarrow 0$$

Let I be the set of pairs $\alpha = (K', L')$, where K' (resp. L') is a finite subset of K (resp. L), such that ψ induces a map ψ_α from the submodule $A^{K'}$ of $A^{\oplus K}$ to the submodule $A^{L'}$ of $A^{\oplus L}$. For each $\alpha \in I$, let M_α be the cokernel of ψ_α and $\phi_\alpha : A^{L'} \to M_\alpha$ the canonical map, such that we have a commutative diagram with exact rows:

$$\begin{tikzcd}
A^{\oplus K} \arrow[r, "\psi"] & A^{\oplus L} \arrow[r, "\phi"] & M \arrow[r] & 0 \\
A^{K'} \arrow[u] \arrow[r, "\psi_\alpha"] & A^{L'} \arrow[u] \arrow[r, "\phi_\alpha"] & M_\alpha \arrow[u] \arrow[r] & 0
\end{tikzcd}$$

We order the set I be the relation $(K', L') \preceq (K'', L'')$ if $K' \subseteq K'$ and $K' \subseteq K''$. For $\alpha \preceq \beta$, let $\varphi_{\beta\alpha} : M_\alpha \to M_\beta$ be the homomorphism induced by the inclusion of $A^{L'}$ to $A^{L''}$. It is immediate to verify that I is filtered and $(M_\alpha, \varphi_{\beta\alpha})$ is a direct system indexed by I. Passing to direct limit, we obtain a commutative diagram

$$\begin{tikzcd}
A^{\oplus K} \arrow[r, "\psi"] & A^{\oplus L} \arrow[r, "\phi"] & M \arrow[r] & 0 \\
\varinjlim A^{K'} \arrow[u, "i"] \arrow[r] & \varinjlim A^{L} \arrow[u, "j"] \arrow[r] & \varinjlim M_\alpha \arrow[u] \arrow[r] & 0
\end{tikzcd}$$

with exact rows. Since i and j are bijective, we conclude that φ is bijective by five lemma. In the case M can be generated by n elemetns, we have $|L| \leq n$, so each $|L'| \leq n$, which means M_α can be generated by n elements. □

Let A and B be two rings, E an A-module, F an B-module and G a (B, A)-bimodule. Recall that we have a canonical homomorphism of $\mathbb{Z}$-modules

$$\nu : F \otimes_B \operatorname{Hom}_A(E, G) \to \operatorname{Hom}_A(E, F \otimes_B G)$$

such that, for all $y \in F$ and $\phi \in \mathrm{Hom}_A(E, G)$, $\nu(y \otimes \phi)$ is the A-linear mapping $x \mapsto y \otimes \phi(x)$.

Proposition 7.2.28. *Let A, B be two rings, E an A-module, F an B-module and G a (B, A)-bimodule. Suppose that F is flat. Then, if E is finitely generated (resp. finitely presented), the canonical homomorphism ν is injective (resp. bijective).*

Proof. Consider A, B, F, G as fixed and for each A-module E set

$$T(E) = F \otimes_B \mathrm{Hom}_A(E, G), \quad U(E) = \mathrm{Hom}_A(E, F \otimes_B G)$$

and denote the homomorphism ν by ν_E. For every A-module homomorphism $v : E \to E'$, set $T(v) = 1_F \otimes \mathrm{Hom}(v, 1_G)$ and $U(v) = \mathrm{Hom}(v, 1_F \otimes 1_G)$. Let

$$L_1 \xrightarrow{\psi} L_0 \xrightarrow{\phi} E \longrightarrow 0$$

be a presentation (resp. finite presentation) of E. We suppose the free module L_0 (resp. the free modules L_0 and L_1) to be finitely generated. The diagram

$$\begin{tikzcd} 0 \arrow[r] & T(E) \arrow[r, "T(\phi)"] \arrow[d, "\nu_E"] & T(L_0) \arrow[r, "T(\psi)"] \arrow[d, "\nu_{L_0}"] & T(L_1) \arrow[d, "\nu_{L_1}"] \\ 0 \arrow[r] & U(E) \arrow[r, "U(\phi)"] & U(L_0) \arrow[r, "U(\psi)"] & U(L_1) \end{tikzcd} \tag{2.5.1}$$

is commutative and the second row is exact. Moreover, the sequence

$$0 \longrightarrow \mathrm{Hom}_A(E, G) \longrightarrow \mathrm{Hom}_A(L_0, G) \longrightarrow \mathrm{Hom}_A(L_1, G)$$

is exact, and as F is flat, the first row of (2.5.1) is also an exact sequence. Then we know that ν_{L_0} (resp. ν_{L_0} and ν_{L_1}) is bijective (resp. are bijective). If we assume only that ν_{L_0} is bijective, it follows from (2.5.1) that

$$\nu_{L_0} \circ T(\phi) = U(\phi) \circ \nu_E$$

is injective and hence so is ν_E. If we assume that both ν_{L_0} and ν_{L_1} are bijective, it follows from the four lemma that ν_E is surjective, and as we have just seen that ν_E is injective, it is bijective. □

Now let $\rho : A \to B$ a ring homomorphism such that B is an A-algebra. Recall that for every ordered pair (E, F) of A-modules, we have a canonical B-homomorphism

$$\omega : \rho^*(\mathrm{Hom}_A(E, F)) \to \mathrm{Hom}_B(\rho^*(E), \rho^*(F))$$

such that for all $\phi \in \mathrm{Hom}_A(E, F)$, we have $\omega(\phi \otimes 1) = \phi \otimes 1_B$.

Proposition 7.2.29. *Let $\rho : A \to B$ be a ring homomorphism and E, F two A-modules. Suppose that B is a flat A-module and E is finitely generated (resp. finitely presented). Then the canonical homomorphism ω is injective (resp. bijective).*

Proof. As ω is composed of the canonical homomorphisms

$$B \otimes_A \mathrm{Hom}_A(E, F) \xrightarrow{\nu} \mathrm{Hom}_A(E, B \otimes_A F) \xrightarrow{\cong} \mathrm{Hom}_B(B \otimes_A E, B \otimes_A F)$$

the proposition is a consequence of Proposition 7.2.28. □

Let E be an A-module and (M_i, ϕ_{ji}) be a direct limit of A-modules. Then the canonical map $M_i \to \varinjlim M_i$ induces a homomorphism $\mathrm{Hom}_A(E, M_i) \to \mathrm{Hom}_A(E, \varinjlim M_i)$, hence a canonical homomorphism

$$\alpha : \varinjlim \mathrm{Hom}_A(E, M_i) \to \mathrm{Hom}_A(E, \varinjlim M_i). \tag{2.5.2}$$

Proposition 7.2.30. *If the A-module E is finitely generated (resp. finitely presented), then the canonical homomorphism (2.5.2) is injective (resp. bijective).*

Proof. The proof is similar to that of Proposition 7.2.28, using the fact that taking direct limit is exact. □

Corollary 7.2.31. *Any flat and finitely presented module is projective.*

Proof. Let E be such an A-module. By Proposition 7.2.28, the canonical homomorphism

$$\mathrm{Hom}_A(E, A) \otimes_A E \to \mathrm{Hom}_A(E, E)$$

is bijective, which implies E is projective. □

Proposition 7.2.32. *Let (A_α) be an inductive system of rings and $A = \varinjlim A_\alpha$. For any A-module M of finite presentation, there exists an index α and an A_α-module M_α of finite presentation such that M is isomorphic to $M_\alpha \otimes_{A_\alpha} A$.*

Proof. In fact, we can suppose that $M = A^r/P$ where P is a finitely generated sub-A-module of A^r. As $A^r = \varinjlim A_\alpha^r$ and P is finitely generated, there exists an index α and a finitely generated sub-A_α-module P_α such that P is the canonical image $P_\alpha \otimes_{A_\alpha} A$; the exactness of the tensor product shows that M is isomorphic to $(A_\alpha^r/P_\alpha) \otimes_{A_\alpha} A$. □

We now consider A-algebras. We say an A-algebra B is of finite type if it is isomorphic to a polynomial algebra of the form $A[T_1, \dots, T_n]/\mathfrak{a}$. We say B is of **finite presentation** if moreover the ideal $\mathfrak{a}$ is finitely generated. For any A-algebra A', the ring $B' = B \otimes_A A'$ is of finite type if B is, since it is then isomorphic to a quotient of $A'[T_1, \dots, T_n]$ by the canonical image of $\mathfrak{a} \otimes_A A'$, which is finitely generated if $\mathfrak{a}$ is.

If B is an A-algebra of finite presentation, and C is an B-algebra of finite presentation, then C is an A-algebra of finite presentation. In fact, if we suppose $B = A[S_1, \dots, S_m]/\mathfrak{a}$ and $C = B[T_1, \dots, T_n]/\mathfrak{b}$, where $\mathfrak{a}$ and $\mathfrak{b}$ are finitely generated, then the ring $B[T_1, \dots, T_n] = B \otimes_A A[T_1, \dots, T_n]$ is isomorphic to $A[S_1, \dots, S_m, T_1, \dots, T_n]/\mathfrak{a}'$, where $\mathfrak{a}'$ is a finitely generated; the ideal $\mathfrak{b}$ of $B[T_1, \dots, T_n]$ is then of the form $\mathfrak{b}'/\mathfrak{a}'$, where $\mathfrak{b}'$ is an ideal of $A[S_1, \dots, S_m, T_1, \dots, T_n]$. As $\mathfrak{a}'$ and $\mathfrak{b}'/\mathfrak{a}'$ is finitely generated in $A[S_1, \dots, S_m, T_1, \dots, T_n]$, so is $\mathfrak{b}'$.

If the ring A is Noetherian, then so is $A[T_1, \dots, T_n]$, so any A-algebra of finite type is of finite presentation. However, if A is not Noetherian and $\mathfrak{a}$ is an ideal of A not finitely generated, and $A/\mathfrak{a}$ is a finite algebra, then we can prove that it is not finitely presented.

Proposition 7.2.33. *If B is a finite A-algebra, there exist a surjective homomorphism of A-algebras $\varphi : B' \to B$, where B' is a finite A-algebra that is of finite presentation and a free A-module.*

Proof. In fact, there exists a finite system of generators $(a_i)_{1\leq i\leq m}$ of the A-algebra B, such that each a_i satisfies the relation $F_i(a_i) = 0$, where $F_i \in A[T]$ is a monic polynomial of positive degree. The quotient A-algebra $B'_i = A[T]/(F_i)$ is then free with finite rank over A; let c_i be the class of T in B'_i. There exists a homomorphism of A-algebras $\varphi_i : B'_i \to B$ such that $\varphi_i(c_i) = a_i$ and let $u : B' \to B$ be the tensor product of these homomorphisms, where $B' = B'_1 \otimes_A \cdots \otimes_A B'_m$. By construction φ is surjective, and if $C = A[T_1, \ldots, T_m]$, C is identified with the tensor product $A[T_1]\otimes_A \cdots \otimes_A A[T_m]$ and B' with the tensor product $(A[T_1]/(F_1(T_1)))\otimes_A \cdots \otimes_A (A[T_m]/(F_m(T_m)))$, hence a quotient $C/\mathfrak{c}$, where $\mathfrak{c}$ is the ideal generated by the $F_i(T_i)$. This shows that B' is an A-algebra of finite presentation. □

Corollary 7.2.34. *Let B be a finite A-algebra that is an A-module of finite presentation. Then B is an A-algebra of finite presentation.*

Proof. With the notations of Proposition 7.2.33, the kernel $\mathfrak{a}$ of $\varphi : B \to B$ is an A-module of finite type (Proposition 7.2.26) and a fortiori a finite generated ideal of B'. Therefore B is an B'-algebra of finite presentation, and as B' is an A-algebra of finite presentation, we conclude that B is an A-algebra of finite presentation. □

Proposition 7.2.35. *Any A-algebra B is a filtered limit of A-algebras of finite presentation.*

Proof. For any finite subset L of B, we consider the alebra $C_L = A[(T_m)_{m\in L}]$; if $L \subseteq N$ are two finite subsets of B, let $u_{N,L} : C_L \to C_N$ be the canonical injection such that any T_m for $m \in L$ are mapped to the same element. Let $u_L : C_L \to B$ be the homomorphism of A-algebras sending T_m to m. We consider the ideal $P_L = \ker u_L$ and the set of couples $\alpha = (L, R_L)$, where for a given L, R_L is a finite subset of P_L. It is clear that $u_{N,L}(P_L) \subseteq P_N$ for $L \subseteq N$. We order the set of these couples such that $(L, R_L) \leq (N, R_N)$ if $L \subseteq N$ and if $u_{N,L}(R_L) \subseteq R_N$. It is immediate that this defines an order relation and is filtered, since if (L, R_L) and (N, R_N) are two couples, we can form $M = L \cup N$ and let R_M be the union of the images of $u_{M,L}(R_L)$ and $u_{M,N}(R_N)$. The couple (M, R_M) clearly dominant (L, R_L) and (N, R_N). For any couple $\alpha = (L, R_L)$, we then let $N(R_L) \subseteq P_L)$ be the ideal generated by R_L in C_L; the A-algebra $B_\alpha = C_L/N(R_L)$ is of finite presentation; for $\alpha \leq \beta = (N, R_N)$, we have $u_{N,L}(N(R_L)) \subseteq N(R_N)$, so we have a homomorphism $v_{\beta\alpha} : B_\alpha \to B_\beta$. It is immediate that $(B_\alpha, v_{\beta\alpha})$ is an inductive system of A-algebras. We now prove that its limit B' is isomorphic to B. Let $v_\alpha : B_\alpha \to B'$ be the canonical homomorphism and let $w_\alpha : B_\alpha \to B$ be the homomorphism induced by u_L by passing to quotient. The w_α form an inductive system, with limit $w : B' \to B$, and it suffices to prove that w is bijective. In view of the definition, it is clear that w is surjective. Suppose that $w(x') = 0$ for an element $x' \in B'$; then there exists a couple $\alpha = (L, R_L)$ and an element $x_\alpha \in B_\alpha$ such that $x' = v_\alpha(x_\alpha)$ and $w_\alpha(x_\alpha) = 0$. Then x_α is the canonical image of an element $y_L \in P_L$; if R'_L is the union of R_L with $\{y_L\}$ and $\beta = (L, R'_L)$, we then have $v_{\beta\alpha}(x_\alpha) = 0$, and therefore $x' = 0$. □

Corollary 7.2.36. *Let A be a ring and B be an integral A-algebra. Then B is isomorphic to the filtered limit of finite A-algebras of finite presentation.*

Proof. We use the same reasoning, and choose for any element $m \in B$ a polynomial $F_m \in A[T]$ with positive degree and such that $F_m(m) = 0$. We consider for any finite subset L of B the finite A-algebra $C_L = \bigotimes_{m\in L}(A[T_m]/(F_m(T_m)))$, and define $u_{N,L}$ and u_L as in Proposition 7.2.35. The definition of P_L, R_L, $N(R_L)$ and the order relation are the same. As C_L is a finite A-algebra,

$B_\alpha = C_L/N(R_L)$ is a finite A-algebra of finite presentation, and our assertion follows as in Proposition 7.2.35. □

Proposition 7.2.37. *Let A be a ring and B be an A-algebra.*

(a) If B is of finite type over A, for any filtered system (C_λ) of A-algebras, the canonical map

$$\varinjlim \mathrm{Hom}_A(B, C_\lambda) \to \mathrm{Hom}_A(B, \varinjlim C_\lambda) \tag{2.5.3}$$

which, to any inductive system of homomorphisms, associates its corresponding inductive limit, is an injective map.

(b) In oreder that for any filtered system (C_λ) of A-algebras, the map (2.5.3) is bijective, it is necessary and sufficient that B is an A-algebra of finite presentation.

Proof. Let $(t_i)_{1\leq i\leq n}$ be a system of generators of the A-algebra B. We need to prove that if (θ_λ) and (η_λ) are two inductive systems of homomorphisms $B \to C_\lambda$ such that $\varinjlim \theta_\lambda = \varinjlim \eta_\lambda$, there exists μ such that $\theta_\mu = \eta_\mu$. Now let $\varphi_{\mu\lambda} : C_\lambda \to C_\mu$ and $\varphi_\lambda : C_\lambda \to C = \varinjlim C_\lambda$ be the cannical homomorphisms of the inductive system (C_λ). By hypothesis, for each index i, there exists an index λ_i such that $\varphi_{\lambda_i}(\theta_{\lambda_i}(t_i)) = \varphi_{\lambda_i}(\eta_{\lambda_i}(t_i))$, and if we choose $\lambda_i = \lambda$ for all i, there then exists an index $\mu \geq \lambda$ such that $\varphi_{\mu\lambda}(\theta_\lambda(t_i)) = \varphi_{\mu\lambda}(\eta_\lambda(t_i))$ for all i, which means $\theta_\mu(t_i) = \eta_\mu(t_i)$ for each i, hence $\theta_\mu = \eta_\mu$.

We now prove (b). Suppose that B is of finite presentation, so $B = A[T_1, \dots, T_n]/\mathfrak{a}$, where $\mathfrak{a}$ is a finitely generated ideal. Denote by t_i the class of T_i mod $\mathfrak{a}$ and let $(P_j)_{1\leq j\leq m}$ be a system of generators of $\mathfrak{a}$. Let $\theta : B \to C$ be a homomorphism of A-algebras, and put $c_i = \theta(t_i)$. We then have $P_j(c_1, \dots, c_n) = \theta(P_j(t_1, \dots, t_n)) = 0$ for each j. Now there exists an index λ and elements $x_1, \dots, x_n$ in C_λ such that $c_i = \varphi_\lambda(x_i)$, so $\varphi_\lambda(P_j(x_1, \dots, x_n)) = P_j(c_1, \dots, c_n) = 0$, and there then exists another index $\mu \geq \lambda$ such that $\varphi_{\mu\lambda}(P_j(x_1, \dots, x_n)) = P_j(\varphi_{\mu\lambda}(x_1), \dots, \varphi_{\mu\lambda}(x_n)) = 0$ for all j. We then conclude that there exists a homomorphism of A-algebras $\theta_\mu : B \to C_\mu$ such that $\theta_\mu(t_i) = \varphi_{\mu\lambda}(x_i)$ for each i. If $\theta_\nu = \varphi_{\nu\mu} \circ \theta_\mu$ for any $\nu \geq \mu$, it is clear that $\theta = \varinjlim \theta_\nu$.

Finally we prove the necessity. Let (C_λ) be the filtered system of sub-A-algebras of finite type of B, so that $\varinjlim C_\lambda = B$. Since (2.5.3) is bijective, the idnetity map 1_B factors into $B \to C_\lambda \to B$ for an index λ sufficiently large, and this implies $C_\lambda = B$, so B is of finite type over A. Put then $B = C/\mathfrak{a}$, where $C = A[T_1, \dots, T_n]$ and $\mathfrak{a}$ is an ideal of C. Then $\mathfrak{a}$ is the filtered limit of the inductive system of finitely generated ideals $\mathfrak{a}_\lambda \subseteq \mathfrak{a}$ of C. Let $C_\lambda = C/\mathfrak{a}_\lambda$ and using the exactness of the filtered limit, we see B is isomorphic to the limit of the filtered system (C_λ). Let $p_{\mu\lambda} : C_\lambda \to C_\mu$ and $p_\lambda : C_\lambda \to C$ be the canonical homomorphisms. There exists by hypothesis an index λ and an A-homomorphism $u : B \to C_\lambda$ such that the composition

$$B \xrightarrow{u} C_\lambda \xrightarrow{p_\lambda} B$$

is the identity. Let $q_\lambda : C \to C_\lambda$ be the canonical projection and put $t_i = p_\lambda(q_\lambda(T_i))$. We then have $p_\lambda(u(t_i)) = t_i = p_\lambda(q_\lambda(T_i))$, so $u(t_i) - q_\lambda(T_i) \in \mathfrak{a}/\mathfrak{a}_\lambda$ for each i. Therefore we can find $\mu \geq \lambda$ such that the n elements $u(t_i) - q_\lambda(T_i)$ belongs to $\mathfrak{a}_\mu/\mathfrak{a}_\lambda$, and $p_{\mu\lambda}(u(t_i)) = p_{\mu\lambda}(q_\lambda(T_i)) = q_\mu(T_i)$. By replacing λ by μ and u by $p_{\mu\lambda} \circ u$, we may then assume that $u(t_i) = q_\lambda(T_i)$ for each i. If $\gamma = p_\lambda \circ q_\lambda$ is the canonical homomorphism $C \to C/\mathfrak{a} = B$, we can then $u(\gamma(T_i)) = q_\lambda(T_i)$ for all i, whence $q_\lambda = u \circ \gamma$. But then necessarily $\mathfrak{a} = \mathfrak{a}_\lambda$, since if $z \in \mathfrak{a}$ we have $\gamma(z) = q_\lambda(z) = 0$, so $z \in \mathfrak{a}_\lambda$; hence $B = C_\lambda$. □

Remark 7.2.2. One can wonder if the assumption that (2.5.3) is injective for any filtering inductive system (C_λ) imply that B be an A-algebra of finite type. We immediately see that this is not the case: take B equal to a localized $S^{-1}A$ of A, since $A \to S^{-1}A$ is a epimorphism in the category of rings.

Proposition 7.2.38. *Let A_0 be a ring, (A_λ) be an inductive system of A_0-algebras, and $A - \varinjlim A_\lambda$. If B is an A-algebra of finite presentation, there exists an index λ and an A_λ-algebra B_λ of finite presentation such that B is isomorphic to $B_\lambda \otimes_{A_\lambda} A$.*

Proof. Let $\varphi_\lambda : A_\lambda \to A$ be the canonical homomorphism. By hypothesis, B is isomorphic to an algebra of the form $A[T_1, \dots, T_n]/\mathfrak{a}$, where $\mathfrak{a}$ is a finitely generated ideal. Let $(F_j)_{1\le j\le m}$ be a system of generators of $\mathfrak{a}$. There then exists an index λ such that the coefficients of the polynomials F_j belong to the image of A_λ under φ_λ. Because of this, there is a system of polynomials $(F_{j,\lambda})_{1\le j\le m}$ of $A_\lambda[T_1, \dots, T_n]$ such that $F_j = \varphi_\lambda(F_{j,\lambda})$ for each j. If $\mathfrak{a}_\lambda$ is the ideal of $A_\lambda[T_1, \dots, T_n]$ generated by the $F_{j,\lambda}$, $\mathfrak{a}$ is then the image of $\mathfrak{a}_\lambda \otimes_{A_\lambda} A$ in $A[T_1, \dots, T_n] = A_\lambda[T_1, \dots, T_n] \otimes_{A_\lambda} A$; the ring $B_\lambda = A_\lambda[T_1, \dots, T_n]/\mathfrak{a}_\lambda$ then satisfies the requirement. □

Remark 7.2.3. It is clear that even if B is a finite A-algebra, the localization $S^{-1}B$ of B are not in general A-algebras of finite type. We say that an A-algebra C is **essentially of finite type** if C is A-isomorphic to an A-algebra of the form $S^{-1}B$, where B is a A-algebra of finite type and S a multiplicative subset of B.

Proposition 7.2.39 (Propoerties of algebras essentially of finite type).

(a) If B is an A-algebra essentially of finite type and C is an B-algebra essentially of finite type, then C is an A-algebra essentially of finite type.

(b) Let B be an A-algebra essentially of finite type and A' be an A-algebra. Then $B' = B \otimes_A A'$ is an A-algebra essentially of finite type.

Proof. Let $B = S^{-1}B'$ and $C = T^{-1}C'$, where B' (resp. C') is an A-algebra (resp. B-algebra) of finite type and S (resp. T) is a multiplicative subset of B' (resp. C'). We can then suppose that $C' = B[T_1, \dots, T_n]/\mathfrak{a}$ and as $B[T_1, \dots, T_n] = S^{-1}(B'[T_1, \dots, T_n])$, the ideal $\mathfrak{a}$ is of the form $S^{-1}\mathfrak{a}'$, where $\mathfrak{a}'$ is an ideal of $B'[T_1, \dots, T_n]$. This shows $C' = S^{-1}B''$, where $B'' = B'[T_1, \dots, T_n]/\mathfrak{a}'$ is a B'-algebra of finite type. Hence B'' is an A-algebra of finite type, and $C = T^{-1}(S^{-1}B'')$ is an A-algebra essentially of finite type. The assertion in (b) is clear. □

If B is a local A-algebra essentially of finite type, B is of the form $C_\mathfrak{q}$, where C is an A-algebra of finite type and $\mathfrak{q}$ an ideal of C (Proposition 10.2.36). Let $\mathfrak{p}$ be the image in A of the ideal $\mathfrak{q}$; if we set $S = A - \mathfrak{p}$, $C_\mathfrak{q}$ is also the localization of $S^{-1}C$ at a prime ideal. As $S^{-1}C$ is an algebra of finite type over $A_\mathfrak{p} = S^{-1}A$, we see B is also an $A_\mathfrak{p}$-algebra essentially of finite type, and the homomorphism $A_\mathfrak{p} \to B$ is local.

Proposition 7.2.40. *If B is a local A-algebra essentially of finite type, B is A-isomorphic to a quotient of the A-algebra of the form $C_\mathfrak{q}$, where C is a polynomial algebra $A[T_1, \dots, T_n]$ and $\mathfrak{q}$ is a prime ideal of C.*

Proof. By definition, B is isomorphic to $C'_{\mathfrak{q}'}$, where C' is an A-algebra of finite type and $\mathfrak{q}'$ is a prime ideal of C'. But $C' = C/\mathfrak{b}$ where $C = A[T_1, \dots, T_n]$ and $\mathfrak{b}$ is an ideal of C. Hence $\mathfrak{q}' = \mathfrak{q}/\mathfrak{b}$, where $\mathfrak{q}$ is a prime ideal of C, and $C'_{\mathfrak{q}'}$ is isomorphic to $C_\mathfrak{q}/\mathfrak{b}C_\mathfrak{q}$. □

7.2.6 Structure of flat modules

Lemma 7.2.41. *Let I be a filtered set and $(E_\alpha, \varphi_{\beta\alpha})$ be a direct system of sets indexed by I. Let E be the filtered limit and $\varphi_\alpha : E_\alpha \to E$ the canonical maps. Let $f : I \to I$ be a map such that $f(\alpha) \succ \alpha$ for $\alpha \in I$, and suppose given, for each $\alpha \in I$, a set L_α and maps $u_\alpha : E_\alpha \to L_\alpha$, $v_\alpha : L_\alpha \to E_{f(\alpha)}$ such that the following diagram commutes*

$$\begin{tikzcd} E_\alpha \arrow[rr, "\varphi_{f(\alpha),\alpha}"] \arrow[dr, "u_\alpha"'] & & E_{f(\alpha)} \\ & L_\alpha \arrow[ur, "v_\alpha"'] & \end{tikzcd}$$

Let J be the ordered set obtained by endowing I with the relation $\alpha \preceq \beta$ if $\alpha = \beta$ or $f(\alpha) \preceq \beta$. If $\alpha, \beta \in J$ and $\alpha \preceq \beta$, let $\psi_{\beta\alpha} : L_\alpha \to L_\beta$ be the map such that

$$\psi_{\beta\alpha} = \begin{cases} 1 & \text{if } \alpha = \beta, \\ u_\beta \circ \varphi_{\beta,f(\alpha)} \circ v_\alpha & \text{if } f(\alpha) \preceq \beta. \end{cases}$$

If $\alpha \in J$, let $\psi_\alpha : L_\alpha \to E$ be the map $\varphi_{f(\alpha)} \circ v_\alpha$. Then the ordered set J is filtered, $(L_\alpha, \psi_{\beta\alpha})$ is a direct system indexed by J, (ψ_α) is a dirct system of maps and the map $\psi : \varinjlim_{\alpha \in J} L_\alpha \to E$ induced by ψ_α is bijective.

Proof. It is clear J is filtered. If $\alpha, \beta \in J$ and $\alpha \prec \beta$, we have

$$\psi_\beta \circ \psi_{\beta\alpha} = \varphi_{f(\beta)} \circ v_\beta \circ u_\beta \circ \varphi_{\beta,f(\alpha)} \circ v_\alpha = \varphi_{f(\beta)} \circ \varphi_{f(\beta),\beta} \circ \varphi_{\beta,f(\alpha)} = \varphi_{f(\alpha)} \circ v_\alpha = \psi_\alpha;$$

similarly, if $\alpha, \beta, \gamma \in J$ and $\alpha \prec \beta \prec \gamma$,

$$\begin{aligned} \psi_{\gamma\beta} \circ \psi_{\beta\alpha} &= u_\gamma \circ \varphi_{\gamma,f(\beta)} \circ v_\beta \circ u_\beta \circ \varphi_{\beta,f(\alpha)} \circ v_\alpha \\ &= u_\gamma \circ \varphi_{\gamma,f(\beta)} \circ \varphi_{f(\beta),\beta} \circ \varphi_{\beta,f(\alpha)} \circ v_\alpha = u_\gamma \circ \varphi_{\gamma,f(\alpha)} \circ v_\alpha = \psi_{\gamma\alpha}. \end{aligned}$$

We now prove the last assertion. For $\alpha \in J$, we have

$$\psi_\alpha \circ u_\alpha = \varphi_{f(\alpha)} \circ v_\alpha \circ u_\alpha = \varphi_{f(\alpha)} \circ \varphi_{f(\alpha),\alpha} = \varphi_\alpha,$$

hence $\varphi_\alpha(E_\alpha) = \psi_\alpha(u_\alpha(E_\alpha)) \subseteq \psi_\alpha(L_\alpha)$ and ψ is surjective. Let $\alpha \in J$ and $x, y \in L_\alpha$ be such that $\psi_\alpha(x) = \psi_\alpha(y)$, i.e., $\varphi_{f(\alpha)}(v_\alpha(x)) = \varphi_{f(\alpha)}(v_\alpha(y))$; there then exists $\beta \in I$, $\beta \succeq f(\alpha)$ such that

$$\varphi_{\beta,f(\alpha)}(v_\alpha(x)) = \varphi_{\beta,f(\alpha)}(v_\alpha(y)),$$

hence

$$\psi_{\beta,\alpha}(x) = u_\beta(\varphi_{\beta,f(\alpha)}(v_\alpha(x))) = u_\beta(\varphi_{\beta,f(\alpha)}(v_\alpha(y))) = \psi_{\beta,\alpha}(y).$$

This shows ψ is injective. □

Theorem 7.2.42 (D. Lazard). *For an A-module E, the following conditions are equivalent:*

(i) E is flat;

(ii) For any A-module P that is finitely presented, the canonical homomorphism

$$\mathrm{Hom}_A(P, A) \otimes_A E \to \mathrm{Hom}_A(P, E)$$

is surjective.

(iii) For any A-module P that is finitely presented and any homomorphism $\phi : P \to E$, there exist a finitely generated free A-module L and homomorphisms $\psi : P \to L$ and $\eta : L \to E$ such that $\phi = \eta \circ \psi$.

(iv) There exist a filtered ordered set I and a direct system $(L_i)_{i\in I}$ of free modules such that E is isomorphic to $\varinjlim L_i$.

Proof. We note that (iv)⇒(i) by Proposition 7.2.6, and (i)⇒(ii) by Proposition 7.2.28. We now show that (ii)⇒(iii): let P be a finitely presented A-module and $\phi : P \to E$ a homomorphism; by (ii), there exist $\psi_1, \dots, \psi_n \in \mathrm{Hom}_A(P, A)$ and $w_1, \dots, w_n \in E$ such that $\phi(x) = \sum_i \psi_i(x) w_i$ for $x \in P$. If $\psi : P \to A^n$ is the homomorphism $x \mapsto (\psi_i(x))$ and $\eta : A^n \to E$ is the homomorphism $(a_i) \mapsto \sum_i a_i w_i$, we then have $\phi = \eta \circ \psi$.

Finally, assume that (iii) holds, and let $(E_\alpha, \varphi_{\beta,\alpha})$ be a filtered system of finitely presented A-modules (Proposition 7.2.27). By replacing I with the product $I \times \mathbb{N}$ and set $E_{(\alpha,n)} = E_\alpha$ for each n, we may assume that I has no biggest element. For each $\alpha \in I$, by applying (iii) on the canonical map $\varphi_\alpha : E_\alpha \to E$, we can find a finitely generated A-module L_α and homomorphisms $u_\alpha : E_\alpha \to L_\alpha$, $w_\alpha : L_\alpha \to E$ such that $\phi_\alpha = w_\alpha \circ u_\alpha$. Since L_α is finitely generated free and I has no biggest element, there exists $\beta > \alpha$ and a homomorphism $\tilde{v}_\alpha : L_\alpha \to E_\beta$ such that $w_\alpha = \varphi_\beta \circ \tilde{v}_\alpha$ (see the construction in Proposition 7.2.27):

$$\begin{tikzcd}
E_\alpha \arrow[rr, "\varphi_\alpha"] \arrow[d, "u_\alpha"'] & & E \\
L_\alpha \arrow[urr, "w_\alpha"] \arrow[r, "\tilde{v}_\alpha"] & E_\beta \arrow[ur, "\varphi_\beta"'] \arrow[r, "\varphi_{\gamma\alpha}"] & E_\gamma \arrow[ul, "\varphi_\gamma"]
\end{tikzcd}$$

But note that E_α is finitely presented and we have

$$\varphi_\beta \circ \tilde{v}_\alpha \circ u_\alpha = w_\alpha \circ u_\alpha = \varphi_\alpha = \varphi_\beta \circ \varphi_{\beta,\alpha}$$

so it follows from Proposition 7.2.30 that there exist $\gamma \geq \beta$ such that

$$\varphi_{\gamma\beta} \circ \tilde{v}_\alpha \circ u_\alpha = \varphi_{\gamma\beta} \circ \varphi_{\beta\alpha} = \varphi_{\gamma\alpha}.$$

Put $\gamma = f(\alpha)$ and let $v_\alpha = \varphi_{\gamma\beta} \circ \tilde{v}_\alpha$, we see $v_\alpha \circ u_\alpha = \varphi_{f(\alpha),\alpha}$, so Lemma 7.2.41 gives the claim. □

Corollary 7.2.43. *For any flat module E, the A-modules $T(E)$, $S(E)$, $\bigwedge(E)$, $T^n(E)$, $S^n(E)$, $\bigwedge^n(E)$ are flat.*

Proof. In fact, E is a direct limit of free A-modules (L_i), hence $T(E)$ (resp. $S(E)$, etc.) is a direct limit of free A-modules $(T(L_i))$ (resp. $S(L_i)$, etc.), hence flat. □

7.3 Faithfully flat modules

Proposition 7.3.1. *Let E be an A-module. The following properties are equivalent:*

(i) For a sequence $\mathcal{S}$ of A-modules to be exact, it is necessary and sufficient that the sequence $E \otimes_A \mathcal{S}$ be exact.

(ii) E is flat and, for every A-module N, the relation $E \otimes_A N = 0$ implies $N = 0$.

(iii) E is flat and, for every homomorphism $v : N' \to N$ of A-modules, the relation $1_E \otimes v = 0$ implies $v = 0$.

(iv) E is flat and, for every maximal ideal $\mathfrak{m}$ of A, $\mathfrak{m}E \neq E$.

Proof. Let $\mathcal{S}$ be the sequence $0 \to N \to 0$. If $N \otimes_A M = 0$ then $\mathcal{S} \otimes_A M$ is exact, so $\mathcal{S}$ is exact, and therefore $N = 0$. This shows (i) implies (ii)

We show that (ii) implies (iii). Suppose that (ii) holds and let $v : N' \to N$ be a homomorphism and P its image. As the image of $1_E \otimes v$ is identified with $E \otimes_A P$, the hypothesis $1_E \otimes v = 0$ implies $E \otimes_A P = 0$, hence $P = 0$ by (ii) and consequently $v = 0$.

Now suppose then that (iii) holds and consider a sequence

$$0 \longrightarrow M \xrightarrow{\phi} N \xrightarrow{\psi} P \longrightarrow 0 \tag{3.0.1}$$

of homomorphism of A-modules and the corresponding sequence

$$0 \longrightarrow E \otimes_A M \xrightarrow{1_E \otimes \phi} E \otimes_A N \xrightarrow{1_E \otimes \psi} P \longrightarrow 0 \tag{3.0.2}$$

If the sequence (3.0.1) is exact, so is (3.0.2), since E is flat. Conversely, if (3.0.2) is exact, we have first $1_E \otimes (\psi \circ \phi) = (1_E \otimes \psi) \circ (1_E \otimes \phi) = 0$, hence $\psi \circ \phi = 0$ by hypothesis. Set $H = \operatorname{im} \phi$ and $K = \ker \psi$, then H is contained in K by the above. Consider the exact sequence

$$0 \longrightarrow H \xrightarrow{\iota} K \xrightarrow{\pi} K/H \longrightarrow 0$$

ι and π being the canonical mappings. As E is flat, the sequence

$$0 \longrightarrow E \otimes_A H \xrightarrow{1_E \otimes \iota} E \otimes_A K \xrightarrow{1_E \otimes \pi} E \otimes_A (K/H) \longrightarrow 0$$

is exact, in other words, $E \otimes_A (K/H)$ is isomorphic to $(E \otimes_A K)/(E \otimes_A H)$, which is 0 by hypothesis, since $E \otimes_A H$ (resp. $E \otimes_A K$) is identified with the image of $1 \otimes \phi$ (resp. the kernel of $1 \otimes \psi$). But the relation $1_E \otimes \pi = 0$ implies $\pi = 0$ by hypothesis, hence $K = H$, which proves that the sequence (3.0.1) is exact at N. Similarly we can show that (3.0.1) is exact at M and P, so (iii) implies (i).

Finally we show the equivalence of (ii) and (iv). If (iv) holds, then $E/\mathfrak{m}E = E \otimes_A (A/\mathfrak{m}) \neq 0$ since $A/\mathfrak{m} \neq 0$, whence (iv). Conversely, suppose that (iv) holds. Then every proper ideal $\mathfrak{a}$ of A is contained in a maximal ideal $\mathfrak{m}$, and the hypothesis $E \neq \mathfrak{m}E$ implies $E \neq \mathfrak{a}E$, in other words, $E \otimes_A (A/\mathfrak{a}) \neq 0$. That is to say, for every cyclic A-module $N \neq 0$, $E \otimes_A N \neq 0$. If now N is any nonzero A-module, it contains a cyclic submodule $N' \neq 0$. Since E is flat, $E \otimes_A N'$ is identified with a subgroup of $E \otimes_A B$ and we have just seen that $E \otimes_A N' \neq 0$, hence $E \otimes_A N \neq 0$. □

An A-module E is called **faithfully flat** if it satisfies the equivalent conditions of Proposition 7.3.1. Note that if E is a faithfully flat A-module, E is a faithful A-module: for, if an element

$a \in A$ is such that $ax = 0$ for all $x \in E$, the homothety $h_a : b \mapsto ab$ in A is such that $1_E \otimes h_a = 0$, whence $h_a = 0$ by property (iii) of Proposition 7.3.1, that is $a = 0$ since A has a unit element.

Example 7.3.2.

(a) The direct sum of a flat module and faithfufly flat module is a faithfully flat module by virtue of property (iv) of Proposition 7.3.1 and Lemma 7.2.3.

(b) As A is faithfully flat by virtue of criterion (iv) of Proposition 7.3.1, it follows from (a) that every free module not reduced to 0 is faithqy flat. On the other hand, there exist non-zero direct factors of free modules (in other words, non-zero projective modules) which are faithful but not faithfully flat.

(c) Let A be a PID. For an A-module E to be faithfully flat, it is necessary and sufficient that it be torsion-free and $E \neq pE$ for every irreducible element p of A. This follows immediately from Proposition 7.2.8 and criterion (iv) of Proposition 7.3.1. In particular, the $\mathbb{Z}$-module $\mathbb{Q}$ is flat but not faithfully flat.

Proposition 7.3.3. *Let E be a faithfully flat A-module and $\phi : N' \to N$ an A-module homomorphism. For ϕ to be injective (resp. surjective, bijective), it is necessary andsuficient that $1_E \otimes \phi : E \otimes_A N' \to E \otimes_A N$ be so.*

Proof. This is an immediate consequence of criterion (i) of Proposition 7.3.1. □

Proposition 7.3.4. *Let $0 \longrightarrow E_1 \longrightarrow E_2 \longrightarrow E_3 \longrightarrow 0$ be an exact sequence of A-modules. Suppose that E_1 and E_3 are flat and that one of them is faithfully flat. Then E_2 is faithfully flat.*

Proof. We know already that E is flat by Proposition 7.2.10. We verify that E has property (ii) of Proposition 7.3.1. Let N be an A-module. As E_3 is flat, there is an exact sequence

$$0 \longrightarrow E_1 \otimes_A N \longrightarrow E_2 \otimes_A N \longrightarrow E_3 \otimes_A N \longrightarrow 0$$

If $E \otimes_A N = 0$, it follows that $E_1 \otimes_A N$ and $E_2 \otimes_A N$ are zero. As one of the modules E_1, E_2 is faithfully fiat, this implies that $N = 0$. □

7.3.1 Extension of scalars and faithfully flatness

Proposition 7.3.5. *Let R, S be two rings, E an R-module and F an (R, S)-bimodule. Suppose that E is faithfully flat. Then for F to be a flat (resp. faithfully flat) S-module, it is necessary and sufficient that $E \otimes_R F$ be so.*

Proof. If F is flat, then $E \otimes_R F$ is flat by Proposition 7.2.19. Suppose that $E \otimes_R F$ is flat and let $v : N' \to N$ be an injective S-module homomorphism. The homomorphism

$$1_E \otimes 1_F \otimes v : E \otimes_R F \otimes_S N' \to E \otimes_R F \otimes_S N$$

is then injective. It follows from Proposition 7.3.3 that $1_F \otimes v : F \otimes_S N' \to F \otimes_S N$ is injective; then F is a flat S-module.

Suppose that F is faithfully flat and let N be a S-module such that $E \otimes_R F \otimes_S N = 0$. Since E is faithfully flat, this implies that $F \otimes_S N = 0$, whence $N = 0$ since F is faithfully flat. This proves that $E \otimes_R F$ is faithfully flat.

Suppose that $E \otimes_R F$ is faithfully fiat and let N be a S-module such that $F \otimes_S N = 0$. Then $E \otimes_R F \otimes_S N = 0$, whence $N = 0$, which shows that F is faithfully flat. □

Corollary 7.3.6. *Let A be a ring and E and F two faithfully flat A-modules. Then the A-module $E \otimes_A F$ is faithfully flat.*

Proposition 7.3.7. *Let $\rho : A \longrightarrow B$ be a ring homomorphism. If E is a faithfully flat A-module, the B-module $\rho_*(E) = E \otimes_A B$ is faithfully flat.*

Proof. Note that the B-module B is faithfully flat, so apply Proposition 7.3.5. □

Corollary 7.3.8. *If E is a faithfully flat A-module and $\mathfrak{a}$ is an ideal of A, then the $(A/\mathfrak{a})$-module $E/\mathfrak{a}E$ is faithfully flat.*

Proof. This follows from $E/\mathfrak{a}E = E \otimes_A (A/\mathfrak{a})$ and Proposition 7.3.7. □

Proposition 7.3.9. *Let $\rho : A \longrightarrow B$ be a ring homomorphism. Suppose that B is a faithfully flat A-module. Then, for an A-module E to be flat (resp. faithfully flat), it is necessary and sufficient that the B-module $\rho_*(E) = E \otimes_A B$ be flat (resp. faithfully flat).*

Proof. If E is flat (resp. faithfully flat), $\rho_*(E)$ is flat (resp. faithfully flat) by Corollary 7.2.21 (resp. by Proposition 7.3.7). Suppose that $\rho_*(E)$ is flat and let $v : N' \longrightarrow N$ be an injective A-module homomorphism. By Corollary 7.2.22, the A-module $E \otimes_A B$ is flat, hence the homomorphism $1_E \otimes 1_B \otimes v$ is injective. As the right and left A-module structures on B coincide, this homomorphlsm is identified with

$$1_E \otimes v \otimes 1_B : E \otimes_A N' \otimes_A B \longrightarrow E \otimes_A N' \otimes_A B$$

As B is a faithfully flat A-module, it follows that $1_E \otimes v$ is injective, which shows that E is flat.

Suppose finally that $\rho_*(E)$ is faithfully flat. First of all E is flat by the argument above. Also let N be an A-module such that $E \otimes_A N = 0$. Then $E \otimes_A N \otimes_A B = 0$, whence $E \otimes_A B \otimes_A B = 0$, which may also be written as $(E \otimes_A B) \otimes_B (B \otimes_A N) = 0$. As $\rho_*(E)$ is a faithfully flat B-module, this implies that $B \otimes_A N = 0$, whence $N = 0$ since B is a faithfully flat A-module. □

Proposition 7.3.10. *Let $\rho : A \longrightarrow B$ be a ring homomorphism. Let E be a faithfully flat B-module. For $\rho^*(E)$ to be a flat (resp. faithfully flat) A-module, it is necessary and sufficient that B be a flat (resp. faithfully flat) A-module.*

Proof. Applying Proposition 7.3.5 with $R = B$, $S = A$, E, $F = B$, it is seen that B is a flat (resp. faithfully flat) A-module if and only if $E \otimes_B B = \rho^*(E)$ is a flat (resp. faithfully flat) A-module. □

Corollary 7.3.11. *Let $\rho : A \longrightarrow B$ be a ring homomorphism. For B to be a faithfully flat A-module, it is sufficient that there exist one faithfully flat B-module which is also a faithfully flat A-module.*

Corollary 7.3.12. *Let $\rho : A \longrightarrow B$ and $v : B \longrightarrow C$ be a ring homomorphisms.*

(a) If C is a faithfully flat B-module and B is a faithfully flat A-module, then C is a faithfully flat A-module.

(b) If C is a faithfuflly flat B-module and a faithfully flat A-module, then B is a faithfully flat A-module.

Proof. Part (a) follows from Proposition 7.3.10, and (b) follows from Corollary 7.3.11. □

7.3.2 Faithfully flat rings

Proposition 7.3.13. *Let $\rho : A \to B$ be a ring homomorphism. Suppose that there exists a B-module E such that $\rho^*(E)$ is a faithfully flat A-module. Then*

(a) For every A-module F, the canonical homomorphism $j : F \to B \otimes_A F$ is injective.

(b) For every ideal $\mathfrak{a}$ of A, $\mathfrak{a}^{ec} = \mathfrak{a}$.

(c) The homomoiphisms ρ is injective.

(d) For every maximal ideal $\mathfrak{m}$ of A, there exists a maximal left ideal $\mathfrak{M}$ of B such that $\mathfrak{M}^c = \mathfrak{m}$.

Proof. We prove (a). We know from **??** that for every B-module M, the canonical A-homomorphism $i : \rho^*(M) \to \rho^*(M) \otimes_A B = \rho_*(\rho^*(M))$ defined by $i(y) = y \otimes 1$ is injective and that the A-module $i(\rho^*(M))$ is a direct factor of $\rho^*(M) \otimes_A B$. Since tensor commutes with direct sum, for every A-module F we have

$$i \otimes 1_F = 1_M \otimes j : \rho^*(M) \otimes_A F \to \rho^*(M) \otimes_A B \otimes_A F$$

is injective. Taking $M = E$, it follows that j is injective. Assertion (b) follows from (a) by taking $F = A/\mathfrak{a}$ and (c) from (b) by taking $\mathfrak{a} = \{0\}$.

Finally, if $\mathfrak{m}$ is a maximal ideal of A, then $\mathfrak{m}^{ec} = \mathfrak{m}$ by (b), and consequently $\mathfrak{m}^e \neq B$. Then there exists a maximal ideal $\mathfrak{M}$ of B containing $\mathfrak{m}^e$, and $\mathfrak{m} \subseteq \mathfrak{M}^c$ with $1 \notin \mathfrak{M}^c$. Consequently $\mathfrak{M}^c = \mathfrak{m}$. □

Corollary 7.3.14. *Under the hypotheses of Proposition 7.3.13, if B is Noetherian (resp. Artinian), so is A.*

Proof. If $(\mathfrak{a}_n)$ is a non-stationary increasing (resp. decreasing) sequence of ideals of A, the sequence $(\mathfrak{a}_n^e)$ of ideals of B is non-stationary and increasing (resp. decreasing) since $\mathfrak{a}_n^{ec} = \mathfrak{a}_n$, contrary to the hypothesis. □

An important application of Proposition 7.3.13 is when B is itself a faithfully flat A-module. But in this case we have the following more precise proposition:

Proposition 7.3.15. *Let $\rho : A \to B$ be a ring homomorphism. The following properties are equivalent:*

(i) The A-module B is faithfully flat.

(ii) The homomorphism ρ is injectioe and the A-module $B/\rho(A)$ is flat.

(iii) The A-module B is flat and, for every A-module F, the canonical homomorphism $F \to B \otimes_A F$ is injective.

(iv) The A-module B is flat and, for every ideal $\mathfrak{a}$ of A, $\mathfrak{a}^{ec} = \mathfrak{a}$.

(v) The A-module B is flat and, for every maximal ideal $\mathfrak{m}$ if A, there exists a maximal ideal $\mathfrak{M}$ of B such that $\mathfrak{M}^c = \mathfrak{m}$.

Proof. By Proposition 7.3.13, (i) implies each of the properties (iii), (iv), (v). On the other hand, if (v) holds, then $\mathfrak{m}^e \neq B$ for every maximal ideal $\mathfrak{m}$ of A, and B is a faithfully flat A-module by criterion (iv) of Proposition 7.3.1, hence (v) implies (i).

We shall now prove that (iii)⇒(iv)⇒(ii)⇒(i), which will complete the proof. In the first place, (iii) implies (iv) by taking $F = A/\mathfrak{a}$ in (iii). If (iv) holds, by taking $\mathfrak{a} = \{0\}$ it follows that f is injective. Condition (iv) and Corollary 7.2.18 imply that $B/\rho(A)$ is a flat A-module, that is (iv) implies (ii). Finally, if (ii) holds, Proposition 7.3.4 applied to the exact sequence

$$0 \longrightarrow A \xrightarrow{\rho} B \longrightarrow B/\rho(A) \longrightarrow 0$$

shows that B is a faithfully flat A-module, since A is faithfully flat. □

Under the conditions of Proposition 7.3.15, let us identify A with a subring of B by means of f. The relation $\mathfrak{a}^{ec} = \mathfrak{a}$ then reads $A \cap B\mathfrak{a} = \mathfrak{a}$. On the other hand, if F is an A-module, F is identified with its image in $B \otimes_A F$ under the canonical mapping $x \mapsto 1 \otimes x$. If F' is a submodule of F, then we denote by BF' the sub-B-module of $B \otimes_A F$ generated by F'. With this notation, we have:

Proposition 7.3.16. *Let B be a ring and A a subring of B such that B is a faithfully flat A-module. Let F be an A-module, F_1, F_2 two submodules of F. Then:*

(a) The canonical mapping $B \otimes_A F_1 \to B \otimes_A F$ is an isomorphism of $B \otimes_A F_1$ onto BF_1.

(b) $F \cap BF_1 = F_1$.

(c) $B(F_1 \cap F_2) = BF_1 \cap BF_2$ and $B(F_1 + F_2) = BF_1 + BF_2$.

Proof. As B is a flat A-module, the canonical mapping $B \otimes_A F_1 \to B \otimes_A F$ is injective. Taking account of the identifications made, its image is BF_1, which proves (a). Assertion (b) follows from Corollary 7.2.18, applied with $E = B$, $E' = A$, and using the formulae. Assertion (c) follows from Proposition 7.2.15. □

Proposition 7.3.17. *Let B be a ring and A a subring of B such that B is a faithfully flat A-module. For an A-module F to be finitely generated (resp. finitely presented), it is necessary and sufficient that the B-module $B \otimes_A F$ be finitely generated (resp. finitely presented).*

Proof. Without any hypothesis on B, clearly, if F is a finitely generated A-module, $B \otimes_A F$ is a finitely generated B-module. Conversely, if $B \otimes_A F$ is a finitely generated B-module, it is generated by a finite number of elements of the form $1 \otimes x_i$, with $x_i \in F$. If M is a sub-A-module of F generated by the x_i and j the canonical injection $M \to F$, then $1_B \otimes j$ is a surjective homomorphism, hence j is surjective, which proves that F is finitely generated.

If F admits a finite presentation, so does $B \otimes_A F$ without any hypothesis on B. It remains to prove that, if $B \otimes_A F$ admits a finite presentation, so does F. We already know that F is finitely generated, hence there exists a surjective homomorphism $\phi : L \to F$, where L is a finitely generated free A-module. Let R be the kernel of ϕ, so that $B \otimes_A R$ is identified with the kernel of the surjective homomorphism $1_B \otimes \phi : B \otimes_A L \to B \otimes_A F$. As $B \otimes_A F$ admits a finite presentation by hypothesis, we conclude that $B \otimes_A R$ is finitely generated (Proposition 7.2.26). Then it follows from the argument above that R is a finitely generated A-module and consequently F admits a finite presentation. □

Proposition 7.3.18. *Let B be a ring and A a subring of B such that B is a faithfully flat A-module. For an A-module F to be projective and finitely generated, it is necessary and sufficient that $B \otimes_A F$ be a finitely generated projective B-module.*

Proof. The condition is obviously necessary without any hypothesis on A or B. We prove that it is sufficient. If a finitely generated projective module admits a finite presentation, the hypothesis implies that F admits a finite presentation by virtue of Proposition 7.3.17, hence, by Proposition 7.2.29 for every A-module M, there is a canonical isomorphism

$$\omega : B \otimes_A \mathrm{Hom}_A(F, M) \to \mathrm{Hom}_B(B \otimes_A F, B \otimes_A M)$$

Then let $\phi : M \to M'$ be a surjective A-module homomorphism and consider the commutative diagram

$$\begin{tikzcd} B \otimes_A \mathrm{Hom}_A(F, M) \arrow[r, "\omega"] \arrow[d, "1_B \otimes \mathrm{Hom}(1_F, \phi)"'] & \mathrm{Hom}_B(B \otimes_A F, B \otimes_A M) \arrow[d, "\mathrm{Hom}(1_{B \otimes_A F}, 1_B \otimes \phi)"] \\ B \otimes_A \mathrm{Hom}_A(F, M') \arrow[r, "\omega"] & \mathrm{Hom}_B(B \otimes_A F, B \otimes_A M') \end{tikzcd}$$

As $1_B \otimes \phi$ is surjective and $B \otimes_A F$ is assumed projective, $\mathrm{Hom}(1_{B \otimes_A F}, 1_B \otimes v)$ is surjective and so then is $1_B \otimes \mathrm{Hom}(1_F, \phi)$. But as B is a faithfully flat A-module, $\mathrm{Hom}(1_F, \phi)$ is itself surjective, hence F is a projective A-module. □

Let $\rho : A \to B$ be a ring homomorphism. We consider the following condition

(PM) There exists a B-module E such that $\rho^*(E)$ is a faithfully flat A-module and for any prime ideal $\mathfrak{P}$ of B, we have $E \otimes_B \kappa(\mathfrak{P}) \neq 0$.

The condition (PM) is satisfied when there exists a finitely generated B-module faithfully flat on A and with support equal to $\mathrm{Spec}(B)$. This is the case, in particular, if the A-module B is faithfully flat. Note that the existence of a B-module faithfully flat over A implies ρ is injective by Proposition 7.3.13 and $\rho^* : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is surjective by Corollary 10.2.41.

Example 7.3.19. Suppose that $\rho : A \to B$ is a local homomorphism of local rings and that there exists a B-module E flat over A and such that $E \otimes_B \kappa(\mathfrak{P}) \neq 0$ for any prime ideal $\mathfrak{P}$ of B. Then E is faithfully flat on A and ρ therefore satisfies the property (PM). In fact we have $E/\mathfrak{m}_B E \neq 0$ and therefore $N \neq \mathfrak{m}_B N$ and a fortiori $E \neq \mathfrak{m}_A E$, so the conclusion follows from Proposition 7.3.1.

Proposition 7.3.20. *Let $\rho : A \to B$ be a ring homomorphism satisfying condition (PM).*

(a) Let $v : A \to A'$ be a ring homomorphism, then the homomorphism $\rho' : A' \to A' \otimes_A B$ satisfies condition (PM).

(b) Let $\mathfrak{P}$ be a prime ideal of A and $\mathfrak{p} = \mathfrak{P}^c$, then the canonical homomorphism $\rho_{\mathfrak{p}} : A_{\mathfrak{p}} \to B_{\mathfrak{P}}$ satisfies (PM).

(c) The going-down property holds for ρ.

Proof. Let E be a B-module such that $\rho^*(E)$ is a faithfully flat A-module and for any prime ideal $\mathfrak{P}$ of B, we have $E \otimes_B \kappa(\mathfrak{P}) \neq 0$. For (a), the A'-module $E' = A' \otimes_A E$ is faithfully flat by

Proposition 7.3.5. Let $\mathfrak{P}'$ be a prime ideal of $B' = A' \otimes_A B$ and $\mathfrak{P}$ its contraction in B. Then we have canonical isomomorphisms

$$E' \otimes_{B'} \kappa(\mathfrak{P}') = E \otimes_B \kappa(\mathfrak{P}') = (E \otimes_B \kappa(\mathfrak{P})) \otimes_{\kappa(\mathfrak{P})} \kappa(\mathfrak{P}')$$

since $E \otimes_A \kappa(\mathfrak{P}) \neq 0$, we see $E' \otimes_{B'} \kappa(\mathfrak{P}') \neq 0$, whence ρ' satisfies condition (PM).

Let $\mathfrak{p}$ and $\mathfrak{P}$ be as in (b). By Proposition 10.3.24, the $A_\mathfrak{p}$ module $E_\mathfrak{P}$ is flat. On the other hand, every prime ideal of $B_\mathfrak{P}$ is of the form $\mathfrak{Q}B_\mathfrak{P}$ where $\mathfrak{Q}$ is a prime ideal of B contained in $\mathfrak{P}$. We have $E \otimes_B \kappa(\mathfrak{Q}) \neq 0$ given the hypothesis made on E, and since $E_\mathfrak{P} \otimes_{B_\mathfrak{P}} \kappa(\mathfrak{Q}B_\mathfrak{P})$ is isomorphic to $E \otimes_B \kappa(\mathfrak{Q}B_\mathfrak{P})$, we have $E_\mathfrak{P} \otimes_{B_\mathfrak{P}} \kappa(\mathfrak{Q}B_\mathfrak{P}) \neq 0$, whence (c) by Example 7.3.19. Now (c) follows from (b) by Corollary 10.2.41. □

Proposition 7.3.21. *Let A be a subring of a ring B. For B be a faithfully flat A-module, it is necessary and sufficient that the following condition holds:*

(LE) Every solution $\boldsymbol{y} \in B^n$ of a linear equation

$$P\boldsymbol{y} = \boldsymbol{b} \tag{3.2.1}$$

with $P \in \mathcal{M}_{mn}(A)$ and $\boldsymbol{b} \in A^m$, is of the form $\boldsymbol{y} = \boldsymbol{x} + Q\boldsymbol{z}$, where $\boldsymbol{x} \in A^n$ is a solution of (3.2.1), $\boldsymbol{z} \in B^k$ and $Q \in \mathcal{M}_{nk}(A)$ is such that $PQ = 0$.

Proof. First assume that B is a faithfully flat A-module. Then, as B is a flat A-module, every solution with elements in M of the homogeneous linear system associated with (3.2.1) is of the form $Q\boldsymbol{z}$, where $\boldsymbol{z} \in B^k$, $Q \in \mathcal{M}_{nk}(A)$ and $PQ = 0$. The problem then reduces to proving that the existence of a solution of (3.2.1) with elements in B implies the existence of one solution with elements in A.

Now if we write $\boldsymbol{p}_j \in A^m$ for the j-th column of P, then (3.2.1) is equivalent to the equation $\sum_{j=1}^n \boldsymbol{p}_j \otimes y_j = \boldsymbol{b}$ in $B \otimes_A A^m = B^m$. In other words, if M is the sub-A-module of A^m generated by the $\boldsymbol{p}_j$, the existence of the solution $\boldsymbol{y}$ of (3.2.1) is equivalent to the relation $\boldsymbol{b} \in BM \cap A^m$. But as $BM \cap A^m \cap B^m = M$, it implies $\boldsymbol{d} \in M$, that is, the existence of a solution $\boldsymbol{x} \in A^m$ of (3.2.1).

Now suppose that the property is satisfied. We know already that B is a flat A-module by Proposition 7.2.12. we prove that, for every ideal $\mathfrak{a}$ of A, $B\mathfrak{a} \cap A = a$, which shows that B is a faithfully flat A-module. Now, let $x \in B\mathfrak{a} \cap A$. There exists by hypothesis $y_i \in B$ and $a_i \in \mathfrak{a}$ such that $\sum_i a_i y_i = x$. The property (LE) applied to this linear equation with coefficients and right hand side in A shows that there exist $x_i \in A$ such that $x = \sum_i a_i x_i$, hence $x \in \mathfrak{a}$. □

7.4 Injective modules

7.4.1 Injective modules

An A-module E is called injective if the functor $\mathrm{Hom}_A(-, E)$ is exact. That is, for any exact sequence of A-modules:

$$0 \longrightarrow M' \xrightarrow{\phi} M \xrightarrow{\psi} M' \longrightarrow 0$$

the sequence obtained by applying $\mathrm{Hom}(-, E)$ is exact:

$$0 \longrightarrow \mathrm{Hom}_A(M'', E) \xrightarrow{\mathrm{Hom}_A(\psi,1)} \mathrm{Hom}_A(M, E) \xrightarrow{\mathrm{Hom}_A(\phi,1)} \mathrm{Hom}_A(M'', E) \longrightarrow 0$$

Since the contravariant functor $\mathrm{Hom}_A(-, E)$ is left-exact, this is equivalent to say, for any injective homomorphism $\phi : M' \to M$, the map

$$\mathrm{Hom}_A(\phi, 1) : \mathrm{Hom}_A(M, E) \to \mathrm{Hom}_A(M', E)$$

is surjective.

Proposition 7.4.1. *Let $(E_i)_{i\in I}$ be a family of A-module and $E = \prod_i E_i$. For the A-module E to be injective, it is necessary and sufficient that each E_i is injective.*

Proof. Let $\phi : M' \to M$ be an injective homomorphism of A-modules. For the product homomorphism $\prod_i \mathrm{Hom}_A(M, E_i) \to \prod_i \mathrm{Hom}_A(M', E_i)$ to be injective, it is necessary and sufficient that each homomorphism $\mathrm{Hom}_A(M, E_i) \to \mathrm{Hom}_A(M', E_i)$ is injective. This shows the claim since $\prod_i \mathrm{Hom}_A(M, E_i)$ is identified with $\mathrm{Hom}_A(M, \prod_i E_i)$. □

Proposition 7.4.2 (Baer). *Suppose that E is an A-module. Then the following conditions are equivalent:*

(i) E is injective;

(ii) any homomorphism $f : \mathfrak{a} \to E$ from an ideal $\mathfrak{a}$ of A to E can be extended to A.

(iii) for any ideal $\mathfrak{a}$ of A and any homomorphism $f : \mathfrak{a} \to E$, there exists $e \in E$ such that $f(a) = ae$ for all $a \in \mathfrak{a}$.

Proof. Suppose that E is injective. Let $\mathfrak{a}$ be an ideal of A, $f : \mathfrak{a} \to E$ an A-homomorphism, and $i : \mathfrak{a} \to A$ the canonical injection. Then the map

$$\mathrm{Hom}_A(i, 1) : \mathrm{Hom}_A(A, E) \to \mathrm{Hom}_A(\mathfrak{a}, E)$$

is surjective. If $g \in \mathrm{Hom}_A(A, E)$ is such that $f = g \circ i$, we have

$$f(a) = g(a) = ag(1)$$

for each $a \in \mathfrak{a}$.

Conversely, suppose the condition in (ii) is satisfied. Let M be an A-module, N a submodule of M, and $\phi : N \to E$ a homomorphism. We must find an extension of ϕ to M. Let $\mathscr{P}$ be the set of pairs (P, ψ) where P is a submodule of M containing N and $\psi : P \to E$ extends ϕ. This set is clearly inductive and nonempty, so by Zorn's lemma we can find a maximal element (P, ψ). It suffices to prove that $P = M$. Let $x \in M$ and let $\mathfrak{a}$ be the ideal of $a \in A$ such that $ax \in P$. Put $f(a) = \psi(ax)$ for $a \in \mathfrak{a}$, by assumption f can be extended to A, so ther exists an element $e \in E$ such that $f(a) = ae$ for $a \in \mathfrak{a}$. Let $P' = P + Ax$ and $\psi' : P' \to E$ be the unique homomorphism such that $\phi'(p + ax) = \psi(p) + ae$ for $p \in P, a \in A$. Then (P', ψ') extends (P, ψ), hence $P' = P$, which means $x \in P$. This completes the proof. □

Corollary 7.4.3. *If the ring A is Noetherian, any direct sum of injective A-modules is injective.*

Proof. Let $(E_i)_{i\in I}$ be a family of injective A-modules, E the direct sum, $\mathfrak{a}$ an ideal of A and $f : \mathfrak{a} \to E$ an A-homomorphism. Since A is Noetherian, $\mathfrak{a}$ is finitely generated, and therefore the canonical map

$$\varphi : \bigoplus_{i\in I} \mathrm{Hom}_A(\mathfrak{a}, E_i) \to \mathrm{Hom}_A(\mathfrak{a}, E)$$

is bijective (if $\mathfrak{a}$ is not finitely generated, φ is only injective). Let (f_i) be the preimage of f by φ. Since each E_i is injective, and the family (f_i) has finite support, there exist elements $(e_i)_{i\in I}$ of E such that $f_i(a) = ae_i$ for $a \in \mathfrak{a}$ and $i \in I$, hence $f(a) = a((e_i))$ for each $a \in \mathfrak{a}$, whence E is injective. □

Suppose that A is integral, We say an A-module E is **divisible** if the homothety a_E is injective for every nonzero element a of A.

Corollary 7.4.4. *Suppoe that A is an integral domain.*

(a) Any injective A-module is divisible.

(b) Any torsion free A-module is divisible and injective.

(c) If A is a PID, any divisible A-module is injective.

Proof. If $a \in A$ is nonzero, then a_A is injective; for any A-module E, the homothety a_E is identified with

$$\mathrm{Hom}(a_A, 1_E) = \mathrm{Hom}_A(A, E) \to \mathrm{Hom}_A(A, E)$$

hence E is divisible if $\mathrm{Hom}(a_E, 1_E)$ is surjective for any $a \in A$ nonzero. Assertion (a) then follows.

Let E be a divisible A-module; suppose that A is principal (resp. E is torsion-free) and we show that E is injective by applying Proposition 7.4.2. Let $\mathfrak{a}$ be an ideal of A and $f : \mathfrak{a} \to E$ a homomorphism. Let $x \in \mathfrak{a}$ be such that $\mathfrak{a} = Ax$ (resp. such that $x \neq 0$ if $\mathfrak{a} \neq 0$), and $e \in E$ such that $f(x) = xe$. Then for any $a \in \mathfrak{a}$, we have $f(a) = ae$: this is clear if $a \in Ax$, which proves our assertion if A is principal; if E is torsion free, then since $xa \in \mathfrak{a}$, we have $xf(a) = f(ax) = axe$, hence $f(a) = ae$ (since x is nonzero if $\mathfrak{a} \neq 0$). □

7.4.2 Injective modules and cogenerators

Proposition 7.4.5. *Let B be a ring, F a B-module, and P a (B, A)-bimodule. If E is an injective B-module and P is a flat A-module, then* $\mathrm{Hom}_B(P, E)$ *is an injective A-module.*

Proof. Let $\phi : M' \to M$ be an injective homomorphism of A-modules. We have a commutative diagram

$$\begin{tikzcd}
\mathrm{Hom}_A(M, \mathrm{Hom}_B(P, E)) \arrow[r, "\mathrm{Hom}_A(\phi,1)"] \arrow[d] & \mathrm{Hom}_A(M', \mathrm{Hom}_B(P, E)) \arrow[d] \\
\mathrm{Hom}_B(P \otimes_A M, E) \arrow[r, "\mathrm{Hom}_B(1_P\otimes\phi,1_E)"] & \mathrm{Hom}_B(P \otimes M', E)
\end{tikzcd}$$

where the vertical homomorphisms are canonical isomorphisms. Since P is flat over A, the homomorphism $1_P \otimes \phi : P \otimes_A M' \to P \otimes_A M$ is injective. Since E is injective, $\mathrm{Hom}_B(1_P \otimes \phi, 1_E)$ is surjective, hence so is $\mathrm{Hom}_A(\phi, 1)$, which shows $\mathrm{Hom}_B(P, E)$ is injective. □

We say a A-module E is a **cogenerator** if, for each A-module M and a nonzero element x of M, there exists a homomorphism $\phi : M \to E$ such that $\phi(x) \neq 0$. This concept is the dual of that of a generator: an A-module L is called a generator if, for each A-module M and a nonzero element x of M, there exist a homomorphism $\phi : L \to M$ such that $x \in \phi(L)$. For example, the A-module A is a generator.

Proposition 7.4.6. *Let E be an injective A-module. For E to be a cogenerator, it is necessary and sufficient that* $\mathrm{Hom}_A(S, E) \neq 0$ *for any simple A-module S.*

Proof. This condition is clearly necessary. Conversely, let M be an A-module and x a nonzero element of M; the submodule Ax of M has a simple quotient S. If $\mathrm{Hom}_A(S, E) \neq 0$, then $\mathrm{Hom}_A(Ax, E) \neq 0$ and there exist a homomorphism $\phi : Ax \to E$ such that $f(x) \neq 0$. Since E is injective, ϕ can be then extended to a homomorphism from M to E, which maps x to a nonzero element. This shows E is a cogenerator. □

Example 7.4.7. We know the $\mathbb{Z}$-module $\mathbb{Q}/\mathbb{Z}$ is injective since it is divisible. We now show that it is a cogenerator. In fact, any simple $\mathbb{Z}$-module is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ for some $p \neq 0$, and $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Q}/\mathbb{Z})$ is nonzero: for example, it contains the map induced by the homomorphism $x \mapsto x/p$ from $\mathbb{Z}$ to $\mathbb{Q}$.

Proposition 7.4.8. *Let B be a ring, E a injective B-module that is a cogenerator, P a (B, A)-bimodule. Suppose that P is flat over A and $P \otimes_A S \neq 0$ for any simple A-module S (i.e., faithfully flat over A). Then the A-module* $\mathrm{Hom}_B(P, E)$ *is injective and a cogenerator.*

Proof. In fact, $\mathrm{Hom}_B(P, E)$ is injective by Proposition 7.4.5. For any simple A-module S, $\mathrm{Hom}_A(\mathrm{Hom}_B(P, E))$ is isomorphic to $\mathrm{Hom}_B(P \otimes_A S, E)$, hence is nonzero since $P \otimes_A S \neq 0$ and the B-module E is a cogenerator; the A-module $\mathrm{Hom}_B(P, E)$ is then a cogenerator by Proposition 7.4.6. □

Corollary 7.4.9. *The A-module $E_A = \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})$ is injective and a cogenerator.*

Proof. Apply Proposition 7.4.8 to $B = \mathbb{Z}$, $E = \mathbb{Q}/\mathbb{Z}$ and $P = A$. □

For any A-module M, put $I^0(M) = (E_A)^{\mathrm{Hom}_A(M, E_A)}$ and let $e_M : M \to I^0(M)$ be the homomorphism such that, for $m \in M$,

$$e_M(m) = (\varphi(m))_{\varphi \in \mathrm{Hom}_A(M, E_A)}.$$

Corollary 7.4.10. *The A-module $I^0(M)$ is injective and the homomorphism e_M is injective.*

Proof. The module $I^0(M)$ is injective since E_A is injective (Proposition 7.4.1). The map e_M is injective since E_A is a cogenerator (by the definition of e_M). □

Corollary 7.4.11. *Every A-module is isomorphic to a submodule of an injective A-module.*

Corollary 7.4.12. *For an A-module E to be injective, it is necessary and sufficient that for injective homomorphism $\phi : E \to F$ has an A-linear retraction.*

Proof. Suppose that E is injective and $\phi : E \to F$ is an injective homomorphism. Then

$$\mathrm{Hom}_A(\phi, 1_E) : \mathrm{Hom}_A(F, E) \to \mathrm{Hom}_A(E, E)$$

is surjective; there then exists $\psi \in \mathrm{Hom}_A(F, E)$ such that $\psi \circ \phi = 1_E$, so ψ is a retraction of ϕ. Conversely, there exists an injective A-module I and an injective homomorphism $\phi : E \to I$; if ϕ has a retraction, then E is injective by Proposition 7.4.1. □

7.4.3 Injective hull of modules

Let M be an A-module and N be a submodule of M. The module M is said to be an essential extension of N (or N is said to be an **essential submodule** M) if for every submodule P of M, $P \cap N = \{0\}$ implies $P = \{0\}$. An injective hull of M is defined to be a pair (I, i), where I is an injective A-module and $i : M \to I$ is a homomorphism such that I is an essential extension of $i(M)$. We note that in particular i is injective, so we can identify M with the image $i(M)$ in I, and we then then say that I is an injective hull of M.

Example 7.4.13. Suppose that A is integral and M is torsion-free. Let K be the fraction field of A and $i : M \to K \otimes_A M$ be the canonical homomorphism. Then $(K \otimes_A M, i)$ is an injective hull of M (Corollary 7.4.4).

Theorem 7.4.14. *Let M be an A-module.*

(a) M has an injective hull.

(b) If (I, i) and (J, j) are two injective hulls of M, there exist an isomorphism $\phi : I \to J$ such that $\phi \circ i = j$.

Proof. By Corollary 7.4.11, we can suppose that M is a submodule of an injective A-module E. Consider the set $\mathscr{F}$ of submodules I of E containing M and such that the canonical injection $i : M \to I$ makes I an essential extension of M, and order $\mathscr{F}$ by inclusion. Since $\mathscr{F}$ is inductive, it has a maximal element I. It then suffices to prove that I is a direct factor of E, which shows it is injective. Let N be a submodule of E such that $N \cap I = 0$, and maximal with this property. The homomorphisms

$$I \xrightarrow{\iota} E \xrightarrow{\pi} E/N$$

have injective composition. Since E is injective, there exist a homomorphism $\psi : E/N \to E$ such that $\iota = \psi \circ \pi \circ \iota$, which means $\psi(\pi(x)) = x$ for $x \in I$.

$$\begin{tikzcd} I \arrow[r, "\iota"] \arrow[dr, "\iota"'] & E \arrow[r, "\pi"] & E/N \arrow[dl, "\psi"] \\ & E & \end{tikzcd}$$

Put $I' = \mathrm{im}\,\psi$ and $i' : M \to I'$ the canonical injection. Then $I \subseteq I'$, and it suffices to show that I' is an essential extension of M, since then $I = I'$ and $\psi \circ \pi$ is a projection of E to I.

Now let P be a submodule of I' such that $P \cap M = \{0\}$. We have $P = \psi \circ \pi(Q)$, where Q is a submodule of E containing N; moreover,

$$Q \cap M = \psi \circ \pi(Q \cap M) \subseteq P \cap M = \{0\}$$

hence $Q \cap I = \{0\}$ (the extension $M \to I$ is essential). By the maximality of N, this implies $Q = N$, which means $\pi(Q) = 0$ and hence $P = 0$. This proves the first claim.

Now let (I, i) and (J, j) be two injective hulls of M. Since J is injective, there exists a homomorphism $\phi : I \to J$ such that $\phi \circ i = j$; we have

$$i^{-1}(\ker \phi) = \ker j = \{0\}$$

hence $\ker \phi = 0$ and ϕ is injective. Then $\phi(I)$ is an injective submodule of J, hence a direct factor. Let P be a submodule of J such that $P \cap \phi(I) = \{0\}$. Then since $\phi(i(M)) = j(M) \subseteq \phi(I)$, we have $P \cap j(M) = \{0\}$, whence $P = 0$ since j is an essential extension. This implies $\phi(I) = J$ and ϕ is bijective. □

Remark 7.4.1. Let (I, i) be an injective hull of M and $j : M \to J$ an injective homomorphism of M to an injective A-module J. By the above argument, there exist an injective homomorphism $\phi : I \to J$ such that $\phi \circ i = j$.

Proposition 7.4.15. *Let I be a nonzero injective A-module. The following conditions are equivalent:*

(i) I is indecomposable;

(ii) the intersection of any two nonzero submodules of I is nonzero;

(iii) I is an injective hull of it nonzero submodules;

(iv) the ring $\mathrm{End}_A(I)$ is local.

Proof. Assume that I is indecomposable and let M be a nonzero module of I. Then there exists a submodule I' of I which is an injective hull of M (Remark 7.4.1). Since I' is nonzero and a direct factor of I, we have $I = I'$ if I is indecomposable. This proves (i)⇒(iii).

Now assume (iii), and let E, F be two submodules of M such that $E \cap F = \{0\}$. If $E \neq \{0\}$, then I is an injective hull of E, so $F = 0$ (since I is an essential extension of E). This shows (ii); also, we see (ii) implies (i).

The implication (iv)⇒(i) is given in **??**. Conversely, suppose that I is indecomposable. Note first that any injective endomorphism ϕ of I is bijective (since $\phi(I)$ is then a nonzero direct factor submodule of I). Moreover, any endomorphism ϕ of I, whose restriction to a nonzero submodule E of I is injective, is injective (indeed, since (i)⇒(iii), I is an injective hull of E, so $E \cap \ker \phi = 0$ implies $\ker \phi = 0$). That being the case, let ϕ be a non-invertible element of $\mathrm{End}_A(M)$; according to **??**, we have to prove that $1 - \phi$ is invertible. Since ϕ is not injective, we have $\ker \phi \neq 0$; as the restriction of $1 - \phi$ to $\ker \phi$ is injective, $1 - \phi$ is injective, therefore bijective. □

Corollary 7.4.16. *Let M be an A-module, I an injective hull of M. For I to be indecomposable, it is necessary and sufficient that the intersection of two nonzero submodules of M is nonzero.*

Proof. This condition is necessary by Proposition 7.4.15. Conversely, if I is a direct sum of nonzero submodules I_1, I_2, then

$$I_1 \cap M \neq \{0\}, \quad I_2 \cap M \neq \{0\}, \quad (I_1 \cap M) \cap (I_2 \cap M) = \{0\}$$

which contradicts the assumption. □

Lemma 7.4.17. *Let M be a Noetherian nonzero A-module, I an injective hull of M. Then I has an indecomposable injective submodule.*

Proof. We can clearly suppose that M is a submodule of I. Let N be a submodule of M, such that I is not an injective hull of N and maximal for this property. By Remark 7.4.1 there exists a submodule I_1 of I that is an injective hull of N; then I_1 is a direct factor of I, let J be its complement. We have $J \neq 0$. If J' is a nonzero direct factor of J, we have $J' \cap M \neq \{0\}$ and

$$(J' \cap M) \cap N \subseteq J' \cap I_1 = \{0\}.$$

The submodule $N' = (J' \cap M) + N$ of M is then the direct sum of $J' \cap M$ and N, hence strictly contains N. Moreover N' is contained in the submodule $J' + I_1$ of J, which is a direct sum, therefore injective. By the maximality of N, we then have $J' + I_1 = I$, hence $J' = J$, and J is therefore indecomposable. □

Let $\mathscr{I}$ be the set of classes of injective indecomposable A-modules. We reclal (Corollary 7.4.3) that, if A is Noetherian, any direct sum of injective A-modules is injective.

Theorem 7.4.18. *Let I be an injective A-module.*

(a) If I is an injective hull of a Noetherian A-module M, I is the direct sum of a finite family of (injective) indecomposable submodules.

(b) If A is Noetherian, I is a direct sum of a family of (injective) indecomposable submodules.

(c) If I is a direct sum of a family of (injective) indecomposable submodules, there exist a unique family of cardinals $(\alpha_E)_{E\in\mathscr{I}}$ and a such that I is isomorphic to $\bigoplus_{E\in\mathscr{I}} E^{\oplus\alpha_E}$.

Proof. We note that (c) follows from **??** and **??**. Now we prove (a). Let N be a submodule of M whose injective hull is a direct sum of a finite family of indecomposable submodules, and maximal for this property (there are some since M is noetherian). According to Remark 7.4.1, there exists a submodule I_1 of I which is an injective envelope of N. If $I_1 = I$, the claim is proved. Otherwise, let J be a complement of I_1 in I. Then J is an injective hull of the Noetherian module $J \cap M$, hence has a injective indecomposable submodule J' (Lemma 7.4.17). Then $I_1 + J'$ is injective, a direct sum of injective indecomposable submodules, and an injective hull of the submodule $(I_1 + J') \cap M$ of M which strictly contains N. This contradicts the maximality of N, whence our claim.

Suppose now A is Noetherian. Let X be the union of the sets $\mathrm{Hom}_A(E, I)$ for $E \in \mathscr{I}$. To each subset Y of X we associate an A-module E_Y and a homomorphism $f_Y : E_Y \to I$ in the following way: Y is the union of a family $(Y(E))_{E\in\mathscr{I}}$ where $Y(E) \subseteq \mathrm{Hom}_A(E, I)$, we set

$$E_Y = \bigoplus_{E\in\mathscr{I}} E^{\oplus Y(E)}$$

and the component of f_Y on the direct factor of E_Y corresponding to the element y of $Y(E) \subseteq \mathrm{Hom}_A(E, I)$ is $y : E \to I$ (i.e., the action of f_Y on the y-th component is determined by y). Let Y be a subset of Y such that f_Y is injective and Y is maximal with respect to this property. It suffices to prove that f_Y is bijective. If not, let J be a complement of the injective submodule $\mathrm{im}\, f_Y$ of I. Since J is nonzero, it possesses a Noetherian nonzero submodule (since A is Noetherian), hence a nonzero injective submodule J' which is an injective hull of a Noetherian module. By (a), J' is a nonempty direct sum of a finite family of (injective) indecomposable submodules. There then exists a finite nonempty subset Y' of X such that $f_{Y'}$ maps bijectively from $E_{Y'}$ to J'.

Since $\operatorname{im} f_Y \cap J' = \{0\}$, we have $Y \cap Y' = \varnothing$ and $f_{Y \cup Y'}$ is injective; this contradicts the maximality of Y, whence our assertion. $\square$

Chapter 8

Homological algebras for modules

8.1 Complexes of modules

In this paragraph, we let A be a commutative ring with unit. Without further specifying, all A-modules refers to left A-modules, and all graded modules are of type $\mathbb{Z}$. If M is a graded A-module with graduation $(M_n)_{n\in\mathbb{Z}}$, we set $M^n = M_{-n}$ and say M_n (resp. M^n) is the homogeneous component of descending degree n (resp. of ascending degree n) of M. If $\phi : M \to N$ is a graded homomorphism of degree p of graded A-modules, we note $\phi_n : M_n \to N_{n+p}$ (resp. $\phi^n : M^n \to N^{n-p}$) the homomorphism deduced from ϕ; it is called the homogeneous component of descending degree (resp. ascending) n of ϕ; we also say that ϕ is of descending degree p or of ascending degree $-p$.

8.1.1 Complexes of A-modules

A **differential complex** (or simple complex) of A-modules is a pair (M, d) formed by a graded A-module M and a graded endomorphism $d : M \to M$ of descending degree -1 such that $d \circ d = 0$.

If M_n (resp. M^n) is the homogeneous component of descending (resp. ascending) degree n of M, the datum of d is equivalent to that of the sequence of homomorphisms

$$\cdots \longrightarrow M_{n+1} \xrightarrow{d_{n+1}} M_n \xrightarrow{d_n} M_{n-1} \longrightarrow \cdots$$

resp.

$$\cdots \longrightarrow M^{n-1} \xrightarrow{d^{n-1}} M^n \xrightarrow{d^n} M^{n+1} \longrightarrow \cdots$$

such that $d_n \circ d_{n+1} = 0$ (resp. $d^n \circ d^{n-1} = 0$) for each $n \in \mathbb{Z}$. By abuse of language, we will also call complex the data of such a sequence of A-modules and homomorphisms.

Any graded A-module will be tacitly considered as a complex in providing zero differential; the complexes thus obtained will be called complexes with zero differential. In particular, any A-module M will be equipped with the unique structure of A-complex such that $M_0 = M^0 = M$. The complex (M, d) is said to be zero if M is reduced to 0. In the following, we denote by 0 a zero complex.

Adjointing the ordered set $\mathbb{Z}$ with elements $-\infty$ and $+\infty$, we denote by $\overline{\mathbb{Z}}$ the obtained set, and extend the order relation on $\mathbb{Z}$ to $\overline{\mathbb{Z}}$ by defining $-\infty < n < +\infty$ for any $n \in \mathbb{Z}$. The set $\overline{\mathbb{Z}}$ then

has maximal and minimal elements. If M is a complex, we define the left and right bounds of M to be the elements $b_l(M)$ and $b_r(M)$ of $\overline{Z}$ by

$$b_l(M) = \sup\{n \in \mathbb{Z} : M_n \neq 0\}, \quad b_r(M) = \inf\{n \in \mathbb{Z} : M_n \neq 0\}.$$

We say M is **positive** if $b_r(M) \geq 0$, and **left bounded** if $b_l(M) \neq +\infty$. Similarly, M is **negative** if $b_l(M) \leq 0$, and **right bounded** if $b_r(M) \neq -\infty$. Finally, we say M is **bounded** if it is left bounded and right bounded. The length of M, denote by $l(M)$, is the element $\overline{\mathbb{Z}}$ defined by the following: if M is zero then $l(M) = -\infty$; if M is bounded and nonzero, $l(M) = b_r(M) - b_l(M)$; if M is not bounded, $l(M) = +\infty$.

We say the complex (M, d) is free, projective, flat, injective, if each of its component M_n is. We note that the complex (M, d) is projective or flat if and only if the module M is (Lemma 7.2.3), but M can be free without the complex (M, d) being free (since a direct factor of a module free is not always free), just as (M, d) can be injective without M being injective.

Let (M, d) be a complex. We set $Z(M, d) = \ker d$ and $B(M, d) = \operatorname{im} d$. These are graded submodules of M, which are called **cycles** and **boundaries** of (M, d). The homogeneous components of $Z(M, d)$ and $B(M, d)$ are denoted by $Z_n(M, d) = Z^{-n}(M, d)$ and $B_n(M, d) = B^{-n}(M, d)$. We have

$$Z_n(M, d) = \ker d_n, \quad B_n(M, d) = \operatorname{im} d_{n+1}, \quad Z^n(M, d) = \ker d^n, \quad B^n(M, d) = \operatorname{im} d^{n-1}.$$

Since $d \circ d = 0$, we have $B(M, d) \subseteq Z(M, d)$; two cycles are then said to be **homologous** if their difference is a boundary. The quotient graded module $H(M, d) = Z(M, d)/B(M, d)$ and called the **homology module** of (M, d). Its elements are called the homology classes, and the homogeneous components of $H(M, d)$ are denoted by $H_n(M, d) = H^{-n}(M, d)$.

Example 8.1.1. If M has zero differentials, then $Z(M) = M$ and $B(M) = 0$, and $H(M)$ is identified with M.

Let (M, d) and (N, d) be complexes (note that here we do not distinguish differentials of M and N and we denote them by d). A **morphism** of (M, d) to (N, d) is a graded A-homomorphism α of degree 0 from M to N such that

$$d \circ \alpha = \alpha \circ d.$$

We use $\operatorname{Hom}_{C(A)}(M, N)$ to denote the set of morphisms from M to N (here $C(A)$ means the category of complexes of A-modules). If α is such a morphism, then for each n, we have $d_n \circ \alpha_n = \alpha_{n-1} \circ d_n$ and $d^n \circ \alpha^n = \alpha^{n+1} \circ d^n$. Note that

$$\alpha(Z(M)) \subseteq Z(N), \quad \alpha(B(M)) \subseteq B(N)$$

so we get induced maps

$$Z(\alpha) : Z(M) \to Z(N), \quad B(\alpha) : B(M) \to B(N), \quad H(\alpha) : H(M) \to H(N).$$

The homogeneous components of them are denoted by $Z_n(\alpha)$, $Z^n(\alpha)$, ect. It is easy to check that these definitions behave well for addition and composition of morphisms, and therefore are functorial. If the homomorphism $H(\alpha)$ is bijective, we say α is a **quasi-isomorphism**.

We say a complex (M, d) is **null-homologous** if $H(M) = 0$, which means the canonical morphism $0 \to M$ (resp. $M \to 0$) is a quasi-isomorphism. We say (M, d) is acyclic at descending degree n (resp. ascending degree n) if $H_n(M) = 0$ (resp. $H^n(M) = 0$).

Let (M, d) be a complex and $r \in \mathbb{Z}$. The **r-fold translation** of (M, d) is the complex $(M[r], d[r])$ defined by the following: $M[r]$ is the A-module obtained by descending the graduation of M by r:

$$M[r]_n = M_{n+r}, \quad M[r]^n = M^{n-r}$$

and in particular $M[r]_0 = M_r$; we also note that M is the direct sum of its graded submodules $M[-r]_r$ for $r \in \mathbb{Z}$ (resp. $M[r]^r$ for $r \in \mathbb{Z}$). We put $d[r] = (-1)^r d$, so that $Z(M[r]) = Z(M)[r]$, $B(M[r]) = B(M)[r]$ and $H(M[r]) = H(M)[r]$. For example, we see d is a morphism of M to $M[-1]$ and

$$H(d) : H(M) \to H(M)[-1]$$

is zero. For a morphism $\alpha : M \to N$ and $r \in \mathbb{Z}$, we then have a morphism $\alpha[r] : M[r] \to N[r]$ and

$$\alpha[r]_n = \alpha_{n+r}, \quad \alpha[r]^n = \alpha^{n-r}.$$

On the set $A \times A$, the following definition

$$(a, b) + (a', b') = (a + a', b + b')$$

$$(a, b)(a', b') = (aa', ab' + ba')$$

give a ring structure on $A \times A$, denoted by $A(\varepsilon)$, whose unit is $1 = (1, 0)$. The injection $a \mapsto (a, 0) = a1$ then identify A with a subring of $A(\varepsilon)$. The A-module $A(\varepsilon)$ is free with basis $\{1, \varepsilon\}$ where $\varepsilon = (0, 1)$; we have $\varepsilon^2 = 0$ and ε is central in $A(\varepsilon)$. If A is commutative, $A(\varepsilon)$ is an algebra of dual numbers over A.

Endow $A(\varepsilon)$ with the graduation such that $A(\varepsilon)_0 = A \cdot 1$, $A(\varepsilon)_{-1} = A \cdot \varepsilon$, and $A(\varepsilon)_n = 0$ for $n \neq 0$. It is clear that giving a structure of A-complex on a set M amounts to giving on M a structure of graded $A(\varepsilon)$-modulus, where the differential d corresponding to the homothety ε_C. Similarly, morphisms of complexes correspond to graded homomorphism of graded $A(\varepsilon)$-modules of degree 0. The category of graded $A(\varepsilon)$-modules is then equivalent to the category of complexes of A-modules. We can then apply the theory of graded modules to complexes.

The notion of graded sub-$A(\varepsilon)$-module then corresponds that of sub-complexes: a subcomplex of the complex (M, d) is therefore a graded submodule N of M such that, for all $n \in \mathbb{Z}$, $d_n(N_n) \subseteq N_{n-1}$; if we denote restrict the differential d on N, then (N, d) is a complex structure, called induced by (M, d). Without further specifying, any sub-complex will be provided with of the induced structure. Similarly, we can explain the notions of quotient complexes, exact sequence of complexes, kernel, cokernel, image of a morphism of complex. Also, we have the notations of direct sum of complexes, inductive system and inductive limit of complexes.

Let (M_i, d_i) be a family of complexes. We define the product $\prod_i M_i$ to be the complex M defined by the following:

(a) For each $n \in \mathbb{Z}$, M_n is the product A-module $\prod_i (M_i)_n$.

(b) For each $n \in \mathbb{Z}$, the differential $d_n : M_n \to M_{n-1}$ is the product of the components $(d_i)_n$.

If I is finite, $\prod_i M_i$ is equal to $\bigoplus_i M_i$. We note that in general, the A-module $\prod_i M_i$ is not the

product of the A-modules M_i.

Consider a family (resp. an direct family) $(M_i)_{i\in I}$ of complexes. Let M be the direct sum (resp. direct limit) of M_i, and $\alpha_i : M_i \to M$ the canonical morphism. Then the homomorphism $H(\alpha_i) : H(M_i) \to H(M)$ then defines a canonical homomorphism $\bigoplus_i H(M_i)$ (resp. $\varinjlim H(M_i)$) to $H(M)$. Similarly, the projections $\prod_i M_i \to M_i$ defines a graded homomorphism of degree 0, called canonical, from $H(\prod_i M_i)$ to $\prod_i(H(M_i))$.

Proposition 8.1.2. *For any family $(M_i)_{i\in I}$ of complexes, the canonical homomorphisms*

$$\bigoplus_i H(M_i) \to H(\bigoplus_i M_i), \quad H(\prod_i M_i) \to \prod_i H(M_i)$$

are bijective. Moreover, for any direct system (M_i) of complexes, the canonical homomorphism

$$\varinjlim_i H(M_i) \to H(\varinjlim_i M_i)$$

is bijective.

Proof. This result follows from **??**, **??** and **??**. □

8.1.2 Long exact homological sequence

In this part, we consider a short exact sequence of complexes:

$$0 \longrightarrow L \xrightarrow{\alpha} M \xrightarrow{\beta} N \longrightarrow 0$$

Let Γ be the set of elements $x \in M$ such that $dx \in \operatorname{im}\alpha$. For $x \in \Gamma$, we have

$$d(\alpha^{-1}(dx)) = \alpha^{-1}(dd(x)) = 0, \quad d\beta(x) = \beta(dx) \in \operatorname{im}(\beta \circ \alpha) = 0$$

so $\alpha^{-1}(dx) \in Z(L)$ and $\beta(x) \in Z(N)$. Consider then the homomorphism $\varphi : \Gamma \to H(N) \times H(L)$ defined by

$$\varphi(x) = (\beta(x), \alpha^{-1}(dx)).$$

Lemma 8.1.3. *The image $\varphi(\Gamma)$ of Γ in $H(N)\times H(L)$ is the graph of a homomorphism of degree -1 from $H(N)$ to $H(L)$.*

Proof. If $x \in \Gamma$ and if $\beta(x) \in B(N)$, then $\alpha^{-1}(dx) \in B(L)$: in fact, there exist $y \in N$ such that $\beta(x) = dy$, also $z \in N$ such that $y = \beta(z)$. Then $\beta(x) = d\beta(y) = \beta(dy)$, so $x - dy = \alpha(t)$ for some $t \in L$. This being so, we have $dx = d\alpha(t) = \alpha(dt)$, so $\alpha^{-1}(dx) = dt \in B(L)$. Also, since β is surjective, any element of $Z(N)$ is the image under β of some x in M such that $\beta(dx) = 0$, i.e., $dx \in \operatorname{im}\alpha$, which means $x \in \Gamma$. We then conclude that $\varphi(\Gamma)$ is the graph of a function. Since φ is bihomogeneous of bidegree $(0, -1)$, the claim follows. □

The graded homomorphism of degree -1 from $H(N)$ to $H(L)$ is called the connecting homomorphism relative to the exact sequence (α, β). We denote it by $\partial(\alpha, \beta)$ or $\partial_{\alpha,\beta}$, or simply ∂. Its homogeneous components are denoted by

$$\partial_n(\alpha, \beta) : H_n(N) \to H_{n-1}(L), \quad \partial^n(\alpha, \beta) : H^n(N) \to H^{n+1}(L).$$

By definition, to construct the image of a class $\gamma \in H_n(N)$, we choose a cycle $y \in Z_n(N)$ whose class is γ, and an element x in M_n such that $\beta(x) = y$. Then dx is of the form $\alpha(t)$, $t \in L_{n-1}$, and $\partial(\gamma)$ is defined to be the class of t. In other words, $\partial_n(\alpha, \beta)$ is obtained from the correspondence $\alpha_{n-1}^{-1} \circ d_n \circ \beta_n^{-1}$ from N_n to L_{n-1}, by passing to subsets $Z_n(N)$ and $Z_{n-1}(L)$, then to their quotients $H_n(N)$ and $H_{n-1}(L)$. This then shows that, if we replace L, M, N and α, β by $L[r], M[r], N[r]$ and $\alpha[r], \beta[r]$, then

$$\partial(\alpha[r], \beta[r]) = (-1)^r \partial(\alpha, \beta).$$

Similarly, if λ and μ are invertible elements in the center of A, then

$$\partial(\lambda\alpha, \mu\beta) = \lambda^{-1}\mu^{-1}\partial(\alpha, \beta).$$

The homomorphism $\partial(\alpha, \beta)$ can also be deduced from the snake lemma. For this, just note that the diagram

$$\begin{tikzcd}
 & L_n/B_n(L) \arrow[r, "\alpha_n"] \arrow[d] & M_n/B_n(M) \arrow[r, "\beta_n"] \arrow[d] & N_n/B_n(N) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & Z_{n-1}(L) \arrow[r, "Z_{n-1}(\alpha)"] & Z_{n-1}(M) \arrow[r, "Z_{n-1}(\beta)"] & Z_{n-1}(N) &
\end{tikzcd}$$

commutes with two row exact. The homomorphism $\partial(\alpha, \beta)$ is then the connecting homomorphism in the snake lemma.

Theorem 8.1.4. *The short exact sequence induces a long exact sequence*

$$\cdots \longrightarrow H_{n+1}(N) \xrightarrow{\partial_{n+1}} H_n(L) \xrightarrow{H_n(\alpha)} H_n(M) \xrightarrow{H_n(\beta)} H_n(N) \longrightarrow \cdots$$

Corollary 8.1.5. *If two of the complexes L, M, N are null-homologous, then the third one is null-homologous. For the morphism α (resp. β) to be a quasi-isomorphism, it is necessary and sufficient that N (resp. L) is null-homologous. For $\partial(\alpha, \beta)$ to be bijective, it is necessary and sufficient that M is null-homologous.*

Corollary 8.1.6. *Let α be a morphism of complexes. If* $\ker \alpha$ *and* $\operatorname{coker} \alpha$ *are null-homologous, then α is a quasi-isomorphism.*

Proposition 8.1.7. *Consider a commutative diagram of complexes with exact rows:*

$$\begin{tikzcd}
0 \arrow[r] & L \arrow[r, "\alpha"] \arrow[d, "u"] & M \arrow[r, "\beta"] \arrow[d, "v"] & N \arrow[r] \arrow[d, "w"] & 0 \\
0 \arrow[r] & L' \arrow[r, "\alpha'"] & M' \arrow[r, "\beta'"] & N' \arrow[r] & 0
\end{tikzcd}$$

Then $H(u) \circ \partial(\alpha, \beta) = \partial(\alpha', \beta') \circ H(w)$.

Proof. Let z be a cycle in $H(N)$ and x an element of M such that $\beta(x) = z$. Then we have

$$\begin{aligned}(\partial_{\alpha',\beta'} \circ H(w))(z) &= \partial_{\alpha',\beta'}(w(z)) = (\alpha')^{-1}(dv(x)) = u(\alpha^{-1}(dx)) \\ &= H(u)(\alpha^{-1}(dx)) = H(u) \circ \partial_{\alpha,\beta}(z),\end{aligned}$$

so the claim follows. □

Example 8.1.8. Let M be a complex. Consider the canonical exact sequence

$$0 \longrightarrow Z(M) \longrightarrow M \longrightarrow B(M)[-1] \longrightarrow 0$$

and let $i : B(M) \to Z(M)$ be the canonical injection. Then the connecting homomorphism $\partial : H(B(M))[-1] \to H(Z(M))[-1]$ is identified with $H(i)[-1]$.

8.1.3 Homotopies

Let (M, d) and (N, d) be two complexes, α and β be morphisms from M to N. A **homotopy** from α to β is defined to be a graded A-homomorphism h of degree 1 from M to N such that

$$\beta - \alpha = d \circ h + h \circ d. \tag{1.3.1}$$

We say f and g are homotopic if there exists such a homotopy.

If γ is another morphism from M to N and h (resp. s) is a homotopy from α to β (resp. β to γ), then $h + s$ is a homotopy from α to γ. Therefore, the relation "α is homotopic to β" is an equivalence relation on $\mathrm{Hom}_{C(A)}(M, N)$, whose classes are called homotopy of morphisms from M to N.

Proposition 8.1.9. *If α and β are two homotopic morphisms from M to N, then $H(\alpha) = H(\beta)$.*

Proof. Let h be a homotopy from α to β, then

$$(\beta - \alpha)(Z(M)) = (d \circ h + h \circ d)(Z(M)) = (d \circ h)(Z(M)) \subseteq B(M)$$

hence $H(\beta - \alpha) = 0$ and $H(\alpha) = H(\beta)$. □

Corollary 8.1.10. *A morphism homotopic to a quasi-isomorphism is a quasi-isomorphism.*

Proposition 8.1.11. *Let $\alpha : M \to N$, $\beta : M \to N$, $\gamma : L \to M$, $\eta : N \to P$ be morphisms of complexes. If h is a homotopy from α to β, then $\eta \circ h \circ \gamma$ is a homotopy from $\eta \circ \alpha \circ \gamma$ to $\eta \circ \beta \circ \gamma$.*

Proof. This is clear from the definition, by composing (1.3.1) with η and γ. □

Corollary 8.1.12. *Let M, N, P be complexes, α, β two morphisms from M to N, and γ, η two morphisms from N to P. If h (resp. s) is a homotopy from α to β (resp. from γ to η), then $s \circ \alpha + \eta \circ h$ is a homotopy from $\gamma \circ \alpha$ to $\eta \circ \beta$.*

Proof. In fact, $s \circ \alpha$ is a homotopy from $\gamma \circ \alpha$ to $\eta \circ \alpha$, and $\eta \circ h$ is a homotopy from $\eta \circ \alpha$ to $\eta \circ \beta$. □

Let $\alpha : M \to N$ be a morphism of complexes. We say α is a **homotopy equivalence** if there exist a morphism $\beta : N \to M$ such that $\alpha \circ \beta$ and $\beta \circ \alpha$ are homotopic to identity. In this case, we say β is a **homotopy inverse** of α. If β and β' are homotopy inverses of α, then β and β' are homotopic (in fact, $\beta' = \beta' \circ 1_N$ is homotopic to $\beta' \circ \alpha \circ \beta$, which is homotopic to $1_M \circ \beta = \beta$).

Proposition 8.1.13. *A homotopy equivalence is a quasi-isomorphism; a composition of homotopy equivalences is a homotopy equivalence. A morphism homotopic to a homotopy equivalence is a homotopy equivalence.*

Proof. Let $\alpha : M \to N$ and $\gamma : N \to P$ be homotopy equivalence of compleses, with inverses $\beta : N \to M$ and $\eta : P \to N$. Then

$$H(\beta) \circ H(\alpha) = H(\beta \circ \alpha) = H(1_M) = 1_{H(M)}$$

so $H(\alpha)$ is an isomorphism. Now $(\beta \circ \eta) \circ (\gamma \circ \alpha)$ is homotopic to $\beta \circ 1_N \circ \alpha$ (Proposition 8.1.11), hence to 1_M; similarly, $(\gamma \circ \alpha) \circ (\beta \circ \eta)$ is homotopic to 1_P, so $\gamma \circ \alpha$ is a homotopy equivalence. Finally, if $\mu : M \to N$ is homotopic to α, then $\beta \circ \mu$ is homotopic to $\beta \circ \alpha$, hence to identity. This shows β is a homotopy inverse of μ, so μ is a homotopy equivalence. □

Corollary 8.1.14. *Let $\alpha : M \to N$ be a morphism and $\eta : L \to M$, $\gamma : N \to P$ be homotopy equivalences. Then for $\gamma \circ \alpha \circ \eta$ is a homotopy equivalence (resp. a quasi-isomorphism), it is necessary and sufficient that α is a homotopy equivalence (resp. a quasi-isomorphism).*

Proof. If α is a homotopy equivalence (resp. a quasi-isomorphism), then so is $\gamma \circ \alpha \circ \eta$ by Proposition 8.1.13. Conversely, let $\bar{\gamma}$ and $\bar{\eta}$ be the homotopy inverses of γ and η, respectively. Then $\bar{\gamma} \circ \gamma \circ \alpha \circ \eta \circ \bar{\eta}$ is homotopic to α, whence the conclusion. □

We say a complex M is null-homotopic if the identity map 1_M is homotopic to zero, which means there exists a graded A-homomorphism h of degree 1 on M such that $1_M = d \circ h + h \circ d$. This also amounts to saying that the unique morphism $0 \to M$ (resp. $M \to 0$) is a homotopy equivalence. A null-homotopic complex is null-homologous by Proposition 8.1.13.

Example 8.1.15. Let $\phi : M \to N$ and $\psi : N \to P$ be homomorphisms of A-modules such that $\psi \circ \phi = 0$. Let C be the complex

$$0 \longrightarrow M \xrightarrow{\phi} N \xrightarrow{\psi} P \longrightarrow 0$$

Then C is null-homologous if and only if it is exact, and is null-homotopic if and only if it is splitting. In fact, if C is homotopic to zero, there exist A-homomorphisms $h : P \to N$ and $s : N \to M$ such that

$$\psi \circ h = 1_P, \quad h \circ \psi + \phi \circ s = 1_N, \quad s \circ \phi = 1_M.$$

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r, "\phi"] & N \arrow[r, "\psi"] & P \arrow[r] & 0 \\
0 \arrow[r] & M \arrow[r, "\phi"] & N \arrow[r, "\psi"] \arrow[ul, "s"] & P \arrow[r] \arrow[ul, "h"] & 0
\end{tikzcd}$$

Then the homomorphism h gives a splitting for C. Conversely, if C is splitting, then let $h : P \to N$ be a section of P in N. Then we can define s by $\phi \circ s = 1_N - h \circ \psi$, this is possible since ϕ is injective and $\phi \circ (s \circ \phi - 1_M) = (1_N - h \circ \psi) \circ \phi - \phi = 0$.

8.1.4 Splitting complexes

Proposition 8.1.16. *Let (M, d) be a complex. The following conditions are equivalent:*

(i) there exists a homotopy equivalence from (M, d) to $(H(M), 0)$;

(ii) there exists an A-endomorphism s of degree 1 on M such that $d = d \circ s \circ d$;

(iii) $B(M)$ *and* $Z(M)$ *are direct factors of* M*;*

(iv) (M, d) *is a direct sum of sub-complexes which are either of length* 0 *or of length* 1 *and null-homologous.*

The complex M *is called* ***splitting*** *if the above conditions hold, and* s *is called a* ***split*** *for* M*.*

Proof. Let $\varphi : M \to H(M)$ be a homotopy equivalence; there exists then a homomorphism $\psi : H(M) \to M$ and an endomorphism s on C of degree 1 such that $\psi \circ \varphi = 1_M - s \circ d - d \circ s$. We have $d \circ \psi = \psi \circ 0 = 0$, so

$$0 = d \circ \psi \circ \varphi = d - d \circ s \circ d - d \circ d \circ s = d - d \circ s \circ d$$

so s is the endomorphism on M satisfying conditions in (ii).

We also note that if s is an endomorphism as in (ii), then $d \circ (1_M - s \circ d) = 0$ and $1_M - s \circ d$ is the identity on $Z(M)$, so $1_M - s \circ d$ is a projection from M to $Z(M)$. Similarly, $(d \circ s) \circ d = d$, so $d \circ s$ is a projection from M to $B(M)$. This shows $Z(M)$ and $B(M)$ are direct factors of M, so (ii) implies (iii).

We now show the implication (iii)⇒(iv). For $n \in \mathbb{Z}$, put $Z_n = Z_n(M)$, $B_n = B_n(M)$ and choose submodules K_n and L_n such that

$$M_n = L_n \oplus Z_n, \quad Z_n = K_n \oplus B_n.$$

Let $E_{(n)} = K_n[-n]$ and $F_{(n)}$ be the following complex: $(F_{(n)})_n = L_n$, $(F_{(n)})_{n-1} = B_{n-1}$, and the differential is the restriction of d_n on L_n:

$$\cdots \longrightarrow 0 \longrightarrow L_n \xrightarrow{d_n} B_{n-1} \longrightarrow 0 \longrightarrow \cdots$$

Then $E_{(n)}$ and $F_{(n)}$ are sub-complexes of (M, d) and we have $(M, d) = \bigoplus_{n \in \mathbb{Z}} (E_{(n)} \oplus F_{(n)})$. Each $E_{(n)}$ is, either zero, of length 0; and each $F_{(n)}$ is either null or of length 1 and null-homologous, hence (iv).

Finally, to see (iv)⇒(i), it suffices to note that (i) is satisfied for any complex M of length 0, or of length 1 and null-homologous. □

Example 8.1.17 (Example of splitting complexes).

(a) A complex with zero differentials is splitting.

(b) The null-homotopic complexes are the splitting complexes that are null-homologous, i.e., the complexes M such that $H(M) = 0$ and $Z(M)$ is a direct factor of M.

(c) Let $\phi : M \to N$ be a homomorphism of A-modules and C the complex

$$0 \longrightarrow M \xrightarrow{\phi} N \longrightarrow 0$$

Then C is splitting if and only if $\ker \phi$ is a direct factor of M and $\operatorname{im} \phi$ is a direct factor of N.

(d) We have the following exact sequences

$$0 \longrightarrow Z_n(M) \longrightarrow M_n \longrightarrow B_{n-1}(M) \longrightarrow 0$$

$$0 \longrightarrow H_n(M) \longrightarrow M_n/B_n(M) \longrightarrow B_{n-1}(M) \longrightarrow 0$$

So the complex M is splitting if $B(M)$ and $H(M)$ are projective (resp. if $B_n(M)$ and $H_n(M)$ are injective for each n). In particular, if A is principal, a free complex M is splitting if and only if $H(M)$ is free.

Remark 8.1.1. Suppose that the canonical exact sequence of graded A-modules

$$0 \longrightarrow B(M) \longrightarrow Z(M) \xrightarrow{\pi} H(M) \longrightarrow 0$$

is splitting (this is for example if $H(M)$ is projective or $B(M)$ is injective); let $\sigma : H(M) \to Z(M)$ be a graded A-linear section of π, and ψ the homomorphism $x \mapsto \sigma(x)$ from $H(M)$ to M. Then ψ is a quasi-isomorphism from $(H(M), 0)$ to M such that $H(\psi) = 1_{H(M)}$.

Remark 8.1.2. Suppose that the canonical exact sequence of graded A-modules

$$0 \longrightarrow H(M) \xrightarrow{i} M/B(M) \longrightarrow B(M)[-1] \longrightarrow 0$$

is splitting (this is for example if $B(M)$ is projective or $H(M)$ is injective); let $\tau : M/B(M) \to H(M)$ be a graded A-linear section of i, and ϕ the homomorphism from M to $H(M)$ which associates a element of M the image under τ of its class modulo $B(M)$. Then ϕ is a quasi-isomorphism from M to $(H(M), 0)$ such that $H(\phi) = 1_{H(M)}$.

8.1.5 Cone and cylinder of a morphism of complexes

Let $\alpha : (M, d) \to (N, d)$ be a morphism of complexes. We define graded A-modules $\mathrm{Cyl}(\alpha)$ and $\mathrm{Cone}(\alpha)$ by

$$\mathrm{Cyl}(\alpha) = M \oplus M[-1] \oplus N, \quad \mathrm{Cone}(\alpha) = M[-1] \oplus N$$

and define graded A-linear maps of degree -1:

$$\begin{aligned} &D : \mathrm{Cyl}(\alpha) \to \mathrm{Cyl}(\alpha), && D(x_1, x_2, y) = (dx_1 + x_2, -dx_2, dy + \alpha(x_2)), \\ &D : \mathrm{Cone}(\alpha) \to \mathrm{Cone}(\alpha), && D(x, y) = (-dx, dy + \alpha(x)) \end{aligned}$$

It is easy to see that $(\mathrm{Cyl}(\alpha), D)$ and $(\mathrm{Cone}(\alpha), D)$ are complexes. Equivalently, the differentials of $\mathrm{Cyl}(\alpha)$ and $\mathrm{Cone}(\alpha)$ are given by the following diagrams:

$$\begin{tikzcd}
\cdots \arrow[r] & M_{n+1} \arrow[r, "d"] & M_n \arrow[r, "d"] & M_{n-1} \arrow[r] & \cdots \\
 & \oplus & \oplus \arrow[ul, "1_{M_n}"'] & \oplus \arrow[ul, "1_{M_{n-1}}"'] & \\
\cdots \arrow[r] & M_n \arrow[r, "-d"] \arrow[dr, "\alpha_n"] & M_{n-1} \arrow[r, "-d"] \arrow[dr, "\alpha_{n-1}"] & M_{n-2} \arrow[r] & \cdots \\
 & \oplus & \oplus & \oplus & \\
\cdots \arrow[r] & N_{n+1} \arrow[r, "d"] & N_n \arrow[r, "d"] & N_{n-1} \arrow[r] & \cdots
\end{tikzcd}$$

$$\begin{tikzcd}
\cdots \arrow[r] & M_n \arrow[r, "-d"] \arrow[dr, "\alpha_n"] & M_{n-1} \arrow[r, "-d"] \arrow[dr, "\alpha_{n-1}"] & M_{n-2} \arrow[r] & \cdots \\
 & \oplus & \oplus & \oplus & \\
\cdots \arrow[r] & N_{n+1} \arrow[r, "d"] & N_n \arrow[r, "d"] & N_{n-1} \arrow[r] & \cdots
\end{tikzcd}$$

In particular, it is easy to see that M and N can be viewed as sub-complexes of $\mathrm{Cyl}(\alpha)$ and $\mathrm{Cone}(\alpha)$, and we have the following split exact sequences

$$0 \longrightarrow M \xrightarrow{\iota_M} \mathrm{Cyl}(\alpha) \xrightarrow{\tilde{\pi}} \mathrm{Cone}(\alpha) \longrightarrow 0 \tag{1.5.1}$$

$$0 \longrightarrow N \xrightarrow{\tilde{\iota}_N} \mathrm{Cone}(\alpha) \xrightarrow{\tilde{\pi}_M} M[-1] \longrightarrow 0 \tag{1.5.2}$$

Example 8.1.18. Let $\phi : M \to N$ be a homomorphism of A-modules; then $\mathrm{Cone}(\phi)$ is of the form

$$0 \longrightarrow M \xrightarrow{\phi} N \longrightarrow 0$$

In particular, we see $H_1(\mathrm{Cone}(\phi)) = \ker \phi$ and $H_0(\mathrm{Cone}(\phi)) = \operatorname{coker} \phi$.

We define two maps ι_N and π_N between N and $\mathrm{Cyl}(\alpha)$:

$$\begin{aligned}
\iota_N &: N \to \mathrm{Cyl}(\alpha), \quad y \mapsto (0, 0, y) \\
\pi_N &: \mathrm{Cyl}(\alpha) \to N, \quad (x_1, x_2, y) \mapsto \alpha(x_1) + y.
\end{aligned}$$

Proposition 8.1.19. *The morphisms $\iota_N : N \to \mathrm{Cyl}(\alpha)$ and $\pi_N : \mathrm{Cyl}(\alpha) \to N$ are homotopy inverses of each other.*

Proof. It is clear that $\pi_N \circ \iota_N = 1_N$; on the other hand, if $\sigma : \mathrm{Cyl}(\alpha) \to \mathrm{Cyl}(\alpha)$ is the A-linear map of degree 1 such that $\sigma(x_1, x_2, y) = (0, x_1, 0)$, then

$$D \circ \sigma + \sigma \circ D + \iota_N \circ \pi_N = 1_{\mathrm{Cyl}(\alpha)}$$

so σ is a homotopy equivalence and the claim follows. □

We can summarize Proposition 8.1.19 by the following commutative diagram where rows are exact and columns are homotopy equivalent:

$$\begin{tikzcd}
 & 0 \arrow[r] & N \arrow[r, "\tilde{\iota}_N"] \arrow[d, "\iota_N"] & \mathrm{Cone}(\alpha) \arrow[r, "\tilde{\pi}_M"] \arrow[d, "1"] & M[-1] \arrow[r] & 0 \\
0 \arrow[r] & M \arrow[r, "\iota_M"] \arrow[d, "1"] & \mathrm{Cyl}(\alpha) \arrow[r, "\tilde{\pi}"] \arrow[d, "\pi_N"] & \mathrm{Cone}(\alpha) \arrow[r] & 0 & \\
 & M \arrow[r, "\alpha"] & N & & &
\end{tikzcd}$$

Corollary 8.1.20. *For any morphism $\alpha : M \to N$ of complexes, there exists an injective morphism $\tilde{\alpha} : M \to \tilde{N}$ and a homotopy equivalence $\beta : \tilde{N} \to N$ such that $\alpha = \beta \circ \tilde{\alpha}$.*

Proof. This follows by taking $\tilde{N} = \mathrm{Cone}(\alpha)$, and using Proposition 8.1.19. □

Lemma 8.1.21. *Let $\alpha : M \to N$ be a morphism.*

(a) The connecting homomorphism $\partial_{n+1}(\tilde{\iota}_N, \tilde{\pi}_M) : H_n(M) \to H_n(N)$ is given by $H_n(\alpha)$.

(b) *The connecting homomorphism* $\partial_{n+1}(\iota_M, \tilde{\pi}) : H_n(\mathrm{Cone}(\alpha)) \to H_{n-1}(M)$ *is given by* $H_n(\tilde{\pi}_M)$.

Proof. Let $x \in Z_n(M)$; since $x = \tilde{\pi}_M(x, 0)$ and

$$D(x, 0) = (-dx, \alpha(x)) = (0, \alpha(x)) = \tilde{\iota}_N(\alpha(x))$$

we see $(\tilde{\iota}_N, \tilde{\pi}_M)$ sends x to the class of $\alpha(x)$ in $H_n(N)$. This proves (a).

Let $(x, y) \in \mathrm{Cone}_n(\alpha)$ such that $D(x, y) = 0$; we then have $(-dx, \alpha(x) + dy) = 0$. Since $(x, y) = \tilde{\pi}(0, x, y)$ and

$$D(0, x, y) = (x, -dx, dy + \alpha(x)) = (x, 0, 0) = \iota_M(x)$$

we see $\partial(\iota_M, \tilde{\pi})$ sends (x, y) to the class of x in $H_{n-1}(M)$, whence (b). □

Proposition 8.1.22. *We have a long exact sequence*

$$\cdots \longrightarrow H_n(M) \xrightarrow{H_n(\alpha)} H_n(N) \xrightarrow{H_n(\tilde{\iota}_N)} H_n(\mathrm{Cone}(\alpha)) \xrightarrow{H_n(\tilde{\pi}_M)} H_{n-1}(M) \longrightarrow \cdots \tag{1.5.3}$$

Proof. This follows from the long exact sequence induced from (1.5.2) and noting that the connecting homomorphism $H_n(M) \to H_n(N)$ is given by $H_n(\alpha)$. □

Corollary 8.1.23. *For α to be a quasi-isomorphism, it is necessary and sufficient that* $\mathrm{Cone}(\alpha)$ *is null-homologous.*

Remark 8.1.3. Consider the following diagram with two exact rows induced from (1.5.1) and (1.5.2):

$$\begin{tikzcd}
\cdots \arrow[r] & H_n(M) \arrow[r, "H_n(\iota_M)"] \arrow[d, "1"] & H_n(\mathrm{Cyl}(\alpha)) \arrow[r, "H_n(\tilde{\pi})"] \arrow[d, "H_n(\pi_N)"] & H_n(\mathrm{Cone}(\alpha)) \arrow[r, "\partial_n(\iota_M, \tilde{\pi})"] \arrow[d, "1"] & H_{n-1}(M) \arrow[r] \arrow[d, "1"] & \cdots \\
\cdots \arrow[r] & H_n(M) \arrow[r, "H_n(\alpha)"] & H_n(N) \arrow[r, "H_n(\tilde{\iota}_N)"] & H_n(\mathrm{Cone}(\alpha)) \arrow[r, "H(\tilde{\pi}_M)"] & H_{n-1}(M) \arrow[r] & \cdots
\end{tikzcd} \tag{1.5.4}$$

This diagram is commutative since

(a) $\alpha = \pi_N \circ \iota_M$ so $H_n(\alpha) = H_n(\pi_N) \circ H_n(\iota_M)$.

(b) $H_n(\pi_N) = H_n(\iota_N)^{-1}$ and $\tilde{\iota}_N = \tilde{\pi} \circ \iota_N$, so $H_n(\tilde{\pi}) = H_n(\tilde{\iota}_N) \circ H_n(\pi_N)$.

(c) $H_n(\tilde{\pi}_M) = \partial_n(\iota_M, \tilde{\pi})$.

Now consider a short exact sequence of complexes:

$$0 \longrightarrow M \xrightarrow{\alpha} N \xrightarrow{\beta} L \longrightarrow 0 \tag{1.5.5}$$

Define a graded A-linear map $\varphi : \mathrm{Cone}(\alpha) \to L$ of degree 0 by $\varphi(x, y) = \beta(y)$. We then have a commutative diagram of A-complexes with exact rows:

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r, "\iota_M"] \arrow[d, "1"] & \mathrm{Cyl}(\alpha) \arrow[r, "\tilde{\pi}"] \arrow[d, "\pi_N"] & \mathrm{Cone}(\alpha) \arrow[r] \arrow[d, "\varphi"] & 0 \\
0 \arrow[r] & M \arrow[r, "\alpha"] & N \arrow[r, "\beta"] & L \arrow[r] & 0
\end{tikzcd} \tag{1.5.6}$$

Proposition 8.1.24. *The map φ is a quasi-isomorphism.*

Proof. From the definition of $\mathrm{Cone}(\alpha)$, we have

$$\varphi \circ D(x, y) = \varphi(-dx, dy + \alpha(x)) = \beta(dy) + \beta(\alpha(x)) = \beta(d(y)) = d(\beta(y)) = d(\varphi(x, y)),$$

so φ is a morphism of complexes. Moreover, φ is surjective with kernel identified with the complex (K, d_K) such that $K = M[-1] \oplus \alpha(M)$ and d_K is the restriction of the differential of $\mathrm{Cone}(\alpha)$. If $d_K(x, \alpha(x')) = 0$, then we have $-dx = 0$ and $\alpha(x) + d\alpha(x') = 0$. Since α is injective, this implies $x + dx' = 0$, so

$$(x, \alpha(x')) = (-dx', \alpha(x')) = d_K(x', 0).$$

This shows $H(K) = 0$, whence φ is a quasi-isomorphism. □

Corollary 8.1.25. *The following diagram*

$$\begin{tikzcd}
 & H(\mathrm{Cone}(\alpha)) \arrow[dd, "H(\varphi)"] \arrow[dr, "H(\tilde{\pi}_M)"] & \\
H(N) \arrow[ur, "H(\tilde{\iota}_N)"] \arrow[dr, "H(\beta)"'] & & H(M)[-1] \\
 & H(L) \arrow[ur, "\partial(\alpha,\beta)"'] &
\end{tikzcd}$$

is commutative and $H(\varphi)$ is bijective.

Proof. From the commutative diagram (1.5.6), we have $H(1_M) \circ \partial(\tilde{\alpha}, \tilde{\pi}) = \partial(\alpha, \beta) \circ H(\varphi)$ and $\partial(\iota_M, \tilde{\pi}) = H(\tilde{\pi}_M)$ by Lemma 8.1.21, so

$$\partial(\alpha, \beta) \circ H(\varphi) = H(\tilde{\pi}_M).$$

Moreover, from the diagram (1.5.6) and (1.5.4), $H(\beta) \circ H(\pi_N) = H(\varphi) \circ H(\tilde{\pi}) = H(\varphi) \circ H(\tilde{\iota}_N) \circ H(\pi_N)$. Since $H(\pi_N)$ is bijective, we then have $H(\beta) = H(\varphi) \circ H(\pi_N)$. □

We then have $\partial(\alpha, \beta) = H(\varphi)^{-1} \circ H(\tilde{\pi}_M)$, which provides a new definition of the connecting homomorphism $\partial(\alpha, \beta)$. Note also that if we identify $H(\mathrm{Cone}(\alpha))$ to $H(L)$ by $H(\varphi)$, the previous corollary means that the exact sequence (1.5.3) is then identified with the exact sequence of homology relative to (1.5.5).

8.1.6 Euler-Poincaré characteristic

In this part, we consider a set $\mathscr{C}$ of classes of A-modules which is additive and left exact, i.e. which satisfies the following two conditions:

(A) If M and N are two A-modules of type $\mathscr{C}$, $M \oplus N$ is of type $\mathscr{C}$.

(E) If $0 \to L \to M \to N \to 0$ is an exact sequence of A-modules and if M and N are of type $\mathscr{C}$, then L is of type $\mathscr{C}$.

We say $\mathscr{C}$ is stable if $\mathscr{C}$ satisfies the following two conditions:

(S1) If $0 \to L \to M \to N \to 0$ is an exact sequence of A-modules and L and M are of type $\mathscr{C}$, then M is of type $\mathscr{C}$.

(S2) For any homomorphism f of A-modules of type $\mathscr{C}$, $\ker f$ and $\operatorname{coker} f$ are of type $\mathscr{C}$.

We denote by $K(\mathscr{C})$ the Grothendieck group of $\mathscr{C}$ and $[M]$ the element in $K(\mathscr{C})$ defined by an A-module M. Let G be an abelian group and $\varphi : K(\mathscr{C}) \to G$ be a homomorphism.

Example 8.1.26.

(a) If A is a field, we can let $\mathscr{C}$ to be the classes of finite dimensional vector spaces and $\varphi : K(\mathscr{C}) \to \mathbb{Z}$ be the map that associates M with its dimension $\dim(M)$.

(b) We can let $\mathscr{C}$ be the classes of A-modules of finite length and set $\varphi([M]) = \ell_A(M)$.

We say a graded A-module M is of type $\mathscr{C}$ if each M_n is of type $\mathscr{C}$. Let M be a graded A-module bounded and of type $\mathscr{C}$, with (M_n) the graduation. The **φ-characteristic** of M, denoted by $\chi_\varphi(M)$ or simple $\chi(M)$, is the element $\sum_n (-1)^n \varphi([M_n])$ of G. This definition applies in particular if M is a bounded complex of A-modules.

Example 8.1.27.

(a) If M is bounded of type $\mathscr{C}$, so is $M[r]$ for any $r \in \mathbb{Z}$, and we have $\chi(M[r]) = (-1)^r \chi(M)$.

(b) Let $0 \to L \to M \to N \to 0$ be an exact sequence of graded A-modules of type $\mathscr{C}$. If L, M, N are bounded, then we have

$$\chi(M) = \chi(L) + \chi(N).$$

(c) Let $\alpha : M \to N$ be a morphism of bounded complexes of type $\mathscr{C}$. Then $\operatorname{Cone}(\alpha)$ is bounded of type $\mathscr{C}$, and we have

$$\chi(\operatorname{Cone}(\alpha)) = \chi(N) - \chi(M).$$

(d) Let M be a graded A-module bounded and of type $\mathscr{C}$. The Poincaré polynomial of M relative to φ is the element $P_M(t) = \sum \varphi([M_n])t^n \in G \otimes \mathbb{Z}[t, t^{-1}]$. We have $P_M(1) = \varphi([M])$ and $P_M(-1) = \chi(M)$.

Lemma 8.1.28. *Let M be a bounded complex of type $\mathscr{C}$. If $H(M) = 0$ then $\chi(M) = 0$,*

Proof. This follows from **??**. □

Proposition 8.1.29. *Let M, N be bounded complexes of type $\mathscr{C}$. If M and N are quasi-isomorphic, then $\chi(M) = \chi(N)$.*

Proof. In fact, $\alpha : M \to N$ is a quasi-isomorphism if and only if the mapping cone $\operatorname{Cone}(\alpha)$ is null-homologous. Then since $\chi(\operatorname{Cone}(\alpha)) = \chi(N) - \chi(M)$, we conclude the claim. □

Proposition 8.1.30. *Let M be a bounded complex of type $\mathscr{C}$.*

(a) If $\mathscr{C}$ is stable, $H(M)$ is of type $\mathscr{C}$.

(b) If $H(M)$ is of type $\mathscr{C}$, so are $B(M)$ and $Z(M)$, and we have $\chi(H(M)) = \chi(M)$.

Proof. If $\mathscr{C}$ is stable, for each n the module $Z_n(M)$ is of type $\mathscr{C}$ as the kernel of $d_n : M_n \to M_{n-1}$, and $H_n(M)$ is of type $\mathscr{C}$ as the cokernel of $M_{n+1} \to Z_n$.

Suppose that $H(M)$ is of type $\mathscr{C}$. The canonical exact sequences

$$0 \longrightarrow Z_n(M) \longrightarrow M_n \longrightarrow B_{n-1}(M) \longrightarrow 0$$
$$0 \longrightarrow B_n(M) \longrightarrow Z_n(M) \longrightarrow H_n(M) \longrightarrow 0$$

shows by induction on n that $Z_n(M)$ and $B_n(M)$ are of type $\mathscr{C}$ for each n. We then have

$$\chi(M) = \chi(Z(M)) + \chi(B(M))[-1] = \chi(Z(M)) - \chi(B(M)) = \chi(H(M)).$$

This completes the proof. □

Corollary 8.1.31. *If $\mathscr{C}$ is stable and M is bounded of type $\mathscr{C}$, the graded module $H(M)$ is bounded of type $\mathscr{C}$ and $\chi(H(M)) = \chi(M)$.*

Proposition 8.1.32. *Let $0 \to L \to M \to N \to 0$ be an exact sequence of complexes.*

(a) If $H(L)$, $H(M)$, $H(N)$ are bounded of type $\mathscr{C}$, we have

$$\chi(H(M)) = \chi(H(L)) + \chi(H(N)).$$

(b) If $\mathscr{C}$ is stable. and two of the graded modules of $H(L)$, $H(M)$, $H(N)$ are bounded of type $\mathscr{C}$, then so is the third one.

Proof. Part (a) follows from Lemma 8.1.28 applied to the long exact sequence induced. Part (b) follows similarly. □

Corollary 8.1.33. *Suppose that $\mathscr{C}$ is stable, and let $\alpha : M \to N$ be a morphism of complexes such that $H(M)$ and $H(N)$ are bounded of type $\mathscr{C}$. Then $H(\mathrm{Cone}(\alpha))$ is bounded of type $\mathscr{C}$, and we have*

$$\chi(H(\mathrm{Cone}(\alpha))) = \chi(H(N)) - \chi(H(M)).$$

Proof. This follows from Proposition 8.1.32 applied to the exact sequence

$$0 \longrightarrow N \longrightarrow \mathrm{Cone}(\alpha) \longrightarrow M[-1] \longrightarrow 0$$ □

8.1.7 The de Rham complex

In this part we let A be a commutative k-algebra over some commutative ring k. Let $d^0 : A \to \Omega^1_{A/k}$ be the canonical k-derivation of A into the A-module $\Omega^1_{A/k}$ of k-differentials of A. Let $\Omega_{A/k}$ be the graded k-algebra $\bigwedge_A(\Omega^1_{A/k})$.

Proposition 8.1.34. *There exists a unique k-antiderivation $d : \Omega_{A/k} \to \Omega_{A/k}$ of degree 1 such that $d \circ d = 0$ which extends $d^0 : A \to \Omega^1_{A/k}$.*

Proof. We first show the uniqueness of d. Since $d \circ d = 0$, for $y, x_1, \dots, x_p \in A$, we have

$$d(y dx_1 \wedge \cdots \wedge dx_p) = dy \wedge dx_1 \wedge \cdots \wedge dx_p.$$

The A-module $\Omega^p_{A/k}$ is generated by the elements $dx_1 \wedge \cdots \wedge dx_p$, which proves the uniqueness.

For the existence, it suffices to construct a k-homomorphism $d^1 : \Omega^1_{A/k} \to \Omega^2_{A/k}$ such that $d^1 \circ d^0 = 0$ and

$$d^1(x\omega) = d^0(x) \wedge \omega + x d^1(\omega) \quad \text{for} \quad x \in A, \omega \in \Omega^1_{A/k}. \tag{1.7.1}$$

In fat, it then follows from **??** and **??** that there exists an antiderivation $d : \Omega_{A/k} \to \Omega_{A/k}$ which coincides with d^0 at degree 0 and with d^1 at degree 1. As d^0 is zero on k, the antiderivation d is k-linear; as $d^1 \circ d^0 = 0$, we have $d \circ d = 0$ since $\Omega_{A/k}$ is generated as A-algebra by the elements $d^0(a)$ for $a \in A$.

To define d^1, recall that $\Omega^1_{A/k}$ is equal to the A-module $\mathfrak{I}/\mathfrak{I}^2$, where $\mathfrak{I}$ is the kernel of the multiplication map $m : A \otimes_k A \to A$. Consider the k-linear map $u : A \otimes_k A \to \Omega^2_{A/k}$ defined by $u(x \otimes y) = d^0(y) \wedge d^0(x)$. We have

$$u(ax \otimes y - x \otimes ay) = d^0(y) \wedge d^0(ax) - d^0(ay) \wedge d^0(x) = d^0(xy) \wedge d^0(a)$$

for x, y, a in A, whence

$$u((a \otimes 1 - 1 \otimes a)\xi) = d^0(m(\xi)) \wedge d^0(a), \quad \xi \in A \otimes_k A, a \in A. \tag{1.7.2}$$

Since $\mathfrak{I}$ is generated as an A-module by the elements $(a \otimes 1 - 1 \otimes a)$ for $a \in A$, we then deduce that $u(\mathfrak{I}^2) = 0$; thus u defines a k-linear map $d^1 : \mathfrak{I}/\mathfrak{I}^2 \to \Omega^2_{A/k}$.

Let $\xi = b \otimes 1$ in (1.7.2), where $b \in A$, we obtain $d^1(bd^0(a)) = d^0(b) \wedge d^0(a)$; it then follows that $d^1 \circ d^0 = 0$ and $d^1(a\omega) = d^0(a) \wedge \omega + a d^1(\omega)$ for $a \in A$ and $\omega = bd^0(a)$. Since $\Omega^1_{A/k}$ is generated as an A-module by the elements $bd^0(a)$, formula (1.7.1) is then satisfied for $\omega \in \Omega_{A/k}$, which completes the proof. □

We say the elements $\Omega^p_{A/k}$ are **exterior differential forms** of degree p of A over k, and the antiderivation d is the **exterior differential** of $\Omega_{A/k}$. The complex $(\Omega_{A/k}, d)$ is called the de Rham complex of A over k, and its cohomology is called the de Rham cohomology of A over k.

Example 8.1.35. Let A be the polynomial ring $k[X_1, \dots, X_n]$. Then $\Omega^1_{A/k}$ is the free A-module with basis $dX_1, \dots, dX_n$. Consequently, if for a subset $I = \{i_1, \dots, i_p\}$ of $\{1, \dots, n\}$ we set $dX_I = dX_{i_1} \wedge \cdots \wedge dX_{i_p}$ (here $i_1 < \cdots < i_p$), the A-module $\Omega^p_{A/k}$ has a basis dX_i, where I runs through the set of subsets of $\{1, \dots, n\}$ with cardinal p. We have

$$d(PdX_I) = dP \wedge dX_I = \sum_{i \notin I} (-1)^{n(I,i)} \tfrac{\partial P}{\partial X_i} dX_{I \cup \{i\}},$$

where $n(I, i)$ denotes the number of elements in I that are strictly small than i.

The cycles of $Z^p(\Omega_{A/k})$ are then elements $\omega = \sum_{|I|=p} P_I dX_I$ such that, for any subset J of

$\{1, \dots, n\}$ with $p+1$ elements, we have

$$\sum_{i \in J} (-1)^{n(J,i)} \frac{\partial P_{J \setminus \{i\}}}{\partial X_i} = 0.$$

The element ω is a boundary if we can choose, for each subset J with $(p-1)$ elements and a polynomial $Q_J \in A$ such that

$$P_I = \sum_{j \in I} (-1)^{n(I,j)} \frac{\partial Q_{I \setminus \{j\}}}{\partial X_j}.$$

We shall see that the de Rham complex of A over k is acyclic at positive degrees if k is a $\mathbb{Q}$-algebra.

Now let M be an A-module. We say a k-linear map $\nabla^0 : M \to M \otimes_A \Omega^1_{A/k}$ is a **connection** on M if it satisfies

$$\nabla^0(am) = a\nabla^0(m) + m \otimes da \quad \text{for} \quad a \in A, m \in M. \tag{1.7.3}$$

Proposition 8.1.36. *Let ∇^0 be a connection on M.*

(a) There exists a unique k-linear map ∇ of degree 1 on the $\Omega_{A/k}$-module $M \otimes_A \Omega_{A/k}$ which extends ∇^0 and satisfies the identity

$$\nabla(x\omega) = \nabla(x)\omega + (-1)^p x(d\omega) \quad \textit{for} \quad x \in M \otimes_A \Omega^p_{A/k}, \omega \in \Omega_{A/k}. \tag{1.7.4}$$

(b) The composition ∇^2 is $\Omega_{A/k}$-linear; in particular the map $R = \nabla^1 \circ \nabla^0$ is A-linear, and we have

$$\nabla^2(m \otimes \omega) = R(m)\omega \quad \textit{for} \quad m \in M, \omega \in \Omega_{A/k}$$

Proof. The uniqueness of ∇ is clear. We now define a k-homomorphism $\overline{\nabla} : M \otimes_k \Omega_{A/k} \to M \otimes_A \Omega_{A/k}$ by

$$\overline{\nabla}(m \otimes \omega) = \nabla^0(m)\omega + m \otimes d\omega \quad \text{for} \quad m \in M, \omega \in \Omega_{A/k}.$$

It then follows from (1.7.3) that $\overline{\nabla}(am \otimes \omega) = \overline{\nabla}(m \otimes a\omega)$, so we get a k-homomorphism ∇ on $M \otimes_A \Omega_{A/k}$ which extends ∇^0 at degree 0. We now verify (1.7.4): for $m \in M$, $\alpha \in \Omega^p_{A/k}$, $\omega \in \Omega_{A/k}$,

$$\begin{aligned}
\nabla((m \otimes \alpha)\omega) &= \nabla(m \otimes (\alpha \wedge \omega)) = \nabla^0(m)(\alpha \wedge \omega) + m \otimes d(\alpha \wedge \omega) \\
&= \nabla^0(m)\alpha\omega + (m \otimes d\alpha)\omega + (-1)^p (m \otimes \alpha) d\omega \\
&= (\nabla(m \otimes \alpha))\omega + (-1)^p (m \otimes \alpha) d\omega;
\end{aligned}$$

this proves (1.7.4) for $x = m \otimes \alpha$, and the general case follows by linearity.

Let $x \in M \otimes_A \Omega^p_{A/k}$ and $\omega \in \Omega_{A/k}$; by apply (1.7.4), we obtain

$$\begin{aligned}
\nabla^2(x\omega) &= \nabla(\nabla(x)\omega) + (-1)^p \nabla(x d\omega) \\
&= (\nabla \circ \nabla(x))\omega + (-1)^{p+1} \nabla(x)(d\omega) + (-1)^p \nabla(x)(d\omega) = (\nabla \circ \nabla(x))\omega.
\end{aligned}$$

this shows the first assertion in (b), and the second one is immediate. □

The map $R : M \to M \otimes_A \Omega^2_{A/k}$ is called the **curvature homomorphism** of ∇, and ∇ is called **integrable** if $R = 0$, or equivalently $\nabla \circ \nabla = 0$. In this case, the couple $(M \otimes_A \Omega_{A/k}, \nabla)$ is a complex, called the **de Rham complex** of (M, ∇^0) over k.

8.2 Resolutions

8.2.1 Resolutions of modules

In this part, we identify a module M with the complex $M[0]$. A **left resolution** of M if a pair (P, p) where P is a positive complex and $p : P \to M$ is a quasi-isomorphism. Similarly, a **right resolution** is a pair (e, E) where E is a negative complex and $e : M \to E$ is a quasi-isomorphism. The **length** of a resolution is defined to be the length of the complex. If (P, p) and (P', p') (resp. (e, E) and (e', E')) are rwo left (resp. right) resolutions of M, a morphism $f : P \to P'$ such that $p' \circ f = p$ (resp. $g : E \to E'$ such that $g \circ e = e'$) is called a morphism of resolutions.

A **projective** resolution (resp. **free**, **flat**) of an A-module is defined to be a left resolution (P, p) of M such that the complex P is projective (resp. free, flat). An **injective** resolution of M is a right resolution (e, E) of M such that E is injective.

Example 8.2.1.

(a) Suppose that A is a PID; let M be an A-module and $(x_i)_{i \in I}$ a family of generators of M. Let L_0 be the free module $A^{\oplus I}$ and $p : L_0 \to M$ be the canonical homomorphism such that $p(e_i) = x_i$. The homomorphism p is surjective and its kernel L_1 is a free module, so we have a free resolution for M of length 1:

$$0 \longrightarrow L_1 \longrightarrow L_0 \xrightarrow{p} M \longrightarrow 0$$

If I is finite, L_0 and L_1 are finitely generated.

(b) Suppose that A is commutative; let E be an A-module and u an endomorphism of E. Let E_u be the $A[X]$-module obtained by actting X by u on E. Then we have an exact sequence

$$0 \longrightarrow A[X] \otimes_A E \xrightarrow{\psi} A[X] \otimes_A E \xrightarrow{\varphi} E_u \longrightarrow 0$$

where $\varphi(p \otimes x) = px$ and $\psi(p \otimes x) = Xp \otimes x - p \otimes u(x)$ for $p \in A[X]$ and $x \in E$. This is then a projective resolution (resp. free, finitely generated) for E of length 1 if E is a projective (resp. free, finitely generated) A-module.

Proposition 8.2.2. *Let $f : M \to N$ be a homomorphism of A-modules. Let (P_M, p_M) and (P_N, p_N) be projective resolutions of M and N, respectively. Then there exists a morphism $\tilde{f} : P_M \to P_N$ which is unique up to homotopy equivalence, such that $p_N \circ \tilde{f} = f \circ P_M$.*

Proposition 8.2.3. *Let $f : M \to N$ be a homomorphism of A-modules. Let (e_M, E_M) and (e_N, E_N) be injective resolutions of M and N, respectively. Then there exists a morphism $\tilde{f} : E_M \to E_N$ which is unique up to homotopy equivalence, such that $\tilde{f} \circ p_M = P_M \circ p$.*

8.2.2 The canonical free resolution

For any A-module M, denote by $L_0(M)$ the free A-module $A^{\oplus M}$ with basis M, $(e_m)_{m\in M}$ the canonical basis and $p_M : L_0(M) \to M$ the homomorphism such that $p_M(e_m) = m$ for $m \in M$. Put $Z_0(M) = \ker p_M$ and let $i_M : Z_0(M) \to L_0(M)$ be the canonical injection. We then have an exact sequence

$$0 \longrightarrow Z_0(M) \xrightarrow{i_M} L_0(M) \xrightarrow{p_M} M \longrightarrow 0$$

We define a graded module $L(M)$ by $L_n(M) = 0$ for $n < 0$ and by induction on $n > 0$, that

$$L_n(M) = L_0(Z_{n-1}(M)), \quad Z_n(M) = Z_0(Z_{n-1}(M)).$$

Also, there is a homomorphism $d_n : L_n(M) \to L_{n-1}(M)$ defined by

$$\begin{cases} d_n = 0 & n \leq 0, \\ d_1 = i_M \circ p_{Z_0(M)} & \\ d_m = i_{Z_{n-2}(M)} \circ p_{Z_{n-1}(M)} & n > 1 \end{cases}$$

We then have an exact sequence

$$\cdots \longrightarrow L_n(M) \xrightarrow{d_n} L_{n-1}(M) \longrightarrow \cdots \longrightarrow L_0(M) \xrightarrow{p_M} M \longrightarrow 0$$

which gives a morphism $p_M : (L(M), d) \to M$. Therfore, $(L(M), p_M)$ is a free resolution of M, called the **canonical free resolution** of M.

Let $f : M \to N$ be a homomorphism of A-modules. Then there is a unique homomorphism $L_0(f) : L_0(M) \to L_0(N)$ such that $L_0(f)(e_m) = e_{f(m)}$ for $m \in M$. We have

$$p_N \circ L_0(f) = f \circ p_M$$

so $L_0(f)$ induces an A-homomorphism $Z_0(f) : Z_0(M) \to Z_0(N)$, and

$$i_N \circ Z_0(f) = L_0(f) \circ i_M.$$

Put $L_n(f) = 0$ for $n < 0$ and we define by induction on $n > 0$ homomorphisms $L_n(f) : L_n(M) \to L_n(N)$ and $Z_n(f) : Z_n(M) \to Z_n(N)$ by

$$\begin{cases} L_n(f) = L_0(Z_{n-1}(f)) \\ Z_n(f) = Z_0(Z_{n-1}(f)). \end{cases}$$

Proposition 8.2.4. *The morphism $L(f) : L(M) \to L(N)$ is a morphism of complexes, and we have $p_M \circ L(f) = f \circ p_N$.*

Proof. We must show that, for $n > 0$, the formula

$$d_n^N \circ L_n(f) = L_{n-1}(f) \circ d_n^M.$$

Now we have

$$\begin{aligned} d_1^N \circ L_1(f) &= i_N \circ p_{Z_0(N)} \circ L_0(Z_0(f)) = i_N \circ Z_0(f) \circ p_{Z_0(M)} \\ &= L_0(f) \circ i_M \circ p_{Z_0(M)} = L_0(f) \circ d_1^M, \end{aligned}$$

and for $n > 1$,

$$\begin{aligned} d_n^N \circ L_n(f) &= i_{Z_{n-2}(N)} \circ p_{Z_{n-1}(N)} \circ L_0(Z_{n-1}(f)) = i_{Z_{n-2}(N)} \circ Z_{n-2}(f) \circ p_{Z_{n-1}(M)} \\ &= i_{Z_{n-2}(N)} \circ Z_0(Z_{n-2}(f)) \circ p_{Z_{n-1}(M)} = L_0(Z_{n-2}(f)) \circ i_{Z_{n-2}(M)} \circ p_{Z_{n-1}(M)} \\ &= L_{n-1}(f) \circ d_n^M. \end{aligned}$$

This proves the claim. □

Let $g : N \to P$ be another homomorphism. Then from the definition of L, it is clear that

$$L(g \circ f) = L(g) \circ L(f).$$

Therefore, the operation L defines a functor from the category of A-modules to the category of complexes of free modules.

8.2.3 The canonical injective resolution

Let F the the A-module $\mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})$. For any A-module M, we set $I^0(M) = F^{\mathrm{Hom}_A(M,F)}$ and $e_M : M \to I^0(M)$ the homomorphism that associates a element $m \in M$ the family $(\varphi(m))_{\varphi \in \mathrm{Hom}_A(M,F)}$. By Corollary 7.4.10, the A-module $I^0(M)$ is injective and e_M is injective. Let $K^0(M) = \operatorname{coker} e_M$ and $q_M : I^0(M) \to K^0(M)$ the canonical projection. We then have an exact sequence

$$0 \longrightarrow M \xrightarrow{e_M} I^0(M) \xrightarrow{q_M} K^0(M) \longrightarrow 0$$

We define a graded A-module $I(M)$ by setting $I^n(M) = 0$ for $n < 0$ and define by induction on $n > 0$ that

$$I^n(M) = I^0(K^{n-1}(M)), \quad K^n = K^0(K^{n+1}(M)).$$

Also, there is an A-homomorphism $\delta^n : I^n(M) \to I^{n+1}(M)$ defined by

$$\begin{cases} \delta^n = 0 & n < 0 \\ \delta^0 = e_{K^0(M)} \circ q_M & \\ \delta^n = e_{K^n(M)} \circ q_{K^{n-1}(M)} & n > 0. \end{cases}$$

We then get an exact sequence

$$0 \longrightarrow M \xrightarrow{e_M} I^0(M) \xrightarrow{\delta^0} \cdots \longrightarrow I^n(M) \xrightarrow{\delta^n} I^{n+1}(M) \longrightarrow \cdots$$

so that, if $e_M : M \to (I(M), \delta)$ is the morphism of complexes, we obtain an injective resolution for M, called the **canonical injective resolution** of M.

Let $f : M \to N$ be a homomorphism of A-modules. Let $I^0(f)$ be the homomorphism from $I^0(M) = F^{\mathrm{Hom}_A(M,F)}$ to $I^0(N) = F^{\mathrm{Hom}_A(N,F)}$ sending $(x_\varphi)_{\varphi \in \mathrm{Hom}_A(M,F)}$ to $(x_{\psi \circ f})_{\psi \in \mathrm{Hom}_A(N,F)}$. We

then have

$$I^0(f) \circ e_M = e_N \circ f.$$

Therefore, $I^0(f)$ induces a homomorphism $K^0(f) : K^0(M) \to K^0(N)$ and we have

$$K^0(f) \circ q_M = q_N \circ K^0(f).$$

Again, if we define $I^n(f) = 0$ for $n < 0$ and for $n > 0$,

$$\begin{cases} I^n(f) = I^0(K^{n-1}(f)) \\ K^n(f) = K^0(K^{n-1}(f)) \end{cases}$$

Then we can show as in Proposition 8.2.4 that $I(f) : I(M) \to I(N)$ is a morphism of complexes and $I(f) \circ e_M = e_N \circ f$. If $g : N \to P$ is another homomorphism, then

$$I(g \circ f) = I(g) \circ I(f)$$

so I defines a functor from the category of A-modules to that of complexes of injective A-modules.

8.2.4 Finitely generated resolutions

We have seen that any A-module possesses free resolutions and injective resolutions. Now suppose that A is left Noetherian and let M be a finitely generated A-module. We construct by induction sequences $(L_n)_{n\geq 0}$, $(Z_n)_{n\geq 0}$, $(d_n)_{n\geq 0}$ such that for $n \geq 0$, L_n is a finitely generated free A-module, Z_n is a submodule of L_n and $d_{n+1} : L_{n+1} \to L_n$ a homomorphism.

For this, we first choose a finite family of generators $(m_i)_{i\in I_0}$ of M, put $L_0 = A^{\oplus I_0}$, define $p : L_0 \to M$ by $p(e_i) = m_i$ and set $Z_0 = \ker p$. Now for $n \geq 0$, assume that the modules L_n and Z_n are defined. Then Z_n is a submodule of L_n which is finitely generated (since A is left Noetherian); choose a finite generating family $(x_{n,i})_{i\in I_{n+1}}$ of Z_n, put $L_{n+1} = Z^{\oplus I_{n+1}}$, define d_{n+1} by $d_{n+1}(e_i) = x_{n,i}$ and set $Z_{n+1} = \ker d_{n+1}$. By this process, we get an exact sequence

$$\cdots \longrightarrow L_{n+1} \xrightarrow{d_{n+1}} L_n \longrightarrow \cdots \longrightarrow L_0 \xrightarrow{p} M \longrightarrow 0$$

with each L_n free and finitely generated. In particular, this shows that any finitely generated A-modules possesses a free resolution with each term finitely generated. In fact, we can prove a more general result:

Proposition 8.2.5. *Let M be an A-complex and let $n_0 \in \mathbb{Z}$ suc that $H_n(M) = 0$ for $n < n_0$.*

(a) There exists a free A-complex L such that $L_n = 0$ for $n < n_0$ and a quasi-isomorphism $f : L \to M$.

(b) Suppose that A is left Noetherian and the A-modules $H_n(M)$ are finitely generated. Then there exists a free A-complex L such that $L_n = 0$ for $n < n_0$ and L_n is finitely generated for each n, and a quasi-isomorphism $f : L \to M$.

Proof. Let M' be the sub-complex of M such that $M'_n = M_n$ for $n > n_0$, $M'_{n_0} = Z_{n_0}(M)$, and $M'_n = 0$ for $n < n_0$. Then the canonical injection from M' to M is a quasi-isomorphism, so by

replacing M with M', we may assume that $M_n = 0$ for $n < n_0$. The proposition then follows from by apply **??** for $r \geq n_0$. □

Lemma 8.2.6. *Let M be a complex and $r \in \mathbb{Z}$. There exists a complex N and a quasi-isomorphism $\alpha : N \to M$ such that $\alpha_n : N_n \to M_n$ is an isomorphism for $n < r$ and N_r is a free A-module. If A is left Noetherian and the A-modules $H_r(M)$ and M_{r-1} and finitely generated, N_r can be chose to be finitely generated.*

8.2.5 Minimal projective resolutions

Let M be an A-module and

$$\cdots \longrightarrow P_n \xrightarrow{d_n} P_{n-1} \longrightarrow \cdots \longrightarrow P_0 \xrightarrow{d_0} M \longrightarrow 0 \tag{2.5.1}$$

be a resolution of M. We say (2.5.1) is a minimal projective resolution for M if for $n \geq 0$, the homomorphism $\delta_n : P_n \to \operatorname{im} d_n$ induced by d_n is a projective cover.

Proposition 8.2.7. *Let M be an A-module, P and P' two minimal projective resolutions of M and $f : P \to P'$ a morphism of resolutions. Then f is an isomorphism. In particular, minimal projective resolutions of M are all isomorphic.*

Proof. Let's set $\tilde{P}_n = P_n$ and $\tilde{P}'_n = P'_n$ for $n \neq -1$ and $\tilde{P}_{-1} = \tilde{P}' = M$; let $f_{-1} = 1_M$. We prove by induction that $f_n : \tilde{P}_n \to \tilde{P}'_n$ is an isomorphism. This is clear for $n = -1$; suppose then f_n and f_{n-1} are isomorphisms. Then it follows from the diagram

$$\begin{tikzcd} \tilde{P}_n \arrow[r, "d_n"] \arrow[d, "f_n"] & \tilde{P}_{n-1} \arrow[d, "f_{n-1}"] \\ \tilde{P}'_n \arrow[r, "d'_n"] & \tilde{P}_{n-1} \end{tikzcd}$$

that f_n induces an isomorphism g_n from $\ker d_n$ to $\ker d'_n$. Now from the uniqueness of projective covers, we then conclude that f_{n+1} is an isomorphism. □

Corollary 8.2.8. *Let M be an A-module, P and P' be projective resolutions of M. Suppose that P is minimal. Let $f : P \to P'$ and $g : P' \to P$ be two morphisms of resolutions. Then f is injective, g is surjective, and P' is a direct sum of* $\operatorname{im} f$ *and* $\ker g$*. Moreover* $\ker g$ *is null-homologous.*

Proof. In fact, $\alpha = g \circ f$ is an automorphism of P by Proposition 8.2.7. If $\tilde{f} = f \circ \alpha^{-1}$, then $\operatorname{im} \tilde{f} = \operatorname{im} f$ and $g \circ \tilde{f} = 1_P$, which implies $P' = \operatorname{im} \tilde{f} \oplus \ker g$. Now the sequence

$$0 \longrightarrow \ker g \longrightarrow P' \xrightarrow{g} P \longrightarrow 0$$

is exact, so $\ker g$ is null-homologous. □

Proposition 8.2.9. *Let M be an A-module and (P, p) a projective resolution of M. Let $\mathfrak{r}$ be the Jacobson radical of A. Suppose that, either P_n is finitely generated for all n, or $\mathfrak{r}$ is nilpotent. Then for (P, p) to be minimal, it is necessary and sufficient that the complex $(A/\mathfrak{r}) \otimes_A P$ has zero differentials, or equivalently $d(P_{n+1}) \subseteq \mathfrak{r} P_n$ for all n.*

Proof. If (P, p) is minimal, then by **??** the homomorphism

$$1 \otimes \delta_n : (A/\mathfrak{r}) \otimes_A P_n \to (A/\mathfrak{r}) \otimes_A \operatorname{im} d_n$$

is an isomorphism. It then follows from the exact sequence

$$0 \longrightarrow \operatorname{im} d_{n+1} \xrightarrow{j_n} P_n \xrightarrow{\delta_n} \operatorname{im} d_n \longrightarrow 0$$

that the homomorphism $1 \otimes j_n : (A/\mathfrak{r}) \otimes_A \operatorname{im} d_{n+1} \to (A/\mathfrak{r}) \otimes_A P_n$ is zero. Since $d_{n+1} = j_n \circ \delta_{n+1}$, this shows $1_{A/\mathfrak{r}} \otimes d_{n+1} = 0$ for all n.

Conversely, assume that $1 \otimes d_n$ is zero for all n, which means $\operatorname{im} d_n = \ker d_{n-1}$ is contained in $\mathfrak{r}P_{n-1}$. Since δ_{n-1} is surjective, it then follows from **??** that δ_{n-1} is a projective cover for all $n \geq 1$, so (P, p) is minimal. □

Proposition 8.2.10. *Suppose that A is a local left Noetherian ring, and let M be a finitely generated A-module. Then M possesses a minimal projective resolution (P, p) where P_n is free and finitely generated for all $n \geq 0$.*

Proof. In fact, in this case any finitely generated module has a projective cover, so e may construct the complex (P, d) just as $(L(M), d)$, which means P_0 is the projective cover of M, and P_{n+1} is the projective cover of $\ker d_n$. The resulting complex is clearly minimal. □

8.2.6 Graded resolutions

In this part we let A be a graded rign with graduation $(A_n)_{n\in\mathbb{Z}}$ such that $A_n = 0$ for $n < 0$. We say a graded A-module M is bounded from below if $M_n = 0$ for n small enough. It is clear that every finitely generated graded A-module is bounded from below.

Proposition 8.2.11. *If A be a bounded below A-module (resp. if M is a finitely generated A-module and A is left Noetherian), there exists an exact sequence of graded A-modules*

$$\cdots \longrightarrow L_n \xrightarrow{d_n} L_{n-1} \longrightarrow \cdots \longrightarrow L_1 \xrightarrow{d_1} L_0 \xrightarrow{d_0} M \longrightarrow 0$$

where L_i are free graded modules that are bounded from below (resp. free graded modules that are finitely generated), and d_i are graded homomorphisms of degree 0.

Proof. If N is a graded A-module that is bounded from below (resp. finitely generated and A is left Noetherian), there exist a free graded A-module L that is bounded from below (resp. finitely generated) and a surjective graded homomorphism $L \to N$. Consider the kernel of the map $L \to N$ and repeat this process, we see the claim follows. □

8.2.7 The standard resolution

Suppose that A is an algebra over a commutative ring k. For $n \geq 0$, let B_n be the tensor product of k of $(n+2)$ modules equal to A. Then B_n is an (A, A)-bimodule by actting A on the first and last factors of the tensor product. For $n \geq 1$, we define homomorphisms of bimodules d_n^i and d_n from B_n to B_{n-1} by the formulae

$$d_n^i(x_0 \otimes \cdots \otimes x_{n+1}) = x_0 \otimes \cdots \otimes x_i x_{i+1} \otimes \cdots \otimes x_{n+1} \quad \text{for } 0 \leq i \leq n$$

and $d_n = \sum_{i=0}^{n}(-1)^i d_n^i$. It is clear that, if $i < j$, then

$$d_{n-1}^i \circ d_n^j = d_{n-1}^{j-1} \circ d_n^i$$

so we have

$$d_{n-1} \circ d_n = \sum_{0\le i<j\le n} (-1)^{i+j} d_{n-1}^i \circ d_n^j + \sum_{0\le j\le i\le n-1} (-1)^{i+j} d_{n-1}^i \circ d_n^j = 0$$

Therefore, if we set $B_n = 0$ for $n < 0$ and $d_n = 0$ for $n \le 0$, the sequece (B_n, d_n) is a complex of (A, A)-bimodules, which is then denoted by $B(A)$. For any left A-module M, we denote by $B(A, M)$ the complex formed by $B_n \otimes M$ and $d_n \otimes 1_M$. This is a complex of left A-modules.

We define an A-linear map ε_M from $B_0(A, M) = (A \otimes_k A) \otimes_A M$ to M by the formula

$$\varepsilon_M(a \otimes b \otimes m) = abm \quad \text{for} \quad a, b \in A, m \in M.$$

We have $\varepsilon_M \circ d_1 = 0$, so the graded homomorphism $\bar{\varepsilon}_M : B(A, M) \to M$, which coincides with ε_M at degree M, is a morphism of complexes.

Proposition 8.2.12. *The map $\bar{\varepsilon}_M : B(A, M) \to M$ is a homotopy equivalence of complexes of A-modules. In particular, $(B(A, M), \bar{\varepsilon}_M)$ is a left resolution for the A-module M.*

Proof. For $n \ge 0$, we define a k-linear map

$$s_n(x_0 \otimes \cdots \otimes x_{n+1}) = 1 \otimes x_0 \otimes \cdots \otimes x_{n+1} \quad \text{for} \quad x_0, \ldots, x_{n+1} \in A.$$

This is a homomorphism of left A-modules, and one can verify that

$$d_{n+1}^i \circ s_n = s_{n-1} \circ d_n^{i-1}, \quad d_{n+1}^0 \circ s_n = 1_{B_n}$$

for $n \ge 1$ and $1 \le i \le n+1$. This then implies

$$d_{n+1} \circ s_n + s_{n-1} \circ d_n = 1_{B_n} \quad \text{for} \quad n \ge 1. \tag{2.7.1}$$

Moreover, we have

$$d_1 \circ s_0(x_0 \otimes x_1) = x_0 \otimes x_1 - 1 \otimes x_0 x_1 \quad \text{for} \quad x_0, x_1 \in A. \tag{2.7.2}$$

Let $\eta : A \to A \otimes_k A$ be the map defined by $\eta(a) = 1 \otimes a$, and $\bar{\eta} : A \to B(A)$ the morphism of complexes which coincides with η at degree 0. It is clear that $\bar{\varepsilon}_A \circ \bar{\eta} = 1_A$, and the formulae (2.7.1), (2.7.2) show that $d \circ s + s \circ d = 1_{B(A)} - \bar{\eta} \circ \bar{\varepsilon}_A$. Put $\bar{\eta}_M = \bar{\eta} \otimes 1_M$, $d_M = d \otimes 1_M$ and $s_M = s \otimes 1_M$, we then deduce that

$$\bar{\varepsilon}_M \circ \bar{\eta}_M = 1_M, \quad d_M \circ s_M + s_M \circ d_M = 1_{B(A,M)} - \bar{\eta}_M \circ \bar{\varepsilon}_M.$$

Therefore $\bar{\varepsilon}_M$ is a homotopy equivalence of complexes of A-modules. □

The left resolution $(B(A, M), \bar{\varepsilon}_M)$ is called the **standard resolution** of the A-module M. If A and M are projective k-modules (Resp. free, flat), the resolution $B(A, M)$ is a projective (resp. free, flat) resolution of M.

8.2.8 Resolutions and Grothendieck groups

If $\mathscr{C}$ is a set of classes of A-modules, we say a left resolution (P, p) is **bounded of type** $\mathscr{C}$ if the complex P is bounded of type $\mathscr{C}$.

Theorem 8.2.13. *Let $\mathscr{C}_0$ and $\mathscr{C}$ be two additive and left exact sets of classes of A-modules such that $\mathscr{C}_0 \subseteq \mathscr{C}$ and any A-module of type $\mathscr{C}$ has a left resolution bounded of type $\mathscr{C}$. Then the induced homomorphism $\alpha : K(\mathscr{C}_0) \to K(\mathscr{C})$ is bijective; if M is an A-module of type $\mathscr{C}$ and (P, p) is a left resolution of M bounded of type $\mathscr{C}_0$, we have $\alpha^{-1}([M]_{\mathscr{C}}) = \chi_{\mathscr{C}_0}(P)$.*

8.3 Tensor product

From now on, we will assume that A is a k-algebra where k is a commutative ring. The role of k is of an auxiliary nature; we have in mind mainly the following three special cases:

(a) we consider a general ring A, and put $k = \mathbb{Z}$.

(b) we consider a general ring A, and let k to be the center of A.

(c) we consider a commutative ring A and set $k = A$.

8.3.1 Tensot product of complexes

Let (M, d) be a complex of right A-modules and (N, d) be a complex of left A-modules. Then we can endow the tensor product $M \otimes_A N$ a graduation by setting

$$(M \otimes_A N)_n = \sum_{p+q=n} (M_p \otimes N_q).$$

Let D be the k-linear endomorphism of degree -1 on $M \otimes_A N$ such that

$$D(x \otimes y) = dx \otimes y + (-1)^p x \otimes dy, \quad x \in M_p, y \in N_q. \tag{3.1.1}$$

We have $D \circ D = 0$ since, by (3.1.1)

$$D^2(x \otimes y) = ddx \otimes y + (-1)^{p-1} dx \otimes dy + (-1)^p dx \otimes dy - x \otimes ddy = 0.$$

The resulting complex $(M \otimes_A N, D)$ is called the **tensor product** of the complexes (M, d) and (N, d).

Example 8.3.1 (Example of tensor products of complexes).

(a) If N is reduced to a single term N_0, then $(M \otimes N)_n = M_n \otimes_A N_0$ and $D = d \otimes 1_{N_0}$. For example $M \otimes_A A$ is identified with M.

(b) For any integer r, we have $(M \otimes_A N)[r] = M[r] \otimes_A N$. However, $(M \otimes_A N)[r]$ and $M \otimes_A N[r]$ are in general different (this is a sign issue).

Let p, q be integers, $x \in Z_p(M)$, $y \in Z_q(N)$; then the element $x \otimes y$ of $M_p \otimes N_q$ belongs to $Z_{p+q}(M \otimes N)$ by (3.1.1). Moreover, if $x' \in M_{p+1}$, $y' \in N_{q+1}$, we have

$$(x + dx') \otimes (y + dy') = x \otimes y + D(x' \otimes y + (-1)^p (x + dx') \otimes y').$$

By passing to quotients, we then deduce a canonical k-linear map

$$\gamma_{p,q}(M,N) : H_p(M) \otimes_A H_q(N) \to H_{p+q}(M \otimes_A N).$$

If we give $H(M) \otimes_A H(N)$ the graduation such that

$$(H(M) \otimes H(N))_n = \sum_{p+q=n} H_p(M) \otimes_A H_q(N)$$

then $\gamma_{p,q}$ together define a graded k-linear map of degree 0

$$\gamma(M,N) : H(M) \otimes_A H(N) \to H(M \otimes_A N).$$

Proposition 8.3.2. *If the complexes M and N are positive, then $M \otimes_A N$ is positive and the canonical k-linear map*

$$\gamma_{0,0}(M,N) : H_0(M) \otimes_A H_0(N) \to H_0(M \otimes_A N)$$

is bijective.

Proof. Consider two exact sequences of the form

$$M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \longrightarrow 0 \qquad N' \xrightarrow{\gamma} N \xrightarrow{\eta} N'' \longrightarrow 0$$

We will show that the canonical homomorphism $\beta \otimes \eta : M \otimes_A N \to M'' \otimes N''$ is surjective with kernel equals to $\mathrm{im}(\alpha \otimes 1_N) + \mathrm{im}(1_M \otimes \gamma)$. For this, consider the commutative diagram with exact rows are columns

$$\begin{tikzcd}
0 & 0 & 0 & \\
M' \otimes_A N'' \arrow[u] \arrow[r, "\alpha\otimes 1_{N''}"] & M \otimes_A N'' \arrow[u] \arrow[r, "\beta\otimes 1_{N''}"] & M'' \otimes_A N'' \arrow[u] \arrow[r] & 0 \\
M' \otimes_A N \arrow[u, "1_{M'}\otimes\eta"] \arrow[r, "\alpha\otimes 1_N"] & M \otimes_A N \arrow[u, "1_M\otimes\eta"] \arrow[r, "\beta\otimes 1_N"] & M'' \otimes_A N \arrow[u, "1_{M''}\otimes\eta"] \arrow[r] & 0 \\
M' \otimes_A N' \arrow[u, "1_{M'}\otimes\gamma"] \arrow[r, "\alpha\otimes 1_{N'}"] & M \otimes_A N' \arrow[u, "1_M\otimes\gamma"] \arrow[r, "\beta\otimes 1_{N'}"] & M'' \otimes_A N' \arrow[u, "1_{M''}\otimes\gamma"] \arrow[r] & 0
\end{tikzcd} \tag{3.1.2}$$

The first assertion is clear since we have $\beta \otimes \eta = (\beta \otimes 1_{N''}) \circ (1_M \otimes \eta)$, where both maps are surjective. Now, for an element $z \in M \otimes N$ to be in the kernel of $\beta \otimes \eta$, it is necessary and sufficient that $(1_M \otimes \eta)(z)$ to be contained in the kernel of $\beta \otimes 1_{N''}$, which, in view of the exactness of (3.1.2), is equal to the image of $\alpha \otimes 1_{N''}$. Since the homomorphism $1_{M'} \otimes \eta : M' \otimes_A N \to M' \otimes_A N''$, we then conclude that $(\beta \otimes \eta)(z) = 0$ if and only if there exists $a \in M' \otimes_A N$ such that

$$(1_M \otimes \eta)(z) = (\alpha \otimes \eta)(a) = (1_M \otimes \eta)(\alpha \otimes 1_N(a)).$$

If $b = z - \alpha \otimes 1_N(a)$, then we have $(1_M \otimes \eta)(b) = 0$, which means $b \in \mathrm{im}(1_M \otimes \gamma)$. This in turn implies $z \in \mathrm{im}(\alpha \otimes 1_N) + \mathrm{im}(1_M \otimes \gamma)$, which is our claim. Finally, by applying our claim to the following exact sequences

$$M_1 \longrightarrow M_0 \longrightarrow H_0(M) \longrightarrow 0 \qquad N_1 \longrightarrow N_0 \longrightarrow H_0(N) \longrightarrow 0$$

and noting that the image of $M_1 \otimes N_0$ and $M_0 \otimes N_1$ generate $B_0(M \otimes_A N)$, we conclude that $H_0(M \otimes_A N)$ is identified with $H_0(M) \otimes_A H_0(N)$, which completes the proof. □

Let $\alpha : M \to M'$ and $\beta : N \to N'$ be morphism of complexes of right A-module and left A-modules, respectively. Then $\alpha \otimes \beta : M \otimes_A N \to M' \otimes_A N'$ is a morphism of complex of k-modules. In fact, it is graded of degree 0, and for $x \in M_p$, $y \in N_q$,

$$\begin{aligned}(\alpha \otimes \beta)(D(x \otimes y)) &= \alpha(dx) \otimes \beta(y) + (-1)^p \alpha(x) + \beta(dy) \\ &= d\alpha(x) \otimes \beta(y) + (-1)^p \alpha(x) \otimes d(\beta(y)) = D(\alpha(x) \otimes \beta(y)).\end{aligned}$$

Moreover, we have the following commutative diagram

$$\begin{tikzcd} H(M) \otimes_A H(N) \arrow[r, "\gamma(M,N)"] \arrow[d, "H(\alpha)\otimes H(\beta)"'] & H(M \otimes_A N) \arrow[d, "H(\alpha\otimes\beta)"] \\ H(M') \otimes_A H(N') \arrow[r, "\gamma(N',N')"] & H(M' \otimes_A N') \end{tikzcd}$$

Let A° be the opposite k-algebra of A, M° (resp. N°) the complex M (resp. N) considered as a complex of left A°-modules (resp. right A°-modules). Let

$$\sigma(M, N) : M \otimes_A N \to N^\circ \otimes_{A^\circ} N^\circ$$

be the unique graded k-linear map of degree 0 such that, for $x \in M_p$, $y \in N_q$, we have

$$\sigma(M, N)(x \otimes y) = (-1)^{pq} x \otimes y.$$

Proposition 8.3.3. *The map $\sigma(M, N) : M \otimes_A N \to N^\circ \otimes_{A^\circ} M^\circ$ is an isomorphism of complexes of k-modules, whose inverse is $\sigma(N^\circ, N^\circ)$.*

Proof. Since the map $\sigma(M, N)$ and $\sigma(N^\circ, N^\circ)$ are inverses of each other, it amounts to show that $\sigma(M, N)$ is a morphism of complexes. Now for $x \in M_p = M_p^\circ$, $y \in N_q = N_q^\circ$, we have (we denote by D° the differential of $N^\circ \otimes_{A^\circ} M^\circ$)

$$\begin{aligned}\sigma(M, N)(D(x \otimes y)) &= \sigma(M, N)(dx \otimes y + (-1)^p x \otimes dy) \\ &= (-1)^{(p+1)q} y \otimes dx + (-1)^{p+p(q+1)} dy \otimes x \\ &= (-1)^{pq} dy \otimes x + (-1)^{pq+q} y \otimes dx \\ &= (-1)^{pq} D^\circ(y \otimes x) = D^\circ \circ \sigma(M, N)(x \otimes y).\end{aligned}$$

This proves the claim. □

The isomorphism $\sigma(M, N) : M \otimes_A N \to N^\circ \otimes_{A^\circ} M^\circ$ is called the **commutation isomorphism** of the tensor product $M \otimes_A N$.

Let $\alpha : M \to M'$ and $\beta : N \to N'$ be morphism of complexes of right A-module and left A-modules, respectively. Then we have a commutative diagram

$$\begin{tikzcd} M \otimes_A N \arrow[r, "\sigma(M,N)"] \arrow[d, "\alpha\otimes\beta"'] & N^\circ \otimes_{A^\circ} M^\circ \arrow[d, "\beta\otimes\alpha"] \\ M' \otimes_A N' \arrow[r, "\sigma(M',N')"] & N'^\circ \otimes_{A^\circ} M'^\circ \end{tikzcd}$$

Now assume that A is commutative. We consider three complexes M, N, P of A-modules. The canonical homomorphism of A-modules

$$\varphi : (M \otimes_A N) \otimes_A P \to M \otimes_A (N \otimes_A P)$$

is an isomorphism of complexes, which can be verified from the definition of differentials. Moreover generally, let $(M^{(i)}, d^{(i)})_{1 \leq i \leq r}$ be a family of complexes of A-modules. Define a graduation on the A-module $M = \bigotimes_{i=1}^{r} M^{(i)}$ such that

$$M_n = \sum_{p_1+p_2+\cdots+p_r=n} (M^{(1)})_{p_1} \otimes \cdots \otimes (M^(r))_{p_r}$$

and define a graded A-homomorphism of degree -1 by

$$D(x_1 \otimes \cdots \otimes x_r) = \sum_{j=1}^{r} (-1)^{p_1+\cdots+p_{j-1}} x_1 \otimes \cdots \otimes x_{j-1} \otimes dx_j \otimes x_{j+1} \otimes \cdots \otimes x_r$$

where $x_i \in (M^{(i)})_{p_i}$ for each $i = 1, \ldots, n$. Then (M, D) is a complex of A-modules, called that tensor product of the family $(M^{(i)}, d^{(i)})$. We define similarly a graded homomorphism of degree 0

$$\gamma(M^{(i)}) : \bigotimes_{i=1}^{r} H(M^{(i)}) \to H(\bigotimes_{i=1}^{r} M^{(i)}).$$

Remark 8.3.1. Suppose that each $M^{(i)}$ has a structure of graded A-algebra and $d^{(i)}$ is an antiderivation. Then with the graded algebra structure on the tensot product $\bigotimes_{i=1}^{r} M^{(i)}$, the differential D is an antiderivation.

8.3.2 Tensor products and homotopies

Proposition 8.3.4. *Let M, M' be complexes of right A-modules and N, N' be complexes of left A-modules. Let $\alpha_1 : M \to M'$, $\alpha_2 : M \to M'$ and $\beta_1 : N \to N'$, $\beta_2 : N \to N'$ be morphism of complexes.*

(a) If α_1 is homotopic to α_2 and β_1 is homotopic to β_2, then the two morphisms $\alpha_1 \otimes \beta_1$ and $\alpha_2 \otimes \beta_2$ from $M \otimes N$ to $M' \otimes N'$ are homotopic.

(b) If α_1 and β_1 are homotopy equivalences, then $\alpha_1 \otimes \beta_1$ is a homotopy equivalence.

(c) If M and N are null-homotopic, then $M \otimes_A N$ is null-homotopic.

Proof. If α_1 is homotopic to α_2 and β_1 is homotopic to β_2, there exist graded homomorphisms $s : M \to M'$ and $h : N \to N'$ od degree 1 such that

$$\alpha_1 - \alpha_2 = ds + sd, \quad \beta_1 - \beta_2 = dh + hd.$$

Let $S : M \otimes_A N \to M' \otimes_A N'$ be the unique graded homomorphism of degree 1 such that, for $x \in M_p$, $y \in N_q$, we have

$$S(x \otimes y) = s(x) \otimes \beta_1(y) + (-1)^p \alpha_2(x) \otimes h(y).$$

We then have

$$\begin{aligned}
&(DS+SD)(x\otimes y) = D(s(x)\otimes\beta_1(y)+(-1)^p\alpha_2(x)\otimes h(y)) + S(dx\otimes y)+(-1)^pS(x\otimes dy)\\
&= ds(x)\otimes\beta_1(y)+(-1)^{p+1}s(x)\otimes d\beta_1 y+(-1)^p d\alpha_2(x)\otimes h(y)+\alpha_2(x)\otimes dh(y)\\
&\quad + s(dx)\otimes\beta_1(y)+(-1)^{p-1}\alpha_2(dx)\otimes h(y)+(-1)^p s(x)\otimes\beta_1(dy)+\alpha_2(x)\otimes h(dy)\\
&= (ds+sd)(x)\otimes\beta_1(y)+\alpha_2(x)\otimes(dh+hd)(y)\\
&= (\alpha_1-\alpha_2)(x)\otimes\beta_1(y)+\alpha_2(x)\otimes(\beta_1-\beta_2)(y)\\
&= \alpha_1(x)\otimes\beta_1(y)-\alpha_2(x)\otimes\beta_2(y).
\end{aligned}$$

This shows $DS+SD=\alpha_1\otimes\beta_1-\alpha_2\otimes\beta_2$, whence (a). The rest of the assertions follow from (a) immediately. □

Corollary 8.3.5. *Let N be a splitting complex of left A-modules such that $H(N)$ is flat. Then for any complex M of right A-modules, the canonical map*

$$\gamma(M,N): H(M)\otimes_A H(N)\to H(M\otimes_A N)$$

is bijective. In particular, this happens if $B(M)$ and $H(M)$ are projective.

Proof. By Proposition 8.1.16, there exists a homotopy equivalence $\beta: N\to H(N)$, so from Proposition 8.3.4 we conclude that $1_M\otimes\beta$ is a homotopy equivalence from $M\otimes_A N$ to $M\otimes_A H(N)$. Since

$$H(1_M\otimes\beta)\circ\gamma(M,N)=\gamma(M,H(N))\circ(1_M\otimes H(\beta))$$

and $H(1_M\otimes\beta)$ and $H(\beta)$ are bijective, it suffices to show that $\gamma(M,H(N))$ is bijective, and we are then reduced to the case where N is flat and have zero differential. In this case the canonical exact seequences

$$0\longrightarrow Z(M)\xrightarrow{i}M\xrightarrow{\delta}B(M)[-1]\longrightarrow 0$$
$$0\longrightarrow B(M)\xrightarrow{j}Z(M)\xrightarrow{\pi}H(M)\longrightarrow 0$$

induces the following exact sequences:

$$0\longrightarrow Z(M)\otimes_A N\xrightarrow{i\otimes 1}M\otimes_A N\xrightarrow{\delta\otimes 1}B(M)[-1]\otimes_A N\longrightarrow 0$$
$$0\longrightarrow B(M)\otimes_A N\xrightarrow{j\otimes 1}Z(M)\otimes_A N\xrightarrow{\pi\otimes 1}H(M)\otimes_A N\longrightarrow 0$$

Since $d=i\circ j\circ\delta$, we have $D=d\otimes 1_N=(i\otimes 1)\circ(j\otimes 1)\circ(\delta\otimes 1)$. This shows the canonical map $Z(M)\otimes_A N\to Z(M\otimes_A N)$ and $B(M)\otimes_A N\to B(M\otimes_A N)$ are bijective, hence so is $\gamma(M,N)$ by passing to quotient. □

We now consider a positive complex E which is flat at each degree. We shall show that the operation $-\otimes E$ preserves quasi-isomorphisms. For this, we first establish some lemmas.

Lemma 8.3.6. *Let M be a complex of right A-modules and E a complex of left A-modules. Suppose that $H(M)=0$ and E is flat and right bounded. Then $H(M\otimes_A E)=0$.*

Proof. For $k \in \mathbb{Z}$, let $T^{(k)}$ be the sub-complex of $M \otimes_A E$ such that

$$T_n^{(k)} = \sum_{p+q=n, q \leq k} M_p \otimes_A E_q.$$

Then $T^{(k-1)} \subseteq T^{(k)}$ and we have an exact sequence of complexes:

$$0 \longrightarrow T^{(k-1)} \xrightarrow{i_k} T^{(k)} \xrightarrow{\pi} M \otimes_A E_k[-k] \longrightarrow 0$$

where i_k is the canonical inclusion and π the canonical projection. By Corollary 8.3.5, we have $H(M \otimes_A E_k[-k]) = 0$, so i_k is a quasi-isomorphism. We have $T^{(k)} = 0$ for k small enough, since E is right bounded, hence $H(T^{(k)}) = 0$ for any k by induction on k. Finally, the canonical morphism $\varinjlim T^{(k)} \to M \otimes_A E$ is evidently an isomorphism, so $H(M \otimes_A E) = 0$ (Proposition 8.1.2). □

Lemma 8.3.7. *If $\alpha : M \to N$ is a morphism of complexes of right bounded A-modules and E is a complex of right A-modules, then the complexes* $\mathrm{Cone}(\alpha) \otimes_A E$ *and* $\mathrm{Cone}(\alpha \otimes 1_E)$ *are isomorphic.*

Proof. By definition, $\mathrm{Cone}(\alpha) \otimes_A E$ is the graded module $(M[-1] \oplus N) \otimes_A E$ with the differential D defined by

$$D((x, y) \otimes z) = (-dx, dy + \alpha(x)) \otimes z + (-1)^p (x, y) \otimes dz$$

for $x \in M_{p-1}, y \in N_p, z \in E_q$. On the other hand, the complex $\mathrm{Cone}(\alpha \otimes 1_E)$ is the graded module $(M \otimes_A N)[-1] \oplus (N \otimes_A E)$ with the differential D defined by

$$\begin{aligned} D(x \otimes z, y \otimes z) &= (-dx \otimes z - (-1)^{p-1} x \otimes dz, dy \otimes z + (-1)^p y \otimes dz + \alpha(x) \otimes z) \\ &= (-dx \otimes z, dy \otimes z + \alpha(x) \otimes z) + (-1)^p (x \otimes dz, y \otimes dz) \end{aligned}$$

where $x \in M_{p-1}, y \in N_p, z \in E_q$. Our claim is then immediate. □

Proposition 8.3.8. *Let $\alpha : M \to N$ be a quasi-isomorphism of complexes of right A-modules and E be a complex of right A-modules which is flat and right bounded. Then*

$$\alpha \otimes 1_E : M \otimes_A E \to N \otimes_A E$$

is a quasi-isomorphism of complexes of k-modules.

Proof. In fact, by Corollary 8.1.23, α (resp. $\alpha \otimes 1_E$) is a quasi-isomorphism if and only if $\mathrm{Cone}(\alpha)$ (resp. $\mathrm{Cone}(\alpha \otimes 1_E)$) is exact. We then conclude the assertion from Lemma 8.3.6 and Lemma 8.3.7. □

8.3.3 The twisted product and its properties

For an A-module E, we denote by $p_E : L(E) \to E$ the canonical free resolution of E. Now let M be a right A-module and N a left A-module. The **twisted product** of M and N are defined to be the graded k-module

$$\mathrm{Tor}^A(M, N) = H(L(M) \otimes_A L(N)).$$

The homogeneous components of $\mathrm{Tor}^A(M,N)$ are then

$$\mathrm{Tor}_n^A(M,N) = H_n(L(M) \otimes L(N)).$$

Since $L(M)$ and $L(N)$ and positive, we have $\mathrm{Tor}_n^A(M,N) = 0$ for $n < 0$.

Let $\alpha : M \to M'$ be a homomorphism of right A-modules and $\beta : N \to N'$ a homomorphism of left A-modules. We set $\mathrm{Tor}^A(\alpha,\beta) = H(L(f) \otimes_A L(\beta))$; this is a graded homomorphism of k-modules

$$\mathrm{Tor}^A(\alpha,\beta) : \mathrm{Tor}^A(M,N) \to \mathrm{Tor}^A(M',N')$$

whose homogeneous components are then

$$\mathrm{Tor}_n^A(\alpha,\beta) : \mathrm{Tor}_n^A(M,N) \to \mathrm{Tor}_n^A(M',N').$$

By Proposition 8.3.2, the canonical homomorphism

$$\gamma_{0,0} : H_0(L(M) \otimes_A L_0(N)) \to H_0(L(M) \otimes_A L(N))$$

is bijective; using the isomorphisms $M \to H_0(L(M))$ and $N \to H_0(L(N))$, we then get a canonical isomorphism

$$\gamma_{M,N} : M \otimes_A N \to \mathrm{Tor}_0^A(M,N).$$

Recall that we have $L(1_M) = 1_{L(M)}$ and $L(1_N) = 1_{L(N)}$, so by passing to homology,

$$\mathrm{Tor}^A(1_M, 1_N) = 1_{\mathrm{Tor}^A(M,N)}.$$

If $\alpha' : M' \to M''$ (resp. $\beta' : N' \to N''$) is a homomorphism of right A-modules (resp. left A-modules), then $L(\beta' \circ \beta) = L(\beta') \circ L(\beta)$ and $L(\alpha' \circ \alpha) = L(\alpha') \circ L(\alpha)$, so

$$\mathrm{Tor}^A(\alpha' \circ \alpha, \beta' \circ \beta) = \mathrm{Tor}^A(\alpha',\beta') \circ \mathrm{Tor}^A(\alpha,\beta).$$

Therefore, the operation Tor^A is a bifunctor on its two variables.

Consider the following morphisms of k-complexes:

$$L(M) \otimes_A N \xleftarrow{1_{L(M)} \otimes p_N} L(M) \otimes_A L(N) \xrightarrow{p_M \otimes 1_{L(N)}} M \otimes_A L(N)$$

and the k-homomorphisms induced on homology:

$$H(L(M) \otimes_A N) \xleftarrow{\psi_M(N)} \mathrm{Tor}^A(M,N) \xrightarrow{\psi_N(M)} H(M \otimes_A L(N))$$

By Proposition 8.3.8, $1_{L(M)} \otimes p_N$ and $p_M \otimes 1_{L(N)}$ are quasi-isomorphisms, so we conclude that:

Proposition 8.3.9. *The k-homomorphisms*

$$\psi_M(N) : \mathrm{Tor}^A(M,N) \to H(L(M) \otimes_A N)$$
$$\psi_N(M) : \mathrm{Tor}^A(M,N) \to H(M \otimes_A L(N))$$

are bijective.

Corollary 8.3.10. *If M or N is flat, then* $\mathrm{Tor}_i^A(M,N) = 0$ *for* $i > 0$.

Proof. Suppose that N (resp. M) is flat; then $p_M \otimes 1_N : L(M) \otimes_A N \to M \otimes_A N$ (resp. $1_M \otimes p_N : M \otimes_A L(N) \to M \otimes_A N$) is a quasi-isomorphism by Proposition 8.3.8, hence $H_i(L(M) \otimes_A N)$ (resp. $H_i(M \otimes_A L(N))$) is zero for $i > 0$. □

Remark 8.3.2. If $\beta : N \to N'$ is a homomorphism of left A-modules, we have

$$(1_{L(M)} \otimes \beta) \circ (1_{L(M)} \otimes 1_N) = (1_{L(M)} \otimes 1_N) \circ (1_{L(M)} \circ L(\beta)),$$

so the diagram

$$\begin{tikzcd} \mathrm{Tor}^A(M,N) \arrow[r, "\psi_M(N)"] \arrow[d, "\mathrm{Tor}^A(1,\beta)"] & H(L(M) \times_A N) \arrow[d, "H(1\otimes\beta)"] \\ \mathrm{Tor}^A(M,N') \arrow[r, "\psi_M(N')"] & H(L(M) \otimes_A N') \end{tikzcd}$$

is commutative. Simialrly, if $\alpha : M \to M'$ is a homomorphism of right A-modules, we have a commutative diagram:

$$\begin{tikzcd} \mathrm{Tor}^A(M,N) \arrow[r, "\psi_N(M)"] \arrow[d, "\mathrm{Tor}^A(\alpha,1)"] & H(M \times_A L(N)) \arrow[d, "H(\alpha\otimes 1)"] \\ \mathrm{Tor}^A(M',N) \arrow[r, "\psi_N(M')"] & H(M' \otimes_A L(N)) \end{tikzcd}$$

Proposition 8.3.11. *The map* $(\alpha,\beta) \mapsto \mathrm{Tor}^A(\alpha,\beta)$*:*

$$\mathrm{Hom}_A(M,M') \times \mathrm{Hom}_A(N,N') \to \mathrm{Hom}_k(\mathrm{Tor}^A(M,N), \mathrm{Tor}^A(M',N'))$$

is k-linear.

Proof. Let $\alpha \in \mathrm{Hom}_A(M,M')$, $\beta_1, \beta_2 \in \mathrm{Hom}_A(N,N')$, and $\lambda_1, \lambda_2 \in k$. Then the morphisms $\lambda_1(L(\alpha) \otimes \beta_1) + \lambda_2(L(\alpha) \otimes \beta_2)$ and $L(\alpha) \otimes (\lambda_1\alpha_1 + \lambda_2\beta_2)$ from $L(M) \otimes_A N$ to $L(M) \otimes_A N'$ coincide; by Proposition 8.3.9 and Remark 8.3.2, we then have

$$\mathrm{Tor}^A(\alpha, \lambda_1\beta_1 + \lambda_2\beta_2) = \lambda_1 \mathrm{Tor}^A(\alpha,\beta_1) + \lambda_2 \mathrm{Tor}^A(\alpha,\beta_2).$$

Similarly, the map $\alpha \mapsto \mathrm{Tor}^A(\alpha,\beta)$ is k-linear. □

Corollary 8.3.12. *Let $\lambda \in k$. If λ annihilates M or N, it annihilates* $\mathrm{Tor}^A(M,N)$.

Proof. In fact, we have $\lambda 1_{\mathrm{Tor}(M,N)} = \mathrm{Tor}^A(\lambda 1_M, 1_N) = \mathrm{Tor}^A(1_M, \lambda 1_N)$, so the claim follows. □

Proposition 8.3.13. *Let $(M_i)_{i\in I}$ be a family of right A-modules and $(N_j)_{j\in J}$ be a family of left A-modules. The following canonical homomorphism is bijective.*

$$\bigoplus_{i\in I, j\in J} \mathrm{Tor}^A(M_i, N_j) \to \mathrm{Tor}^A(\bigoplus_{i\in I} M_i, \bigoplus_{j\in J} N_j)$$

Proof. It suffices to show that for a right module M (resp. for a left module N), the canonical homomorphism $\bigoplus_{j\in J} \mathrm{Tor}^A \to \mathrm{Tor}^A(M, \bigoplus_{j\in J} N_j)$ (resp. the canonical homomorphism $\bigoplus_{i\in I} \mathrm{Tor}^A(M_i, N) \to \mathrm{Tor}^A(\bigoplus_{i\in I} M_i, N)$) is bijective. This follows from Proposition 8.1.2 and the isomorphisms $\bigoplus_j (L(M) \otimes_A N_j) \to L(M) \otimes_A \left(\bigoplus_j N_j\right)$ and $\bigoplus_i (M_i \otimes_A L(N)) \to \left(\bigoplus_i M_i\right) \otimes_A L(N)$. □

Simialrly, since tensor product commutes with direct limits, we have the following:

Proposition 8.3.14. *Let $(M_\alpha, \phi_{\alpha'\alpha})_{\alpha\in I}$ be a inductive system of right A-modules and $(N_\beta, \psi_{\beta'\beta})_{\beta\in J}$ be a inductive system of left A-modules. The following graded k-homomorphism is bijective:*

$$\varinjlim_{(\alpha,\beta)\in I\times J} \mathrm{Tor}^A(M_\alpha, N_\beta) \to \mathrm{Tor}^A(\varinjlim_{\alpha\in I} M_\alpha, \varinjlim_{\beta\in J} N_\beta)$$

Corollary 8.3.15. *Let $(M_i, \phi_{ji})_{i\in I}$ be a inductive system of right A-modules and $(N_i, \psi_{ji})_{i\in I}$ be a inductive system of left A-modules. The following canonical graded k-homomorphism is bijective:*

$$\varinjlim_{i\in I} \mathrm{Tor}^A(M_i, N_i) \to \mathrm{Tor}^A(\varinjlim_{i\in I} M_i, \varinjlim_{i\in I} N_i)$$

8.3.4 The long exact sequence of twisted products

Let M be a right A-module. Recall that for a left A-module N, we have an isomorphism $\psi_M(N) : \mathrm{Tor}^A(M, N) \to H(L(M) \otimes_A N)$. Now consider an exact sequence

$$\mathscr{E} : \ 0 \longrightarrow N' \xrightarrow{\alpha} N \xrightarrow{\beta} N'' \longrightarrow 0$$

of left A-modules. The induced sequence k-complexes

$$\mathscr{E}^M : \ 0 \longrightarrow L(M) \otimes_A N' \xrightarrow{1\otimes\alpha} L(M) \otimes_A N \xrightarrow{1\otimes\beta} L(M) \otimes_A N'' \longrightarrow 0$$

is then exact by Lemma 8.3.6. Let $\partial(\mathscr{E}^M) : H(L(M) \otimes_A N'') \to H(L(M) \otimes_A N')$ be the connecting homomorphism. The corresponding homomorphism:

$$\partial(M, \mathscr{E}) : \mathrm{Tor}^A(M, N'') \to \mathrm{Tor}^(M, N')$$

is called the connecting homomorphism of the twisted product relative to the module M and the exact sequence $\mathscr{E}$. This is a graded k-homomorphism of degree -1, whose homogeneous components are $\partial_n(M, \mathscr{E}) : \mathrm{Tor}^A_n(M, N'') \to \mathrm{Tor}^A_{n-1}(M, N')$.

Theorem 8.3.16. *We have a long exact sequence*

$$\cdots \longrightarrow \mathrm{Tor}^A_1(M, N'') \xrightarrow{\partial_1(M,\mathscr{E})} M \otimes_A N' \xrightarrow{1\otimes\alpha} M \otimes_A N \xrightarrow{1\otimes\beta} M \otimes_A N'' \longrightarrow 0$$

Proof. In fact, the diagram

$$\begin{array}{ccccccccc}
\mathrm{Tor}(M, N') & \xrightarrow{\mathrm{Tor}(1,\alpha)} & \mathrm{Tor}(M, N) & \xrightarrow{\mathrm{Tor}(1,\beta)} & \mathrm{Tor}(M, N'') & \xrightarrow{\partial(M,\mathscr{E})} & \mathrm{Tor}(M, N') & \xrightarrow{\mathrm{Tor}(1,\alpha)} & \mathrm{Tor}(M, N) \\
\downarrow{\scriptstyle \psi_M(N')} & & \downarrow{\scriptstyle \psi_M(N)} & & \downarrow{\scriptstyle \psi_M(N'')} & & \downarrow{\scriptstyle \psi_M(N')} & & \downarrow{\scriptstyle \psi_M(N)} \\
H(L(M) \otimes N') & \xrightarrow{H(1\otimes\alpha)} & H(L(M) \otimes N) & \xrightarrow{H(1\otimes\beta)} & H(L(M) \otimes N'') & \xrightarrow{\partial(\mathscr{E}^M)} & H(L(M) \otimes N') & \xrightarrow{H(1\otimes\alpha)} & H(L(M) \otimes N)
\end{array}$$

is commutative. Now the first row is exact and the vertical maps are isomorphisms, so our claim follows. □

Corollary 8.3.17. *If we have* $\mathrm{Tor}_1^A(M, N'') = 0$ *(for example, if* N'' *is flat), then the sequence*

$$0 \longrightarrow M \otimes_A N' \xrightarrow{1\otimes\alpha} M \otimes_A N \xrightarrow{1\otimes\beta} M \otimes_A N'' \longrightarrow 0$$

is exact.

Example 8.3.18. Let $\mathfrak{a}$ be an ideal of A and consider the exact sequence

$$0 \longrightarrow \mathfrak{a} \longrightarrow A \longrightarrow A/\mathfrak{a} \longrightarrow 0$$

of left A-modules. Since A is a flat module, we have $\mathrm{Tor}^A(M, A) = 0$, so from the long exact sequence in Theorem 8.3.16 we deduce isomorphisms

$$\mathrm{Tor}_{i+1}^A(M, A/\mathfrak{a}) \to \mathrm{Tor}_i^A(M, \mathfrak{a}) \quad \text{for} \quad i > 0$$

and an exact sequence

$$0 \longrightarrow \mathrm{Tor}_1^A(M, A/\mathfrak{a}) \longrightarrow M \otimes_A \mathfrak{a} \longrightarrow M \otimes_A A \longrightarrow M \otimes_A (A/\mathfrak{a}) \longrightarrow 0$$

It then follows that $\mathrm{Tor}_1^A(M, A/\mathfrak{a})$ is identified with the kernel of the canonical map $M \otimes_A \mathfrak{a} \to M$. For example, if M is a module of the form $A/\mathfrak{b}$ where $\mathfrak{b}$ is a right ideal of A, we obtain an isomorphism $\mathrm{Tor}_1^A(A/\mathfrak{b}, A/\mathfrak{a}) \cong (\mathfrak{a} \cap \mathfrak{b})/\mathfrak{a}\mathfrak{b}$.

Proposition 8.3.19. *Let* $M \to M'$ *be a homomorphism of right* A*-modules and*

$$\begin{aligned} \mathscr{E} :\ & 0 \longrightarrow E' \longrightarrow E \longrightarrow E'' \longrightarrow 0 \\ \mathscr{F} :\ & 0 \longrightarrow F' \longrightarrow F \longrightarrow F'' \longrightarrow 0 \end{aligned}$$

be a commutative diagram of left A*-modules with exact rows. Then the diagram of* k*-modules*

$$\begin{tikzcd} \mathrm{Tor}^A(M, E'') \arrow[r, "\partial(M,\mathscr{E})"] \arrow[d] & \mathrm{Tor}^A(M, E') \arrow[d] \\ \mathrm{Tor}^A(M', F'') \arrow[r, "\partial(M',\mathscr{F})"] & \mathrm{Tor}^A(M', F') \end{tikzcd}$$

is commutative.

Proof. Note that we have the following commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & L(M) \otimes_A E' \arrow[r] \arrow[d] & L(M) \otimes_A E \arrow[r] \arrow[d] & L(M) \otimes_A E'' \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & L(M') \otimes_A F' \arrow[r] & L(M') \otimes_A F \arrow[r] & L(M') \otimes_A F'' \arrow[r] & 0 \end{tikzcd}$$

so the result follows from the natruality of the connecting homomorphism. □

8.3.5 Künneth formula

Now consider a complex (M, d) of right A-modules and (N, d) a complex of left A-modules. We have the following canonical exact sequences

$$0 \longrightarrow Z(M) \xrightarrow{j} M \xrightarrow{\delta} B(M)[-1] \longrightarrow 0 \tag{3.5.1}$$

$$0 \longrightarrow B(M) \xrightarrow{i} Z(M) \xrightarrow{\pi} H(M) \longrightarrow 0 \tag{3.5.2}$$

We then obtain a k-homomorphism

$$H(\delta \otimes 1) : H(M \otimes_A N) \to H(B(M) \otimes_A N)[-1],$$

and a connecting homomorphism

$$\partial(B(M), H(N)) : \mathrm{Tor}_1^A(H(M), H(N)) \to B(M) \otimes_A H(N).$$

If we give $\mathrm{Tor}_1^A(H(M), H(N))$ the graduation whose degree n homogeneous component is $\sum_{p+q=n} \mathrm{Tor}_1^A(H_p(M), H_q(N))$, this homomorphism is then graded of degree 0. Finally, wecall that we have a canonical homomorphism

$$\gamma(B(M), N) : B(M) \otimes_A H(N) \to H(B(M) \otimes_A N).$$

Theorem 8.3.20. *Suppose that the A-modules $B(M)$ and $Z(M)$ are flat. There exists a unique graded homomorphism of k-modules of degree -1,*

$$\alpha : H(M \otimes_A N) \to \mathrm{Tor}_1^A(H(M), H(N))$$

completing the following diagram

$$\begin{tikzcd}
H(M \otimes_A N) \arrow[r, "\alpha"] \arrow[d, "H(\delta\otimes 1)"'] & \mathrm{Tor}_1^A(H(M), H(N))[-1] \arrow[d, "\partial(B(M),H(N))"] \\
H(B(M) \otimes_A N)[-1] & (B(M) \otimes_A H(N))[-1] \arrow[l, "\gamma(B(M),N)"']
\end{tikzcd}$$

and such that the following sequence of k-modules is exact:

$$0 \longrightarrow H(M) \otimes_A H(N) \xrightarrow{\gamma(M,N)} H(M \otimes_A N) \xrightarrow{\alpha} \mathrm{Tor}_1^A(H(M), H(N))[-1] \longrightarrow 0 \tag{3.5.3}$$

Proof. Since $B(M)$ is flat, we have the following exact sequence (Corollary 8.3.17) induced from (3.5.1):

$$0 \longrightarrow Z(M) \otimes_A N \xrightarrow{j\otimes 1} M \otimes_A N \xrightarrow{\delta\otimes 1} (B(M) \otimes_A N)[-1] \longrightarrow 0 \tag{3.5.4}$$

We claim that the connecting homomorphism from $H(B(M) \otimes_A N)$ to $H(Z(M) \otimes_A N)$ is given by $H(i \otimes 1)$. To see this, let $z \in Z(B(M) \otimes_A N)$; since $B(M)$ is flat, we have $Z(B(M) \otimes_A N) = B(M) \otimes_A Z(N)$, so z is of the form $z = \sum_\lambda da_\lambda \otimes b_\lambda$, where $a_\lambda \in M$, $b_\lambda \in N$, and $db_\lambda = 0$. The image of the class of z under the connecting homomorphism is by definition given by the class of $D(\sum a_\lambda \otimes b_\lambda) = \sum da_\lambda \otimes b_\lambda = (i \otimes 1)(z)$, so our claim is justified. Now, the long exact sequence

associated with (3.5.4) is then

$$\begin{tikzcd}
\cdots \arrow[r] & H(B(M)\otimes_A N) \arrow[r, "H(i\otimes 1)"] & H(Z(M)\otimes_A N) \arrow[dll, "H(j\otimes 1)"'] \\
& H(M\otimes_A N) \arrow[r, "H(\delta\otimes 1)"] & H(B\otimes_A N)[-1] \arrow[r] & \cdots
\end{tikzcd}$$

On the other hand, since $Z(M)$ is flat, the following equence deduced from (3.5.2) is exact:

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Tor}_1^A(H(M),H(N)) \arrow[r, "\partial"] & B(M)\otimes_A H(N) \arrow[dll, "i\otimes 1"'] \\
& Z(M)\otimes_A H(N) \arrow[r, "\pi\otimes 1"] & H(M)\otimes_A H(N) \arrow[r] & 0
\end{tikzcd}$$

Recall that we have the following canonical homomorphisms:

$$\begin{aligned}
\gamma_B &= \gamma(B(M),N) : B(M)\otimes_A H(N) \to H(B(M)\otimes_A N) \\
\gamma_Z &= \gamma(Z(M),N) : Z(M)\otimes_A H(N) \to H(Z(M)\otimes_A N) \\
\gamma_H &= \gamma(H(M),N) : H(M)\otimes_A H(N) \to H(M\otimes_A N)
\end{aligned}$$

whence a commutative diagram of graded k-modules, with exact rows:

$$\begin{tikzcd}
B(M)\otimes_A H(N) \arrow[r, "i\otimes 1"] \arrow[d, "\gamma_B"] & Z(M)\otimes_A H(N) \arrow[r, "\pi\otimes 1"] \arrow[d, "\gamma_Z"] & H(M)\otimes_A H(N) \arrow[rr] \arrow[d, "\gamma_H"] & & 0 \\
H(B(M)\otimes_A N) \arrow[r, "H(i\otimes 1)"] & H(Z(M)\otimes_A N) \arrow[r, "H(j\otimes 1)"] & H(M\otimes_A N) \arrow[r, "H(\delta\otimes 1)"] \arrow[d, dashed, "\alpha"] & H(B(M)\otimes_A N)[-1] & \\
& 0 \arrow[r] & \mathrm{Tor}_1^A(H(M),H(N))[-1] \arrow[r, "\partial"] & (B(M)\otimes_A H(N))[-1] \arrow[u, "\gamma_B"]
\end{tikzcd}$$

Since the complexes $B(M)$ and $Z(M)$ have zero differentials and are flat, the homomorphisms γ_B and γ_Z are bijective by Corollary 8.3.5. This implies, by the four lemma, on the one hand that the γ_H is injective with image equal to $\ker H(\delta\otimes 1)$ (since $\pi\otimes 1$ is surjective and γ_Z is bijective, we have $\operatorname{im}\gamma_H = \operatorname{im} H(j\otimes 1)$), on the other hand that $\gamma_B\circ\partial(B(M),H(N))$ is injective with image equal to $\operatorname{im} H(\delta\otimes 1)$. These together proves the theorem. □

Corollary 8.3.21. *Suppose that $B(M)$ and $B(N)$ are projective and $Z(M)$ is flat. Then the exact sequence (3.5.3) splits.*

Proof. It suffices to show that, if $B(M)$ and $B(N)$ are projective, then the canonical homomorphism

$$\gamma(M,N) : H(M)\otimes_A H(N) \to H(M\otimes_A N)$$

possesses a k-linear retraction. For this, we recall that by Remark 8.1.2, there exists quasi-isomorphisms $\varphi : M \to H(M)$ and $\psi : N \to H(N)$ such that $H(\varphi) = 1_{H(M)}$ and $H(\psi) = 1_{H(N)}$.

In the commutative diagram

$$\begin{tikzcd} H(M) \otimes_A H(N) \arrow[r, "\gamma(M,N)"] \arrow[d, "H(\varphi)\otimes H(\psi)"'] & H(M \otimes_A N) \arrow[d, "H(\varphi\otimes\psi)"] \\ H(M) \otimes_A H(N) \arrow[r, "\gamma(H(M),H(N))"] & H(M) \otimes_A H(N) \end{tikzcd}$$

the maps $H(\varphi) \otimes H(\psi)$ and $\gamma(H(M), H(N))$ are identities, whence our claim. □

Corollary 8.3.22 (Universal Coefficients Formula). *Suppose that the ring A is a PID. If the complexes M and N are free, the sequence (3.5.3) of A-modules is exact and split.*

Proof. In this case, $B(M)$, $Z(M)$, and $B(N)$ are submodules of the free modules M and N, hence are free, and we can apply Corollary 8.3.21. □

Corollary 8.3.23 (Künneth Formula). *Suppose that M and $H(M)$ are flat and M is right bounded. Then the canonical homomorphism*

$$\gamma(M, N) : H(M) \otimes_A H(N) \to H(M \otimes_A N)$$

is bijective.

Proof. By Theorem 8.3.20, it suffices to prove that $B(M)$ and $Z(M)$ are flat. Now from the exact sequences (3.5.1) and (3.5.1), we see the flatness of $B_{n-1}(M)$ implies that of $Z_n(M)$, which in turn imples that $B_n(M)$ is flat. Since $B_n(M) = 0$ for n small enough, the assertion then follows by induction on n. □

Corollary 8.3.24. *Let $\alpha : M \to M'$ be a quasi-isomorphism of complexes of right A-modules that are flat and right bounded. Then for any complex N of left A-modules, the morphism $\alpha \otimes 1_E : M \otimes_A N \to M' \otimes_A N$ is a quasi-isomorphism.*

8.4 Modules of extensions

We retain the assumption that A is a k-algebra over a commutative ring k. Without further specification, by A-modules we mean left A-modules.

8.4.1 The Hom complex of complexes

Let (M, d) and (N, d) be A-complexes. Consider the graded k-module $\mathrm{Homgr}_A(M, N)$: for each $n \in \mathbb{Z}$, the homogeneous component $\mathrm{Homgr}_A(M, N)_n$ is the k-module of A-linear graded homomorphisms of degree n from M to N. In other words, $\mathrm{Homgr}_A(M, N)$ is identified with the A-module

$$\bigoplus_{n\in\mathbb{Z}} \prod_{p\in\mathbb{Z}} \mathrm{Hom}_A(M_p, N_{p+n}) = \bigoplus_{n\in\mathbb{Z}} \prod_{p+q=n} \mathrm{Hom}_A(M^p, N_q).$$

We define a k-linear map $D_n : \mathrm{Homgr}_A(M, N)_n \to \mathrm{Homgr}_A(M, N)_{n-1}$ by the formula

$$D_n(f) = d \circ f - (-1)^n f \circ d. \tag{4.1.1}$$

It is clear that we have

$$\begin{aligned} D_{n-1} \circ D_n(f) &= D_{n-1}(d \circ f - (-1)^n f \circ d) \\ &= d^2 \circ f - (-1)^n d \circ f \circ d - (-1)^{n-1} d \circ f \circ d - f \circ d^2 = 0 \end{aligned}$$

The couple $(\mathrm{Homgr}_A(M,N), D)$ is then a complex of k-modules, called the **Hom complex** of M and N. For simplicity, we just denote this complex by $(\mathrm{Hom}(M,N), D)$. For example, $\mathrm{Hom}(A,N)$ is canonically identified with N, and for $r \in \mathbb{Z}$ we have $\mathrm{Hom}(M,N)[r] = \mathrm{Hom}(M, N[r])$.

The elements of $Z_n(\mathrm{Hom}(M,N))$ are the graded homomorphisms f of degree n from M to N such that $d \circ f = (-1)^n f \circ d$, which are the morphisms from the complex M to $N[n]$. We call these homomorphisms as **morphisms of complexes of degree n** from M to N. If $f, g \in Z_n(\mathrm{Hom}(M,N))$ and $s \in \mathrm{Hom}(M,N)_{n+1}$, then the condition $f - g = Ds$ amounts to that s is a homotopy of the morphisms f and g from M to $N[n]$, so $H_n(\mathrm{Hom}(M,N))$ is the k-module of homotopy classes of morphisms of degree n from M to N.

Let $\gamma \in Z_n(\mathrm{Hom}(M,N))$ be represented by $f \in Z_n(\mathrm{Hom}(M,N))$ and $p \in \mathbb{Z}$. Then f is a morphism from M to $N[n]$, so $H_p(f)$ is a homomorphism from $H_p(M)$ to $H_{p+n}(N)$. Since $H_p(f)$ does not depend on the homotopy class of f, we get a canonical induced homomorphism of k-modules:

$$H_n(\mathrm{Hom}(M,N)) \to \mathrm{Hom}_A(H_p(M), H_{p+n}(N)),$$

whence a canonical graded k-linear homomorphism of degree 0:

$$\lambda(M,N) : H(\mathrm{Hom}(M,N)) \to \mathrm{Hom}(H(M), H(N)).$$

The homogeneous component of $\lambda(M,N)$ are denoted by

$$\lambda^n(M,N) : H^n(\mathrm{Hom}(M,N)) \to \prod_{p+q=n} \mathrm{Hom}_A(H_p(M), H^q(N)).$$

Proposition 8.4.1. *If M is positive and N is negative, the complex* $\mathrm{Hom}(M,N)$ *is negative, and the canonical k-linear map*

$$\lambda^0(M,N) : H^0(\mathrm{Hom}(M,N)) \to \mathrm{Hom}_A(H_0(M), H^0(N))$$

is bijective.

Proof. We have the following exact sequences:

$$\begin{tikzcd} 0 \arrow[r] & H & & 0(N) \arrow[r, "i"] & N^0 \arrow[r] & N^1 \\ & & M_1 \arrow[r, "d_1"] & M_0 \arrow[r, "\pi"] & H_0(M) \arrow[r] & 0 \end{tikzcd} \tag{4.1.2}$$

Since $\mathrm{Hom}^0(M,N)$ is identified with $\mathrm{Hom}_A(M_0, N^0)$, the k-modules $Z^0(\mathrm{Hom}(M,N))$ is identified with the set of homomorphisms $f : M_0 \to N^0$ such that $d^0 \circ f = 0$ and $f \circ d = 0$. Since $B^0(\mathrm{Hom}(M,N))$ is zero, the map λ^0 then associates the class of f modulo $\{0\}$ to the homomorphism $\varphi : H_0(M) \to H^0(N)$ such that $f = i \circ \varphi \circ \pi$, hence our proposition. □

Let $\alpha : M' \to M$ and $\beta : N \to N'$ be morphisms of complexes. Then the canonical

homomorphism $\mathrm{Hom}(\alpha,\beta) : \mathrm{Hom}(M,N) \to \mathrm{Hom}(M',N')$, defined by $f \mapsto \beta \circ f \circ \alpha$, is a morphisms of complexes, which follows immediately from (4.1.1). Moreover, the following diagram is commutative:

$$\begin{tikzcd}
H(\mathrm{Hom}(M,N)) \arrow[r, "\lambda(M,N)"] \arrow[d, "H(\mathrm{Hom}(\alpha,\beta))"'] & \mathrm{Hom}(H(M),H(N)) \arrow[d, "\mathrm{Hom}(H(\alpha),H(\beta))"] \\
H(\mathrm{Hom}(M',N')) \arrow[r, "\lambda(M',N')"] & \mathrm{Hom}(H(M'),H(N'))
\end{tikzcd}$$

Proposition 8.4.2. *Let* $0 \longrightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} N \longrightarrow 0$ *be an exact sequence of complexes.*

(a) If F is a projective complex and E is an injective complex, the following sequences are exact:

$$0 \longrightarrow \mathrm{Hom}(F,M') \longrightarrow \mathrm{Hom}(F,M) \longrightarrow \mathrm{Hom}(F,M'') \longrightarrow 0$$
$$0 \longrightarrow \mathrm{Hom}(M',E) \longrightarrow \mathrm{Hom}(M,E) \longrightarrow \mathrm{Hom}(M'',E) \longrightarrow 0$$

(b) If the sequence $0 \longrightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} N \longrightarrow 0$ *splits, then for any complex E, the sequences*

$$0 \longrightarrow \mathrm{Hom}(E,M') \longrightarrow \mathrm{Hom}(E,M) \longrightarrow \mathrm{Hom}(E,M'') \longrightarrow 0$$
$$0 \longrightarrow \mathrm{Hom}(M',E) \longrightarrow \mathrm{Hom}(M,E) \longrightarrow \mathrm{Hom}(M'',E) \longrightarrow 0$$

are exact as complexes of k-modules.

Proof. In case (a), we have the exact sequences

$$0 \longrightarrow \mathrm{Hom}_A(F_p,M'_q) \longrightarrow \mathrm{Hom}_A(F_p,M_q) \longrightarrow \mathrm{Hom}_A(F_p,M''_q) \longrightarrow 0$$
$$0 \longrightarrow \mathrm{Hom}_A(M'_p,E_q) \longrightarrow \mathrm{Hom}_A(M_p,E_q) \longrightarrow \mathrm{Hom}_A(M''_p,E_q) \longrightarrow 0$$

for any $p,q \in \mathbb{Z}$. By taking product and direct sum, we then conclude (a). The proof of (b) is similar. □

8.4.2 Hom complex and homotopies

Proposition 8.4.3. *Let $\alpha_1 : M' \to M$, $\alpha_2 : M' \to M$, $\beta_1 : N \to N'$, $\beta_2 : N \to N'$ be morphisms of complexes.*

(a) If α_1 is homotopic to α_2 and β_1 is homotopic to β_2, then $\mathrm{Hom}(\alpha_1,\beta_1)$ *is homotopic to* $\mathrm{Hom}(\alpha_2,\beta_2)$.

(b) If α_1 and β_1 are homotopy equivalences, so is $\mathrm{Hom}(\alpha_1,\beta_1)$.

(c) If M and N are null-homotopic, so is $\mathrm{Hom}(M,N)$.

Proof. If $\alpha_1 \sim \alpha_2$ and $\beta_1 \sim \beta_2$, there exist homomorphisms $s : M' \to N$ and $h : N \to N'$ of degree 1 such that

$$\alpha_1 - \alpha_2 = ds + sd, \quad \beta_1 - \beta_2 = dh + hd.$$

Let $W : \mathrm{Hom}(M,N) \to \mathrm{Hom}(M',N')$ be the graded homomorphism of degree 1 such that

$$W(f) = hf\alpha_1 + (-1)^n \beta_2 f s$$

for $f \in \mathrm{Hom}(M,N)_n$. We then have

$$\begin{aligned}(DW+WD)(f) &= D[hf\alpha_1 + (-1)^n\beta_2 fs] + W[df - (-1)^n fd] \\ &= dhf\alpha_1 - (-1)^{n+1}hf\alpha_1 d + (-1)^n d\beta_2 fs + \beta_2 fsd \\ &\quad + hdf\alpha_1 + (-1)^{n-1}\beta_2 dfs - (-1)^n hfd\alpha_1 + \beta_2 fds \\ &= [dh+hd]f\alpha_1 + \beta_2 f[sd+ds] \\ &= (\beta_1-\beta_2)f\alpha_1 + \beta_2 f(\alpha_1-\alpha_2) \\ &= \beta_1 f\alpha_1 - \beta_2 f\alpha_2.\end{aligned}$$

This shows $DW + WD = \mathrm{Hom}(\alpha_1,\beta_1) - \mathrm{Hom}(\alpha_2,\beta_2)$, so assertion (a) follows. The rest of the claims follow from (a). □

Corollary 8.4.4. *If M is splitting and $H(M)$ is projective (resp. if N is splitting and $H(N)$ is injective), the canonical homomorphism*

$$\lambda(M,N) : H(\mathrm{Hom}(M,N)) \to \mathrm{Hom}(H(M),H(N))$$

is bijective.

8.5 Koszul complex

8.5.1 The Koszul complex associated with a linear form

Let A be a ring, E an A-module, $\alpha : E \to A$ a linear form, and $\bigwedge(E)$ the exterior algebra of the A-module E. For $x \in \bigwedge(E)$, we denote by $d_\alpha(x)$ the interior product $x \lrcorner \alpha$. In other words, d_α is given by

$$d_\alpha(e_1 \wedge \cdots \wedge e_n) = \sum_{i=1}^{n} (-1)^{i+1}\alpha(e_i)e_1 \wedge \cdots \wedge \widehat{e_i} \wedge \cdots \wedge e_n \tag{5.1.1}$$

for $e_1,\dots,e_n$ in E. The map $d_\alpha : \bigwedge(E) \to \bigwedge(E)$ is an antiderivation of degree -1 with squre zero, which is the unique antiderivation on the A-algebra $\bigwedge(E)$ extending $\alpha : \bigwedge^1(E) \to \bigwedge^0(E)$. The resulting complex $(\bigwedge(E), d_\alpha)$ is denoted by $K^A(\alpha)$ or $K(\alpha)$, called the **Koszul complex associated with α**. The homogeneous components of $K(\alpha)$ is then $K_n(\alpha) = \bigwedge(E) = K^{-n}(\alpha)$. It is clear that $K(\alpha)$ is positive and $H_0(K(\alpha)) = A/\mathfrak{a}$ where $\mathfrak{a}$ is the ideal $\alpha(E)$ of A.

Now for any complex of A-modules M, we put

$$\begin{aligned} K^A_\bullet(\alpha,M) &= M \otimes_A K^A(\alpha) & K^\bullet_A(\alpha,M) &= \mathrm{Hom}(K^A(\alpha),M), \\ H^A_\bullet(\alpha,M) &= H(M \otimes_A K^A(\alpha)) & H^\bullet_A(\alpha,M) &= H(\mathrm{Hom}(K^A(\alpha),M)). \end{aligned}$$

There are then canonical homomorphisms

$$\gamma_0 : H_0(M) \otimes_A A/\mathfrak{a} \to H^A_0(\alpha,M), \quad \lambda^0 : H^0_A(\alpha,M) \to \mathrm{Hom}_A(A/\mathfrak{a}, H^0(M)).$$

By Proposition 8.3.2 and **??**, if the complex M is positive (resp. negative), then $K^A_\bullet(\alpha,M)$ (resp. $K^\bullet_A(\alpha,M)$) is positive (resp. negative), and γ_0 (resp. λ_0) is bijective.

Let $f : M \to N$ be a morphism of complexes. Then we have the following morphisms:

$$K^A_\bullet(\alpha, f) : K^A_\bullet(\alpha, M) \to K^A_\bullet(\alpha, N), \quad K^\bullet_A(\alpha, f) : K^\bullet_A(\alpha, M) \to K^\bullet_A(\alpha, N),$$

which are nothing but $f \otimes 1_{K(u)}$ and $\mathrm{Hom}(1_{K(u)}, f)$. The induced maps on homology modules are denoted by $H^A_\bullet(\alpha, f)$ and $H^\bullet_A(\alpha, f)$. It is clear that these constructions are functorial.

Proposition 8.5.1. *For $x \in E$, let $L_x : y \mapsto x \wedge y$ be the left multiplication on $\bigwedge(E)$; then*

$$d_\alpha \circ L_x + L_x \circ d_\alpha = \alpha(x) \cdot 1_{\wedge(E)}.$$

Proof. In fact, we have

$$(d_\alpha \circ L_x + L_x \circ d_\alpha)(y) = d_\alpha(x \wedge y) + x \wedge d_\alpha(y);$$

since d_α is an antiderivation, this is equal to $d_\alpha(x) \wedge y = \alpha(x)y$. □

Corollary 8.5.2. *If α is surjective then $K(\alpha)$ is null-homotopic, so is $K^A_\bullet(\alpha, M)$ and $K^\bullet_A(\alpha, M)$ for any complex M.*

Proof. If α is surjective, then in particular there exist $x \in E$ such that $\alpha(x) = 1$. Then $K(\alpha)$ is null-homotopic by Proposition 8.5.1, with homotopy given by L_x. The complexes $K^A_\bullet(\alpha, M)$ and $K^\bullet(\alpha, M)$ are then null-homotopic by **??**. □

Corollary 8.5.3. *Let M be a complex and $\mathrm{Ann}(M)$ its annihilator. Then $\mathfrak{a} + \mathrm{Ann}(M)$ annihilates $H^A_\bullet(\alpha, M)$ and $H^\bullet_A(\alpha, M)$.*

Proof. For any $\lambda \in \mathfrak{a}$, the homothety $\lambda_{K(\alpha)}$ is homotopic to zero by Proposition 8.5.1, hence so is $1_M \otimes \lambda_{K(\alpha)}$ and $\mathrm{Hom}(\lambda_{K(\alpha)}, 1_M)$ (Proposition 8.3.4 and **??**); it follows that λ annihilates $H^A_\bullet(\alpha, M)$ and $H^\bullet_A(\alpha, M)$. If $\lambda \in \mathrm{Ann}(M)$, then $1_M \otimes \lambda_{K(\alpha)}$ and $\mathrm{Hom}(\lambda_{K(\alpha)}, 1_M)$ are already zero maps. □

Suppose that E is projective (resp. $K(\alpha)$ is acyclic at positive degrees). Then the complex $\bigwedge(E)$ is projective (resp. is a resolution of $A/\mathfrak{a}$). By **??** (resp. **??**), we then have, for any A-module M, the homomorphisms

$$H^A_\bullet(\alpha, M) \to \mathrm{Tor}^A_\bullet(A/\mathfrak{a}, M) \qquad \mathrm{Ext}^\bullet_A(A/\mathfrak{a}, M) \to H^\bullet_A(\alpha, M),$$

resp.

$$\mathrm{Tor}^A_\bullet(A/\mathfrak{a}, M) \to H^A_\bullet(\alpha, M) \qquad H^\bullet_A(\alpha, M) \to \mathrm{Ext}^\bullet_A(A/\mathfrak{a}, M).$$

If E is projective and $K(\alpha)$ is acyclic at positive degrees, the homomorphisms above are bijective and inverses of each other (**??**).

Proposition 8.5.4. *Let $(E_i)_{i \in I}$ be a family of A-modules, where I is finite and totally ordered. Let α be a linear form on $\bigoplus_{i \in I} E_i$ and α_i its restriction on E_i. Then the canonical isomorphism of A-algebras:*

$$\eta : \bigotimes_{i \in I}^{g} \bigwedge(E_i) \to \bigwedge(\bigoplus_{i \in I} E_i)$$

is an isomorphism from the complex $\bigotimes_{i \in I} K(\alpha_i)$ to $K(\alpha)$.

Proof. In fact, by Remark 8.3.1, the differential D of the complex $\bigotimes_{i\in I} K(\alpha_i)$ is an antiderivation; the antiderivations d_α and $\eta \circ D \circ \eta^{-1}$ on $\bigwedge(\bigoplus E_i)$ both coincide on $\bigoplus E_i$ with the map $x \mapsto \alpha(x) \cdot 1$, hence are equal (**??**). □

Proposition 8.5.5. *Let M and N be two complexes of A-modules. Then we have the following canonical isomorphisms of complexes:*

$$M \otimes_A K^A_\bullet(\alpha, N) \to K^A_\bullet(\alpha, M \otimes_A N), \tag{5.1.2}$$

$$\mathrm{Hom}(N, K^\bullet_A(\alpha, M)) \to \mathrm{Hom}(K^A_\bullet(\alpha, N), M). \tag{5.1.3}$$

Proof. Recall that we have the following isomorphisms:

$$M \otimes_A (N \otimes_A K(\alpha)) \to (M \otimes_A N) \otimes_A K(\alpha),$$
$$\mathrm{Hom}(N, \mathrm{Hom}(K(\alpha), M)) \to \mathrm{Hom}(N \otimes_A K(\alpha), M);$$

The claim thus follows in view of the definition of $K^A_\bullet$ and $K^\bullet_A$. □

Corollary 8.5.6. *Let $\alpha : E \to A$ and $\beta : F \to A$ be two linear forms. Then we have the following isomorphisms of complexes:*

$$K^A_\bullet(\alpha \oplus \beta, M) \to K^A_\bullet(\alpha, K^A_\bullet(\beta, M)) \tag{5.1.4}$$

$$K^\bullet_A(\beta, K^\bullet_A(\alpha, M)) \to K^\bullet_A(\alpha \oplus \beta, M); \tag{5.1.5}$$

which by passing to homology induce the following isomorphisms of A-modules:

$$H^A_\bullet(\alpha \oplus \beta, M) \to H^A_\bullet(\alpha, K^A_\bullet(\beta, M)), \tag{5.1.6}$$

$$H^\bullet_A(\beta, K^\bullet_A(\alpha, M)) \to H^\bullet_A(\alpha \oplus \beta, M). \tag{5.1.7}$$

Proof. This follows by setting $N = K(\beta)$ in (5.1.2) and (5.1.3). Note that $K^A_\bullet(\alpha, K(\beta))$ is equal by definition to $K(\alpha) \otimes_A K(\beta)$, which is identified with $K(\alpha \oplus \beta)$, where $\alpha \oplus \beta$ is the linear form $(x, y) \mapsto \alpha(x) + \beta(y)$. □

Note that the homomorphism deduced from the product of the algebra $\bigwedge(E)$

$$m : K^A(\alpha) \otimes_A K^A(\alpha) \to K^A(\alpha)$$

is a morphism of complexes (since d_α is an antiderivation). Suppose that E is free with rank n and composing with the morphism $K^A(\alpha) \to \bigwedge^n(E)[-n]$ (which is just the identity in degree n), we deduce a morphism of complexes

$$\chi : K^A(\alpha) \otimes_A K^A(\alpha) \to \bigwedge^n(E)[-n];$$

by **??**, this morphism corresponds to a canonical morphism of complexes:

$$\phi : K^A(\alpha) \to \mathrm{Hom}(K^A(\alpha), \bigwedge^n(E)[-n])$$

which is bijective. For any complex M, we then deduce an isomorphism of complexes

$$\begin{tikzcd} K^A_\bullet(\alpha, M) = M \otimes_A K^A(\alpha) \arrow[r, "1_M \otimes \phi"] \arrow[d, dashed] & M \otimes \mathrm{Hom}(K^A(\alpha), \bigwedge^n(E)[-n]) \arrow[d] \\ K^\bullet_A(\alpha, M \otimes_A \bigwedge^n(E)[-n]) \arrow[r, equal] & \mathrm{Hom}(K^A(\alpha), M \otimes_A \bigwedge^n(E)[-n]) \end{tikzcd}$$

and hence a canonical isomorphism on homology modules:

$$H^A_\bullet(\alpha, M) \to H^{n-\bullet}_A(\alpha, M \otimes_A \textstyle\bigwedge^n(E)). \tag{5.1.8}$$

Since E is free of rank n, we know the module $\bigwedge^n(E)$ is isomorphic to A, so in particular, we have an isomorphism $H^A_\bullet(\alpha, M) \to H^{n-\bullet}_A(\alpha, M)$. Note however that this isomorphism is not canonical.

Proposition 8.5.7. *Consider an exact sequence of complexes:*

$$0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$$

(a) If E is flat then there is a long exact sequence of $H^A_\bullet(\alpha, -)$:

$$\cdots \longrightarrow H^A_n(\alpha, L) \longrightarrow H^A_n(\alpha, M) \longrightarrow H^A_n(\alpha, N) \longrightarrow H^A_{n-1}(\alpha, L) \longrightarrow \cdots$$

(b) If E is projective then there is also a long exact sequence of $H^\bullet_A(\alpha, -)$:

$$\cdots \longrightarrow H^n_A(\alpha, L) \longrightarrow H^n_A(\alpha, M) \longrightarrow H^n_A(\alpha, N) \longrightarrow H^{n+1}_A(\alpha, L) \longrightarrow \cdots$$

Proof. If E is flat (resp. projective) then $\bigwedge(E)$ is flat (resp. projective), so the sequence

$$0 \longrightarrow K^A_\bullet(\alpha, L) \longrightarrow K^A_\bullet(\alpha, M) \longrightarrow K^A_\bullet(\alpha, N) \longrightarrow 0$$

resp. the sequence

$$0 \longrightarrow K^\bullet_A(\alpha, L) \longrightarrow K^\bullet_A(\alpha, M) \longrightarrow K^\bullet_A(\alpha, N) \longrightarrow 0$$

The rest then follows from the long exact sequence theorem for homology modules. □

Proposition 8.5.8. *Let $\rho : A \to B$ be a ring homomorphism, $\rho_*(E)$ the B-module $E \otimes_A B$, and $\rho_*(\alpha) : \rho^*(E) \to B$ the linear form $1 \otimes \alpha$. Then the canonical homomorphism*

$$\psi : \textstyle\bigwedge_B(B \otimes_A E) \to B \otimes_A \bigwedge_A(E)$$

is an isomorphism of complexes of B-modules. In particular:

(a) for any complex N of B-modules, we have an isomorphism $\rho^*(K^B_\bullet(\rho_*(\alpha), N)) \to K^A_\bullet(\alpha, \rho^*(N))$ of complexes of A-modules, which is given by the following composition:

$$N \otimes_B (\textstyle\bigwedge_B(B \otimes_A E)) \xrightarrow{1_N \otimes \psi} N \otimes_B B \otimes_A \bigwedge_A(E) \longrightarrow B \otimes_A \bigwedge_A(E)$$

(b) *for any complex M of A-modules, we have an isomorphism $K^A_\bullet(\alpha, \rho_*(M)) \to \rho_*(K^A_\bullet(\alpha, M))$ of complexes of B-modules, whence an isomorphism*

$$H^A_\bullet(\alpha, \rho_*(M)) \to \rho_*(H^A_\bullet(\alpha, M))$$

if B is flat over A.

Proof. The first claim follows from **??**, the rest is then immediate. □

Let F be an A-module and $\beta : F \to A$ a linear form. Let $f : E \to F$ be a homomorphism such that $\beta \circ f = \alpha$. Then it follows from formula (**??**) that the homomorphism $\bigwedge(f) : \bigwedge(E) \to \bigwedge(F)$ satisfies

$$d_\alpha \circ \bigwedge(f) = \bigwedge(f) \circ d_\beta$$

hence defines a morphism $\bigwedge(f) : K^A(\alpha) \to K^A(\beta)$ of complexes. If M is an A-complex, we then get morphisms:

$$1_M \otimes \bigwedge(f) : K^A_\bullet(\alpha, M) \to K^A_\bullet(\beta, M), \quad \mathrm{Hom}(\bigwedge(f), 1_M) : K^\bullet_A(\alpha, M) \to K^\bullet_A(\beta, M).$$

8.5.2 The canonical Koszul complex of $S(E)$

Let A be a ring, E an A-module, $S(E)$ the symmetric algebra over E, and $S(E) \otimes_A E$ the $S(E)$-module induced by extending scalars. Let $\alpha : S(E) \otimes_A E \to S(E)$ be the linear form defined by $\alpha(s \otimes x) = sx$ for $s \in S(E)$ and $x \in E$. By the canonical isomorphism of $S(E)$-modules (**??**)

$$\bigwedge_{S(E)}(S(E) \otimes_A E) \to S(E) \otimes_A \bigwedge(E)$$

the differential of the complex $K^{S(E)}(\alpha)$ then corresponds to a map

$$d : S(E) \otimes_A \bigwedge(E) \to S(E) \otimes_A \bigwedge(E)$$

such that for $x_1, \dots, x_p, y_1, \dots, y_q$ in E, we have

$$d((x_1 \cdots x_p) \otimes (y_1 \wedge \cdots \wedge y_q)) = \sum_{i=1}^{q} (-1)^{i+1} y_i x_1 \cdots x_p \otimes (y_1 \wedge \cdots \wedge \widehat{y_i} \wedge \cdots \wedge y_q). \tag{5.2.1}$$

Note that d maps $S^p(E) \otimes \bigwedge^q(E)$ to $S^{p+1}(E) \otimes \bigwedge^{q-1}(E)$, so the complex $S(E) \otimes \bigwedge(E)$ breaks down into the direct sum of complexes described by the following diagrams

$$0 \longrightarrow S^0(E) \otimes_A \bigwedge^n(E) \longrightarrow S^1(E) \otimes_A \bigwedge^{n-1}(E) \longrightarrow \cdots \longrightarrow S^n(E) \otimes_A \bigwedge^0(E) \longrightarrow 0$$

which we denote by $\mathcal{E}_n$. If the A-module E is a direct sum of a finite family $(E_i)_{i \in I}$ where I is totally ordered, the canonical bijection

$$\bigotimes_{i \in I}^{g} (S(E_i) \otimes_A \bigwedge(E_i)) \to S(E) \otimes_A \bigwedge(E)$$

is an isomorphism of A-complexes (this follows from **??** and formula (5.2.1)).

Proposition 8.5.9. *If E is a flat A-module, then the complex $\mathscr{E}_n$ is exact for $n > 0$.*

Proof. □

8.5.3 Koszul complexes and alternating maps

Let k be a ring, M an k-module, I a finite set and $p \geq 0$ an integer. We say a map $m : I^p \to M$ is **alternating** if the following conditions are satisfied:

(a) for any permutation $\sigma \in \mathfrak{S}_p$ and any sequence $(\alpha_1, \dots, \alpha_p) \in I^p$, we have

$$m(\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(p)}) = \operatorname{sgn}(\sigma) m(\alpha_1, \dots, \alpha_p);$$

(b) for any sequence $(\alpha_1, \dots, \alpha_p) \in I^p$ such that two of the indices in $(\alpha_1, \dots, \alpha_p)$ are equal, we have $m(\alpha_1, \dots, \alpha_p) = 0$.

We denote by $C^p(I, M)$ the k-module of alternating maps from I^p to M.

If E_0 is a k_0-module and $(e_i)_{i \in I}$ is a family of elements in E_0, we define a map

$$\tau : \operatorname{Hom}_k(\textstyle\bigwedge^p(E_0), M) \to C^p(I, M)$$

by setting $\tau(f)(\alpha_1, \dots, \alpha_p) = f(e_{\alpha_1} \wedge \cdots \wedge e_{\alpha_p})$ for $f \in \operatorname{Hom}_k(\bigwedge^p(E_0), M)$. We also have a map

$$\eta : C^p(I, M) \to M \otimes_k \textstyle\bigwedge^p(E_0).$$

To define η, consider an element $m \in C^p(I, M)$; for any element $(\alpha_1, \dots, \alpha_p)$ of I^p, the element $m(\alpha_1, \dots, \alpha_p) \otimes (e_{\alpha_1} \wedge \cdots \wedge e_{\alpha_p})$ of $\bigwedge^p(E_0) \otimes_k M$ only depends on the subset $J = \{\alpha_1, \dots, \alpha_p\}$; we denote it by $\eta_J(m)$. The map η is then given by

$$\eta(m) = \sum_J \eta_J(m).$$

where J runs through subset of I with exactly p elements. By **??**, if the k-module E_0 is free with basis $(e_i)_{i \in I}$, the k-linear maps τ and η are bijective.

Let M be a k-module and $\boldsymbol{x} = (x_i)_{i \in I}$ be a finite permutable family of k-endomorphisms of M. Consider the polynomial $A = k[(X_i)_{i \in I}]$ and endow M with the A-module structure such that $P(X_i)m = P(x_i)m$ for $P \in A$ and $m \in M$. Also, let $\alpha : A^I \to A$ be the linear form that sends e_i to X_i for each $i \in I$, where $(e_i)_{i \in I}$ is the canonical basis for A^I. Consider the Koszul complex of k-modules $K^A_\bullet(\alpha, M)$ and $K^\bullet_A(\alpha, M)$; we have the canonical isomorphisms

$$\begin{gathered} K^\bullet_A(\alpha, M) = \operatorname{Hom}_A(\textstyle\bigwedge_A(A^I), M) \to \operatorname{Hom}_k(\bigwedge_k(k^I), M), \\ M \otimes_k \textstyle\bigwedge_k(k^I) \to M \otimes_A \bigwedge_A(A^I) = K^A_\bullet(\alpha, M); \end{gathered}$$

whence by composition with the isomorphisms τ and η of the isomorphisms of k-modules

$$\theta^p : K^p_A(\alpha, M) \to C^p(I, M), \quad \theta_p : C^p(I, M) \to K^A_p(\alpha, M).$$

By transporting or structure, we then get differentials ∂^p and ∂_p on $C^p(I, M)$:

$$\partial^p : C^p(I, M) \to C^{p+1}(I, M), \quad \partial_p : C^p(I, M) \to C^{p-1}(I, M).$$

For example, the differential ∂^p is given by

$$(\partial^p m)(\alpha_1, \dots, \alpha_{p+1}) = \sum_{j=1}^{p+1} (-1)^{j+1} x_{\alpha_j} m(\alpha_1, \dots, \widehat{\alpha_j}, \dots, \alpha_{p+1}). \tag{5.3.1}$$

The complex $(C^p(I, M), \partial^p)$ (resp. the complex $(C^p(I, M), \partial_p)$) is denoted by $K^\bullet(\boldsymbol{x}, M)$ (resp. $K_\bullet(\boldsymbol{x}, M)$) and called the ascending (resp. descending) **Koszul complex** associated with the module M and the sequence $(x_i)_{i \in I}$. We then have isomorphisms of complexes of k-modules:

$$\theta^\bullet : K_A^\bullet(\alpha, M) \to K^\bullet(\boldsymbol{x}, M)$$

Remark 8.5.1. Conversely, let B be a k-algebra, E a free B-module with basis $(e_i)_{i \in I}$, and M a B-module. The giving a linear form $\alpha : E \to B$ is equivalent to giving a family $\boldsymbol{x} = (x_i)_{i \in I}$ of elements of B, by the relation $x_i = \alpha(e_i)$. The complex of k-modules underlying $K_B^\bullet(\alpha, M)$ (resp. $K_\bullet^B(\alpha, M)$) is then identified, by the isomorphisms $\theta^\bullet$ (resp. $\theta_\bullet$), with the Koszul complex $K^\bullet(\boldsymbol{x}, M)$ (resp. $K_\bullet(\boldsymbol{x}, M)$). For example, $K^B(\alpha)$ is identified with $K^\bullet(\boldsymbol{x}, B)$.

We introduce the notations $H_\bullet(\boldsymbol{x}, M)$, $H^\bullet(\boldsymbol{x}, M)$, etc. The previous results apply mutatis mutandis, with the module A^I being free. For example, we have isomorphisms

$$H_0(\boldsymbol{x}, M) \to M/\mathfrak{x}M, \quad H^0(\boldsymbol{x}, M) \to \mathrm{Hom}_A(A/\mathfrak{x}, M),$$

where $\mathfrak{x}$ denotes the ideal $\sum Ax_i$ generated by x_i; and if $K_\bullet(\boldsymbol{x}, A)$ is acyclic at positive degrees, we have isomorphisms

$$H_\bullet(\boldsymbol{x}, M) \to \mathrm{Tor}_\bullet^A(k, M), \quad \mathrm{Ext}_A^\bullet(k, M) \to H^\bullet(\boldsymbol{x}, M).$$

Finally, suppose that I is totally ordered, for example $I = \{1, \dots, n\}$; then we can identify $\bigwedge^n(A^I)$ to A be choosing the basis element $e_1 \wedge \cdots \wedge e_n$. Simialrly, we can identify $K_p^A(\alpha, M)$ with $K_A^{n-p}(\alpha, M)$. By transporting structure by the isomorphisms θ_p and θ^{n-p}, we get an isomorphism

$$C^p(I, M) \to C^{n-p}(I, M)$$

where an element $m \in C^p(I, M)$ corresponds to an element $\check{m}$ of $C^{n-p}(I, M)$ such that

$$m(\alpha_1, \dots, \alpha_p) = \check{m}(\beta_1, \dots, \beta_{n-p})$$

if $(\alpha_1, \dots, \alpha_p, \beta_1, \dots, \beta_{n-p})$ is an even permutation of $\{1, \dots, n\}$. Also note that when $I = \{1, \dots, n\}$, we can identify $C^p(I, M)$ with the set of families $m(\alpha_1, \dots, \alpha_p)$ of elements of M where $\alpha_1 < \cdots < \alpha_p$.

Example 8.5.10. Let $M = k[T_1, \dots, T_n]$; the Koszul complex $K(\partial/\partial T, M)$ associated with the sequence $(\partial/\partial T_1, \dots, \partial/\partial T_n)$ is then identified with the de Rham complex of $k[X_1, \dots, X_n]$ over k. In fact, for an element $m \in C^p(I, M)$, where $I = \{1, \dots, n\}$, we can associate a differential form

$$\omega(m) = \sum_{\alpha_1 < \cdots < \alpha_p} m(\alpha_1, \dots, \alpha_p) dx_{\alpha_1} \wedge \cdots \wedge d_{x_{\alpha_p}}.$$

The assertion follows from the following computation

$$\begin{aligned} d\omega(m) &= \sum_{\alpha_1<\cdots<\alpha_p} \sum_{i=1}^{n} (\partial/\partial T_i)(m(\alpha_1,\ldots,\alpha_p)) dx_i \wedge dx_{\alpha_1} \wedge \cdots \wedge d_{x_{\alpha_p}} \\ &= \sum_{\alpha_1<\cdots<\alpha_{p+1}} \sum_{i=1}^{p+1} (-1)^{i+1} (\partial/\partial T_{\alpha_i})(m(\alpha_1,\ldots,\widehat{\alpha_i},\ldots,\alpha_{p+1})) dx_{\alpha_1} \wedge \cdots \wedge d_{x_{\alpha_{p+1}}} \\ &= \omega(\partial^p m). \end{aligned}$$

which shows ω is a complex isomorphism.

8.5.4 Koszul complexes and completely secant sequences

We now turn to the most important case, where E is just the free module A. Let $\alpha : A \to A$ be a linear form on A and $\alpha(1) = x \in A$. The complex $K(\alpha)$ is then of length 1 and given by

$$0 \longrightarrow A \xrightarrow{x_A} A \longrightarrow 0$$

Hence for any A-module M, the complexes $K^A_\bullet(\alpha, M)$ and $K^\bullet_A(\alpha, M)$ are just

$$0 \longrightarrow M \xrightarrow{x_M} M \longrightarrow 0$$

We then have isomorphisms

$$H_0(x, M) \xrightarrow{\sim} A/xA \otimes_A M \xleftarrow{\sim} H^1(x, M), \quad H_1(x, M) \xrightarrow{\sim} \mathrm{Hom}_A(A/xA, M) \xleftarrow{\sim} H^0(x, M).$$

Lemma 8.5.11. *Let K be an A-complex such that $K_i = 0$ for $i \neq 0, 1$, and M an A-complex.*

(a) If K is flat, for any integer $p \in \mathbb{N}$ we have an exact sequence

$$0 \longrightarrow H_0(K \otimes_A H_p(M)) \longrightarrow H_p(K \otimes_A M) \longrightarrow H_1(K \otimes_A H_{p-1}(M)) \longrightarrow 0$$

(b) If K is projective, for any integer $p \in \mathbb{N}$ we have an exact sequence

$$0 \to H^1(\mathrm{Hom}(K, H^{p-1}(M))) \to H_p(\mathrm{Hom}(K, M)) \to H^0(\mathrm{Hom}(K, H_{p-1}(M))) \to 0$$

Proof. We only prove (a), since (b) follows similarly. For each i, let $K_{(i)}$ be the complex $K_i[-i]$. We then have an exact sequence of complexes, which splits as sequences of A-modules:

$$0 \longrightarrow K_{(0)} \xrightarrow{\alpha} K \xrightarrow{\beta} K_{(1)} \longrightarrow 0$$

The sequence of complexes

$$0 \longrightarrow K_{(0)} \otimes_A M \xrightarrow{\alpha\otimes 1} K \otimes_A M \xrightarrow{\beta\otimes 1} K_{(1)} \otimes_A M \longrightarrow 0 \tag{5.4.1}$$

is then exact, with K being flat. By **??**, the homomorphisms

$$\gamma(K_{(0)}, M) : K_{(0)} \otimes_A H_p(M) \to H_p(K_{(0)} \otimes_A M) \tag{5.4.2}$$
$$\gamma(K_{(1)}, M) : K_{(1)} \otimes_A H_{p-1}(M) \to H_p(K_{(1)} \otimes_A M) \tag{5.4.3}$$

are bijective. We now calculate the connecting homomorphism $\partial(\alpha \otimes 1, \beta \otimes 1)$: by definition, it maps the class of a cycle $\sum a_i \otimes b_i$ to the class of $\sum da_i \otimes b_i$, which means

$$\partial(\alpha \otimes 1, \beta \otimes 1) \circ \gamma(K_{(1)}, M) = \gamma(K_{(0)}, M) \circ (d_K \otimes 1).$$

Combining with the isomorphisms (5.4.2) and (5.4.3), the long exact sequence associated with (5.4.1) is then of the form

$$K_1 \otimes H_p(M) \xrightarrow{d_K \otimes 1} K_0 \otimes H_p(M) \longrightarrow H_p(K \otimes M) \longrightarrow K_1 \otimes H_{p-1}(M) \xrightarrow{d_K \otimes 1} K_0 \otimes H_{p-1}(M)$$

which proves (a) by taking homology modules on both ends. □

Proposition 8.5.12. *For any complex M, we have an exact sequence*

$$0 \longrightarrow A/xA \otimes_A H_p(M) \longrightarrow H_p(x, M) \longrightarrow \mathrm{Hom}_A(A/xA, H_{p-1}(M)) \longrightarrow 0$$

Proof. This follows by applying Lemma 8.5.11(a) to the complex $K(\alpha)$, which is flat. □

Corollary 8.5.13. *For $H_p(x, M) = 0$, it is necessary and sufficient that the homothety with ratio x is surjective on $H_p(M)$ and injective on $H_{p-1}(M)$.*

Proof. By the exact sequence in Proposition 8.5.12, for $H_p(x, M) = 0$ it is necessary and sufficient that $A/xA \otimes_A H_p(M)$ and $\mathrm{Hom}_A(A/xA, H_{p-1}(M))$ are both zero. Since $A/xA \otimes_A H_p(M)$ is identified with $H_p(M)/xH_p(M)$ and $\mathrm{Hom}_A(A/xA, H_{p-1}(M))$ is identified with the elements of $H_{p-1}(M)$ annihilated by x, we see the corollary follows. □

Corollary 8.5.14. *Let $\boldsymbol{x} = (x_1, \ldots, x_n)$ be a sequence of elements of A, M an A-module, and $\tilde{\boldsymbol{x}} = (x_1, \ldots, x_{n-1})$. Then we have an exact sequence*

$$0 \longrightarrow A/x_nA \otimes_A H_p(\tilde{\boldsymbol{x}}, M) \longrightarrow H_p(\boldsymbol{x}, M) \longrightarrow \mathrm{Hom}_A(A/x_n, H_{p-1}(\tilde{\boldsymbol{x}}, M)) \longrightarrow 0$$

Proof. By noting that $K^A_\bullet(\boldsymbol{x}, M)$ is the tensor product of $K(x)$ and $K^A_\bullet(\tilde{\boldsymbol{x}}, M)$, this is just an application of Proposition 8.5.12. □

Corollary 8.5.15. *Let $\boldsymbol{x} = (x_1, \ldots, x_n)$ be a sequence of elements of A and M an A-module. For $H_i(\boldsymbol{x}, M) = 0$ for any $i > 0$, it is necessary and sufficient that the homothety with ratio x is bijective on $H_i(\tilde{\boldsymbol{x}}, M)$ for $i > 0$, and injective on $M/\tilde{\mathfrak{x}}M$, where $\tilde{\mathfrak{x}}$ is the ideal generated by $\tilde{\boldsymbol{x}}$.*

Let $\boldsymbol{x} = (x_i)_{i \in I}$ be a sequence of elements of A. We say $\boldsymbol{x}$ is **completely secant** for M if $H_i(\boldsymbol{x}, M) = 0$ for each $i > 0$. If the family $\boldsymbol{x}$ is finite, this also means $H^i(\boldsymbol{x}, M) = 0$ for $i < |I|$. Now Corollary 8.5.15 just gives a equivalent condition for a sequence $\boldsymbol{x} = (x_1, \ldots, x_n)$ to be completely sequence, and in particular, we get a special example:

Proposition 8.5.16. *Let $\boldsymbol{x} = (x_1, \dots, x_n)$ be a sequence of elements of A. If for each i the homothety with ratio x_i is injective on the A-module $M_i = M/(x_1M + \cdots + x_{i-1}M)$, then the sequence $\boldsymbol{x}$ is completely secant for M.*

Proof. We say a sequence $\boldsymbol{x} = (x_1, \dots, x_n)$ is M-regular if it satisfies the conditions given in the proposition. It is clear that if $\boldsymbol{x}$ is M-regular then so is $\tilde{\boldsymbol{x}} = (x_1, \dots, x_{n-1})$. So by induction using Corollary 8.5.15, we reduce to the case where $n = 1$, and this is trivial by Corollary 8.5.13. □

We note that the regular property of $\boldsymbol{x} = (x_1, \dots, x_n)$ depends on the order of the x_i: for example the sequence $(1, 0)$ is clearly M-regular, but $(0, 1)$ is not regular unless M is zero. On the other hand, the fact that a sequence is completely secant does not depend on the order of its terms.

Example 8.5.17. Let k be a ring, $A = k[X_1, \dots, X_n]$, and $\boldsymbol{x} = (X_1, \dots, X_n)$. Then $\boldsymbol{x}$ is A-regular and Proposition 8.5.16 restores the acyclicity at positive degrees of the complex $S_k(k^n) \otimes_k \bigwedge_k(k^n)$ (Proposition 8.5.9). Similarly, the sequence $\boldsymbol{x} = (X_1, \dots, X_n)$ is regular in the ring $k[\![X_1, \dots, X_n]\!]$.

Proposition 8.5.18. *Let A be a ring and $\boldsymbol{x} = (x_1, \dots, x_n)$ a sequence of elements of A. Let $\mathfrak{x}$ be the ideal generated by $\boldsymbol{x}$ in A.*

(a) If $\mathfrak{x} = A$ then the family $\boldsymbol{x}$ is completely secant for M.

(b) Let $(a_{ij}) \in \mathrm{GL}_n(A)$ and put $y_i = \sum_j a_{ij}x_j$. If the sequence $\boldsymbol{x}$ is completely secant for M, then $\boldsymbol{y} = (y_1, \dots, y_n)$ is also completely secant.

(c) If $k_1, \dots, k_n$ are positive integers, the sequence $(x_1^{k_1}, \dots, x_n^{k_n})$ is completely secant for M if and only if $\boldsymbol{x}$ is completely secant for M.

(d) Let N be a flat A-module. If the family $\boldsymbol{x}$ is completely secant for M, so it is for $M \otimes_A N$.

(e) Let $0 \to L \to M \to N \to 0$ be an exact sequence of A-modules. If the family $\boldsymbol{x}$ is completely secant for L and N, so it is for M.

Proof. The first assertion is trivial. Let $(a_{ij}) \in \mathrm{GL}_n(A)$ be as in (b) and $f : A^n \to A^n$ be the isomorphism defined by $(a_{ij})^t$. Then the map $1_M \otimes \bigwedge(f)$ is an isomorphism from $K_\bullet(\boldsymbol{y}, M)$ to $K_\bullet(\boldsymbol{x}, M)$, whence (b) follows.

To prove (c), it suffices to show that if $k \geq 1$ is an integer, the sequence $(x_1, \dots, x_{n-1}, x_n^k)$ is completely secant for M if and only if $\boldsymbol{x}$ is. Let $\tilde{\boldsymbol{x}} = (x_1, \dots, x_{n-1})$, then by Corollary 8.5.15, the first condition (resp. the second) means the homothety with ratio x_n^k (resp. x_n) is bijective on $H_i(\tilde{\boldsymbol{x}}, M)$ for $i > 0$ and injective on $M/\tilde{\mathfrak{x}}M$. These two conditions are clearly equivalent, so (c) follows.

Let N be a flat A-module. Then the complex $K_\bullet(\boldsymbol{x}, M \otimes_A N)$ is isomorphic to $K_\bullet(\boldsymbol{x}, M) \otimes_A N$, hence $H_\bullet(\boldsymbol{x}, M \otimes_A N) = H_\bullet(\boldsymbol{x}, M)$. This proves (d), and assertion (e) follows from the long exact sequence induced from the given short exact sequence. □

Remark 8.5.2. Analogue results for regular sequences of Proposition 8.5.18(c), (d), and (e) also holds.

Remark 8.5.3. If the family $\boldsymbol{x}$ is completely secant for A, the complex $K_\bullet(\boldsymbol{x}, A)$ then defines a free resolution for the A-module $A/\mathfrak{x}$. Then for $i \geq 0$ we have the following isomorphisms

$$\mathrm{Ext}_A^{n-i}(A/\mathfrak{x}, M) \longrightarrow H^{n-i}(\boldsymbol{x}, M) \longrightarrow H_i(\boldsymbol{x}, M) \longrightarrow \mathrm{Tor}_i^A(A/\mathfrak{x}, M) \tag{5.4.4}$$

Example 8.5.19. We say the sequence $\boldsymbol{x} = (x_1, \ldots, x_n)$ is ***M*-coregular** if the homothety $(x_i)_M$ is surjective on the module

$$\ker(x_1)_M \cap \cdots \cap \ker(x_{i-1})_M$$

for each i. Similar to Proposition 8.5.16, we can show that $H_i(\boldsymbol{x}, M) = 0$ for $i < n$ if $\boldsymbol{x}$ is M-coregular.

Take for example $A = k[D_1, \ldots, D_n]$, where k is a $\mathbb{Q}$-algebra, and $M = k[T_1, \ldots, T_n]$, where D_i acts on M by $D_i P = \partial P/\partial T_i$. We then verify that the sequence $(D_1, \ldots, D_n)$ is M-coregular. Combine this with Example 8.5.10, we deduce that the de Rham complex of $k[T_1, \ldots, T_n]$ over k is acyclic at positive degrees.

Let A be a ring, M an A-module, $\mathfrak{x}$ an ideal of A. We recall that the $\mathfrak{x}$-adic topology on M is the topology compatible with the module structure on M and such that $\mathfrak{x}^r M$ form a fundamental neighborhood of 0 in M. Suppose now $\mathfrak{x}$ is generated by a sequence $\boldsymbol{x} = (x_1, \ldots, x_n)$ of elements of A. Consider the graded A-module $\bigoplus_r \mathfrak{x}^r M$ and the graded A-homomorphism of degree 0:

$$a_M^{\mathfrak{x}} : A[X_1, \ldots, X_n] \otimes_A M \to \bigoplus_r \mathfrak{x}^r M$$

such that $a_M^{\mathfrak{x}}(P \otimes m) = P(x_1, \ldots, x_n)m$ if P is a homogeneous polynomial and $m \in M$. Let $\mathfrak{d}$ be the ideal of $A[X_1, \ldots, x_n]$ generated by the elements $(x_i X_j - x_j X_i)$ for $1 \leq i < j \leq n$. Then $P(x_1, \ldots, x_n) = 0$ if $P \in \mathfrak{d}$, so $a_M^{\mathfrak{x}}$ factors into a graded A-homomorphism of degree 0:

$$\alpha_M^{\mathfrak{x}} : (A[X_1, \ldots, X_n]/\mathfrak{d}) \otimes_A M \to \bigoplus_r \mathfrak{x}^r M.$$

By tensoring with $A/\mathfrak{x}$, we deduce from $\alpha_M^{\mathfrak{x}}$ another graded A-homomorphism of degree 0:

$$\beta_M^{\mathfrak{x}} : (A/\mathfrak{x})[X_1, \ldots, X_n] \otimes_A M \to \mathrm{gr}_{\mathfrak{x}}(M).$$

For each i, let M_i be the quotient A-module $M/(x_1 M + \cdots + x_{i-1} M)$.

Lemma 8.5.20. *Let A_0 be the ring $\mathbb{Z}[T_1, \ldots, T_n]$ and let $\rho : A_0[X_1, \ldots, X_n] \to A_0[U]$ be the homomorphism of A_0-algebras such that $\rho(X_i) = T_i U$. Then the kernel of ρ is the ideal $\mathfrak{d}_0$ of $A_0[X_1, \ldots, X_n]$ generated by the elements $(T_i X_j - T_j X_i)$ for $1 \leq i < j \leq n$. If $\mathfrak{t}$ is the ideal generated by $(T_1, \ldots, T_n)$, ρ induces an isomorphism*

$$\bar{\rho} : A_0[X_1, \ldots, X_n]/\mathfrak{d}_0 \to \bigoplus_n \mathfrak{t}^n.$$

Proof. □

Theorem 8.5.21. *Consider the following conditions:*

(i) The sequence $\boldsymbol{x}$ is M-regular.

(ii) The sequence $\boldsymbol{x}$ is completely secant for M.

(iii) $H_1(\boldsymbol{x}, M) = 0$.

(iv) The homomorphism $\alpha_M^{\mathfrak{x}} : (A[X_1, \dots, X_n]/\mathfrak{d}) \otimes_A M \to \bigoplus_r \mathfrak{x}^r M$ *is bijective.*

(v) The homomorphism $\beta_M^{\mathfrak{x}} : (A/\mathfrak{x})[X_1, \dots, X_n] \otimes_A M \to \mathrm{gr}_{\mathfrak{x}}(M)$ *is bijective.*

We have (i)⇒(ii)⇒(iii)⇔(iv)⇒(v). If for each i the A-module M_i is separated for the $\mathfrak{x}$-adic topology, the above conditions are equivalent.

Proof. The implication (i)⇒(ii) is already proved, and (ii)⇒(iii) is clear; so is (iv)⇒(v), since $\beta_M^{\mathfrak{x}}$ is identified with $\alpha_M^{\mathfrak{x}} \otimes 1_{A/\mathfrak{x}}$. Also, we note that the homomorphisms $\alpha_M^{\mathfrak{x}}$ and $\beta_M^{\mathfrak{x}}$ are surjective.

To prove (iv)⇒(iii), consider the homomorphism $(\alpha_M^{\mathfrak{x}})_1$ induced on the component of degree 1 by $\alpha_M^{\mathfrak{x}}$. Let E be the graded A-module $A[X_1, \dots, X_n]$; the A-module E_1 is free with basis $X_1, \dots, X_n$, and $\mathfrak{d}_1$ is the sub-A-module of E_1 generated by the elements $x_i X_j - x_j X_i$ for $1 \leq i < j \leq n$. Therefore $((E/\mathfrak{d}) \otimes_A M)_1$ is identified with $K_1(\boldsymbol{x}, M)/B_1(K_\bullet(\boldsymbol{x}, M))$, and the homomorphism $(\alpha_M^{\mathfrak{x}})_1$ is identified with the map from $K_1(\boldsymbol{x}, M)/B_1(K_\bullet(\boldsymbol{x}, M))$ to $B_0(K_\bullet(\boldsymbol{x}, M))$ induced by d_1. Thus the condition that $H_1(\boldsymbol{x}, M) = 0$ is equivalent to the injectivity of $(\alpha_M^{\mathfrak{x}})_1$, which proves the implication (iv)⇒(iii).

To prove that (iii) implies (iv), we consider the ring $A_0 = \mathbb{Z}[T_1, \dots, T_n]$ and let $\mathfrak{t}$ be the ideal of A_0 generated by $T_1, \dots, T_n$. Endow M the A_0-module structure such that $T_i m = x_i m$ for $m \in M$. Then the homology group $H_i(\boldsymbol{x}, M)$ is identified with $H_i(\boldsymbol{T}, M)$, where $\boldsymbol{T} = (T_1, \dots, T_n)$. Since $\boldsymbol{T}$ is regular for A_0, it follows from the implication (i)⇒(ii) that the complex $K_\bullet(\boldsymbol{T}, A_0)$ is a free resolution for the A_0-module $A_0/\mathfrak{t}$, which is identified with $\mathbb{Z}$ with the A_0-structure defined by $T_i \mathbb{Z} = 0$ for each i. Therefore, the condition (iii) is equivalent to $\mathrm{Tor}_1^{A_0}(M, \mathbb{Z}) = 0$.

We first show that (iii) implies $\mathrm{Tor}_1^{A_0}(M, A_0/\mathfrak{t}^r) = 0$ for $r \geq 1$. This is true for $r = 1$ as we have seen. In the general case, consider the exact sequence

$$0 \longrightarrow \mathfrak{t}^r/\mathfrak{t}^{r+1} \xrightarrow{\iota_r} A_0/\mathfrak{t}^{r+1} \xrightarrow{\pi_r} A_0/\mathfrak{t}^r \longrightarrow 0 \tag{5.4.5}$$

The A_0-module $\mathfrak{t}^r/\mathfrak{t}^{r+1}$ is isomorphic to a finite product of modules isomomorphic to $\mathbb{Z}$, so $\mathrm{Tor}_1^{A_0}(M, \mathfrak{t}^r/\mathfrak{t}^{r+1}) = 0$. We then deduce, by induction on r, that $\mathrm{Tor}_1^{A_0}(M, A_0/\mathfrak{t}^r) = 0$ for each $r \geq 1$. The sequence (5.4.5) then provides, by tensoring with M, an exact sequence

$$0 \longrightarrow (\mathfrak{t}^r/\mathfrak{t}^{r+1}) \otimes_{A_0} M \longrightarrow M/\mathfrak{t}^{r+1}M \longrightarrow M/\mathfrak{t}^r M \longrightarrow 0 \tag{5.4.6}$$

hence an isomorphism $(\mathfrak{t}^r/\mathfrak{t}^{r+1}) \otimes_{A_0} M$ to $\mathfrak{x}^r M/\mathfrak{x}^{r+1}M$. By considering the exact sequence

$$0 \longrightarrow \mathfrak{t}^{r+1} \longrightarrow \mathfrak{t}^r \longrightarrow \mathfrak{t}^r/\mathfrak{t}^{r+1} \longrightarrow 0$$

and induction on r, we then conclude that the map $m_r : \mathfrak{t}^r \otimes_{A_0} M \to \mathfrak{x}^r M$, induced by the operations of A_0 on M, is an isomorphism. Now consider the following commutative diagram:

$$\begin{tikzcd}
(A_0[X_1, \dots, X_n]/\mathfrak{d}_0) \otimes_{A_0} M \arrow[r, "\tilde{\rho} \otimes 1_M"] \arrow[d, "\eta"] & \bigoplus_r (\mathfrak{t}^r \otimes_{A_0} M) \arrow[d, "\oplus m_r"] \\
(A[X_1, \dots, X_n]/\mathfrak{d}) \otimes_A M \arrow[r, "\alpha_M^{\mathfrak{x}}"] & \bigoplus_r \mathfrak{x}^r M
\end{tikzcd}$$

where η is the canonical isomorphism of extension of scalars:

$$(A_0[X_1,\dots,X_n]/\mathfrak{d}_0)\otimes_{A_0} M \cong (A_0[X_1,\dots,X_n]/\mathfrak{d}_0)\otimes_{A_0} A\otimes_A M \cong (A[X_1,\dots,X_n]/\mathfrak{d})\otimes_A M.$$

By Lemma 8.5.20, we then see condition (iv) follows.

Finally, consider the follwoing exact sequence induced from (5.4.5):

$$\begin{tikzcd}
\mathrm{Tor}_1^{A_0}(A_0/\mathfrak{t}^{r+1},M) \arrow[r, "\mathrm{Tor}(\iota_r,1_M)"] & \mathrm{Tor}_1^{A_0}(A_0/\mathfrak{t}^{r},M) \arrow[r, "\mathrm{Tor}(\pi_r,1_M)"] & (\mathfrak{t}^r/\mathfrak{t}^{r+1})\otimes_{A_0} M \arrow[dll, "\iota_r\otimes 1_M"'] \\
& (A_0/\mathfrak{t}^r)\otimes_{A_0} M \arrow[r, "\pi_r\otimes 1_M"] & (A_0/\mathfrak{t}^{r+1})\otimes_{A_0} M \arrow[r] & 0
\end{tikzcd} \tag{5.4.7}$$

The kernel of $\pi_r\otimes 1_M$ is identified with $\mathfrak{x}^r M/\mathfrak{x}^{r+1}M$ and the A_0-module $\mathfrak{t}^r/\mathfrak{t}^{r+1}$ is identified with the homogeneous component of degree r of A_0. Therefore, the homomorphism $(\mathfrak{t}^r/\mathfrak{t}^{r+1})\otimes_{A_0} M \to \mathfrak{x}^r M/\mathfrak{x}^{r+1}M$ induced by $\iota_r\otimes 1_M$ is identified with the homogeneous component of degree r of $\beta_M^{\mathfrak{x}}$ and we get the following exact sequence from (5.4.7):

$$\mathrm{Tor}_1^{A_0}(A_0/\mathfrak{t}^{r+1},M) \xrightarrow{\mathrm{Tor}_1^{A_0}(\iota_r,1_M)} \mathrm{Tor}_1^{A_0}(A_0/\mathfrak{t}^{r},M) \xrightarrow{\mathrm{Tor}_1^{A_0}(\pi_r,1_M)} (\mathfrak{t}^r/\mathfrak{t}^{r+1})\otimes_{A_0} M \xrightarrow{(\beta_M^{\mathfrak{x}})_r} \mathfrak{x}^r M/\mathfrak{x}^{r+1}M$$

The condition (v) is then equivalent to the following condition:

(v′) the homomorphlsm $\mathrm{Tor}_1^{A_0}(\pi_r,1_M) : \mathrm{Tor}_1^{A_0}(A_0/\mathfrak{t}^{r+1},M) \to \mathrm{Tor}_1^{A_0}(A_0/\mathfrak{t}^{r},M)$ is surjective for each $r\geq 1$.

We are now left to prove (v)⇒(i) if the modules M_i are separated for the $\mathfrak{x}$-adic topology. Let $\overline{M} = M/x_1M$. By definition, the sequence $\boldsymbol{x}$ is regular for M if and only if $(x_1)_M$ is injective and the sequence $\tilde{\boldsymbol{x}} = (x_2,\dots,x_n)$ is regular for $\overline{M}$. Reasoning by induction on n, it suffices to prove that, if M is separated for the $\mathfrak{x}$-adic topology and if $\beta_M^{\mathfrak{x}}$ is bijective, then $(x_1)_M$ is injective and $\beta_M^{\tilde{\boldsymbol{x}}}$ is bijective. Now the bijectivity of $\beta_M^{\boldsymbol{x}}$ implies in particular that the homothety with ratio x_1 is injective on $\mathrm{gr}_{\mathfrak{x}}(M)$ (since it is mapped by $\beta_M^{\boldsymbol{x}}$ to the homothety of X_1 on $(A/\mathfrak{x})[X_1,\dots,X_n]\otimes_A M$), hence $(x_1)_M$ is injective since the $\mathfrak{x}$-topology on M is separated (Corollary 11.3.30).

We are then left to prove that if $(x_1)_M$ is injective and M verifies the condition (v′), then $\overline{M}$ verifies the condition (v′) for $\tilde{\boldsymbol{x}}$. By hypothesis we have an exact sequence

$$0 \longrightarrow M \xrightarrow{(x_1)_M} M \longrightarrow \overline{M} \longrightarrow 0$$

Put $\overline{A}_0 = A_0/T_1A_0$, $\overline{\mathfrak{t}} = \mathfrak{t}\overline{A}_0$. Let $E\to M$ be a free resolution of the A_0-module M; since the homothety with ratio T_1 is injective on A_0, it is injective on E, and we have an exact sequence of complexes:

$$0 \longrightarrow E \xrightarrow{(T_1)_E} E \longrightarrow \overline{E} \longrightarrow 0$$

where $\overline{E} = E/T_1E$, and a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & E \arrow[r, "(T_1)_E"] \arrow[d, "\gamma"] & E \arrow[r] \arrow[d, "\gamma"] & \overline{E} \arrow[r] \arrow[d, "\bar{\gamma}"] & 0 \\
0 \arrow[r] & M \arrow[r, "(x_1)_M"] & M \arrow[r] & \overline{M} \arrow[r] & 0
\end{tikzcd}$$

Since γ is an quasi-isomorphism, we conclude from the induced long exact sequence that $\bar{\gamma} : \bar{E} \to \overline{M}$ is a free resolution for the $\bar{A}_0$-module $\overline{M}$. For any $\bar{A}_0$-module P, we have a canonical isomorphism $P \otimes_{A_0} E \cong P \otimes_{\bar{A}_0} \bar{E}$, whence by passing to homology an isomorphism

$$\varphi_P : \mathrm{Tor}_1^{A_0}(P, M) \to \mathrm{Tor}_1^{\bar{A}_0}(P, \overline{M}).$$

which is functorial in the sense that if $f : P \to Q$ be an $\bar{A}_0$-homomorphism, then

$$\varphi_Q \circ \mathrm{Tor}_1^{A_0}(f, 1_M) = \mathrm{Tor}_1^{\bar{A}_0}(f, 1_M) \circ \varphi_P.$$

This being so, suppose the condition (v′) holds for M. Let $r \geq 1$ be an integer; we have a commutative diagram with exact rows:

$$\begin{tikzcd}
0 \arrow[r] & A_0/\mathfrak{t}^r \arrow[r, "T_1"] \arrow[d, "\pi_{r-1}"] & A_0/\mathfrak{t}^{r+1} \arrow[r] \arrow[d, "\pi_r"] & \bar{A}_0/\bar{\mathfrak{t}}^{r+1} \arrow[r] \arrow[d, "\bar{\pi}_r"] & 0 \\
0 \arrow[r] & A_0/\mathfrak{t}^r \arrow[r, "T_1"] & A_0/\mathfrak{t}^{r+1} \arrow[r] & \bar{A}_0/\bar{\mathfrak{t}}^{r+1} \arrow[r] & 0
\end{tikzcd}$$

which induces the following commutative diagram

$$\begin{tikzcd}
\mathrm{Tor}_1^{A_0}(A_0/\mathfrak{t}^{r+1}, M) \arrow[r] \arrow[d, "\mathrm{Tor}_1(\pi_r,1)"] & \mathrm{Tor}_1^{A_0}(\bar{A}_0/\bar{\mathfrak{t}}^{r+1}, M) \arrow[r] \arrow[d, "\mathrm{Tor}_1(\bar{\pi}_r,1)"] & M/\mathfrak{x}^r M \arrow[r, "x_1"] \arrow[d] & M/\mathfrak{x}^{r+1} M \arrow[d] \\
\mathrm{Tor}_1^{A_0}(A_0/\mathfrak{t}^r, M) \arrow[r] & \mathrm{Tor}_1^{A_0}(\bar{A}_0/\bar{\mathfrak{t}}^r, M) \arrow[r] & M/\mathfrak{x}^{r-1} M \arrow[r, "x_1"] & M/\mathfrak{x}^r M
\end{tikzcd} \tag{5.4.8}$$

with exact rows. Now the multiplication by x_1 defines an injection from $M/\mathfrak{x}^r M$ to $M/\mathfrak{x}^{r+1} M$: this follows immediately, by induction on r, from the exact sequence

$$0 \longrightarrow \mathfrak{x}^{r-1} M/\mathfrak{x}^r M \longrightarrow M/\mathfrak{x}^r M \longrightarrow M/\mathfrak{x}^{r-1} M \longrightarrow 0$$

and the injectivity of the homothety with ratio x_1 on $\mathrm{gr}_{\mathfrak{x}}(M)$. Therefore, the first horizontal maps in both rows of (5.4.8) are surjective, and condition (v′) then implies that the homomorphism $\mathrm{Tor}_1^{\bar{A}_0}(\bar{\pi}_r, 1_M)$ is surjective for $r \geq 1$. By composing with the isomorphisms $(\varphi_{\bar{A}_0/\bar{\mathfrak{t}}^{r+1}})^{-1}$ and $\varphi_{\bar{A}_0/\bar{\mathfrak{t}}^r}$, we then deduce that the homomorphism

$$\mathrm{Tor}_1^{\bar{A}_0}(\bar{\pi}_r, 1_M) : \mathrm{Tor}_1^{\bar{A}_0}(\bar{A}_0/\bar{\mathfrak{t}}^{r+1}, M) \to \mathrm{Tor}_1^{\bar{A}_0}(\bar{A}_0/\bar{\mathfrak{t}}^r, M)$$

is surjective for $r \geq 1$, whence the condition (v′) for $\overline{M}$. This completes the proof. □

Corollary 8.5.22. *If A is a Zariski ring and $\mathfrak{x}$ is a defining ideal of A. Then for any finitely generated A-module M, the conditions in Theorem 8.5.21 are equivalent.*

Proof. By Proposition 11.4.25 the modules M_i are separated for the $\mathfrak{x}$-adic topology. □

Corollary 8.5.23. *Suppose that A is a graded ring of positive degrees, M a graded A-module bounded below, and the x_i are homogeneous elements of positive degrees. Then the conditions in Theorem 8.5.21 are equivalent.*

Proof. The $\mathfrak{x}$-adic topology is in fact separated for any graded A-module N bounded below, since if $N_n = 0$ for $n < n_0$ we have $\mathfrak{x}^\nu N \subseteq \sum_{i \geq n_0+\nu} N_i$ for any $\nu \geq 0$. □

Corollary 8.5.24. *Suppose that the modules M_i are separated for the $\mathfrak{x}$-adic topology; let $1 \leq p \leq n$ be an integer. For the sequence $\boldsymbol{x}$ to be completely secant for M, it is necessary and sufficient that the sequence $(x_1, \dots, x_p)$ is completely secant for M and the sequence $(x_{p+1}, \dots, x_n)$ is completely secant for $M/(x_1M + \cdots + x_pM)$.*

Remark 8.5.4. Let $\boldsymbol{x} = (x_1, \dots, x_n)$ be a sequence of elements of A such that $H_1(\boldsymbol{x}, A) = 0$. Then from the construction of $K_\bullet(\alpha)$, the kernel of the surjective homomorphism $\alpha : A^n \to \mathfrak{x}$ such that $\alpha(\sum_i a_i e_i) = \sum_i a_i x_i$ is the image of $\bigwedge^2(A^n)$ under d_α, which by (5.1.1) is generated by the elements $x_j e_i - x_i e_j$. Therefore, the A-algebra $A[X_1, \dots, X_n]/\mathfrak{d}$ is isomorphic to the symmetric algebra $S_A(\mathfrak{x})$ (**??**). It then follows from Theorem 8.5.21 that the algebra homomorphism $S_A(\mathfrak{x}) \to \bigoplus_n \mathfrak{x}^n$ induced from the canonical injection of $\mathfrak{x}$ to $\bigoplus_n \mathfrak{x}^n$ is an isomorphism. The same holds for the homomorphism $S_A(\mathfrak{x}/\mathfrak{x}^2) \to \mathrm{gr}_{\mathfrak{x}}(A)$.

8.5.5 Extension class associated with a regular sequence

Let A be a ring, M an A-module and $\boldsymbol{x} = (x_1, \dots, x_n)$ a sequence of elements of A. Let $M_i = M/(x_1M + \cdots + x_{i-1}M)$ for each $i = 0, 1, \dots, n+1$ (we set $M_0 = M$), and let

$$\bar{x}_i : M_{i-1} \to M_i, \quad i = 1, \dots, n$$

be the A-homomorphism composing the homothety with ratio x_i on M_{i-1} with the canonical projection from M_{i-1} to M_i. Finally, let $\pi : M_n \to M/\mathfrak{x}M$ be the canonical projection. Suppose that $\boldsymbol{x}$ is M-regular, then the sequence

$$0 \longrightarrow M \xrightarrow{\bar{x}_1} M_1 \xrightarrow{\bar{x}_2} \cdots \xrightarrow{\bar{x}_n} M_n \xrightarrow{\pi} M/\mathfrak{x}M \longrightarrow 0 \tag{5.5.1}$$

is exact. The element $\theta_{\boldsymbol{x}} \in \mathrm{Ext}^n_A(M/xM, M)$ associated with this sequence is then called the **extension class associated with the M-regular sequence $\boldsymbol{x}$**.

For each integer $1 \leq i \leq n$, the sequence (5.5.1) can be decomposed into the following two exact sequences:

$$0 \longrightarrow M \xrightarrow{\bar{x}_1} M_1 \xrightarrow{\bar{x}_2} \cdots \xrightarrow{\bar{x}_i} M_i \longrightarrow M_{i+1} \longrightarrow 0 \tag{5.5.2}$$

$$0 \longrightarrow M_{i+1} \xrightarrow{\bar{x}_{i+1}} M_{i+1} \xrightarrow{\bar{x}_{i+2}} \cdots \xrightarrow{\bar{x}_n} M_n \xrightarrow{\pi} M/\mathfrak{x}M \longrightarrow 0 \tag{5.5.3}$$

which are none other than the exact sequences associated with the sequence $(x_1, \dots, x_i)$ which is regular for M and that with $(x_{i+1}, \dots, x_n)$ which is regular for M_{i+1}.

Note that the the extension classes associated with (5.5.2) and (5.5.3) are

$$\theta_{(x_1,\dots,x_i)} \in \mathrm{Ext}^i_A(M_{i+1}, M), \quad \theta_{(x_{i+1},\dots,x_n)} \in \mathrm{Ext}^{n-i}_A(M/\mathfrak{x}M, M_{i+1})$$

and we have by **??** that

$$\theta_{(x_1,\dots,x_n)} = \theta_{(x_1,\dots,x_i)} \circ \theta_{(x_{i+1},\dots,x_n)}.$$

Moreover, by Proposition 8.5.16 the Koszul complex $K^\bullet(\boldsymbol{x}, M)$ is acyclic at degrees $\neq n$, so we have an exact sequence

$$0 \longrightarrow M \xrightarrow{\partial^0} K^1(\boldsymbol{x}, M) \xrightarrow{\partial^1} \cdots \longrightarrow K^n(\boldsymbol{x}, M) \xrightarrow{\varepsilon} M/\mathfrak{x}M \longrightarrow 0 \tag{5.5.4}$$

where we identify $K^0(\boldsymbol{x}, M)$ with M and the map ε sends each element $m \in K^n(\boldsymbol{x}, M)$ to the class in $M/\mathfrak{x}M$ of $m(1, 2, \ldots, n) \in M$.

Proposition 8.5.25. *Let $\boldsymbol{x}$ be a M-regular sequence. Then the element of $\mathrm{Ext}^n_A(M/\mathfrak{x}M, M)$ associated with the sequence (5.5.4) is $(-1)^{n(n+1)/2}\theta_{\boldsymbol{x}}$.*

Proof. Recall that $K^i(\boldsymbol{x}, M)$ can be viewed as the set $C^i(I, M)$ where $I = \{1, \ldots, n\}$ and the differential ∂^i is given by (5.3.1). For each $i = 0, \ldots, n$, define an A-linear map

$$\alpha^i : K^i(\boldsymbol{x}, M) \to M_i, \quad m \mapsto m(1, 2, \ldots, i).$$

It is then clear that α^0 is the identity map on M and $\pi \circ \alpha^n = \varepsilon$. Moreover, $\alpha^{i+1} \circ \partial^i(m)$ is the image in M_{i+1} of the element

$$\sum_{j=1}^{i+1} (-1)^{j+1} x_j m(1, 2, \ldots, \widehat{j}, \ldots, i+1).$$

Since x_j annihilates M_{i+1} for $j = 1, \ldots, i$, the element $\alpha^{i+1} \circ \partial^i(m)$ then equals to the image of $(-1)^i x_{i+1} m(1, 2, \ldots, i)$ in M_{i+1} and we therefore have

$$\alpha^{i+1} \circ \partial^i = (-1)^i \bar{x}_{i+1} \circ \alpha^i.$$

By **??** and **??**, the element in $\mathrm{Ext}^n_A(M/\mathfrak{x}M, M)$ is equal to $\prod_{i=1}^n (-1)^i \theta_{\boldsymbol{x}}$, whence our claim. □

Corollary 8.5.26. *suppose further that the modules M_i are separated for the $\mathfrak{x}$-adic topology, and let $(a_{ij}) \in \mathrm{GL}_n(A)$. Put*

$$y_i = \sum_j a_{ij} x_j$$

and $\boldsymbol{y} = (y_1, \ldots, y_n)$. Then the sequence $\boldsymbol{y}$ is regular for M and we have $\theta_{\boldsymbol{y}} = \det(a_{ij})^{-1}\theta_{\boldsymbol{x}}$.

Proof. In fact, the sequence $\boldsymbol{y}$ is regular for M by Proposition 8.5.18 and Theorem 8.5.21; the second assertion then follows from Proposition 8.5.25 and **??**. □

Proposition 8.5.27. *Let $\boldsymbol{x}$ be a regular sequence for M and N is an A-module annihilated by $\boldsymbol{x}$. Then $\mathrm{Ext}^i_A(N, M) = 0$ for $i < n$ and the map $\alpha \mapsto \theta_{\boldsymbol{x}} \circ \alpha$ from $\mathrm{Hom}_A(N, M/\mathfrak{x}M)$ to $\mathrm{Ext}^n_A(N, M)$ is bijective.*

Proof. We prove by induction that the homomorphism

$$\psi^i : \mathrm{Ext}^{i-n}_A(N, M/\mathfrak{x}M) \to \mathrm{Ext}^i_A(N, M), \quad \alpha \mapsto \theta_{\boldsymbol{x}} \circ \alpha$$

is bijective for $i \leq n$. The assertion is trivial for $n = 0$, so suppose that $n \geq 1$ and put $M_1 = M/x_1M$, $\tilde{\boldsymbol{x}} = (x_2, \ldots, x_n)$, so that $\tilde{\boldsymbol{x}}$ is M_1-regular. By the induction hypothesis, the

homomorphism

$$\bar{\psi}^{i-1} : \mathrm{Ext}_A^{i-n}(N, M/\mathfrak{x}M) \to \mathrm{Ext}_A^{i-1}(N, M_1), \quad \alpha \mapsto \theta_{\tilde{\boldsymbol{x}}} \circ \alpha$$

is bijective for $i \leq n$. Now consider the exact sequence

$$0 \longrightarrow M \xrightarrow{(x_1)_M} M \longrightarrow M_1 \longrightarrow 0$$

where the associated connecting homomorphism is

$$\varphi^i : \mathrm{Ext}_A^{i-1}(N, M_1) \to \mathrm{Ext}_A^i(N, A), \quad \beta \mapsto \theta_{x_1} \circ \beta.$$

Since $\mathrm{Ext}^i(1_N, (x_1)_M) = \mathrm{Ext}^i((x_1)_N, 1_M) = 0$, we deduce the exact sequences

$$0 \longrightarrow \mathrm{Ext}_A^{i-1}(N, M) \longrightarrow \mathrm{Ext}_A^{i-1}(N, M_1) \xrightarrow{\varphi^i} \mathrm{Ext}_A^i(N, M) \longrightarrow 0$$

Now by induction hypothesis, $\mathrm{Ext}_A^{i-1}(N, M_1) = 0$ for $i < n$, so $\mathrm{Ext}_A^i(N, M) = 0$ for $i < n$, which implies φ^i is bijective for $i \leq n$. Since for $\alpha \in \mathrm{Ext}_A^{i-n}(N, M/\mathfrak{x}M)$ we have

$$\psi^i(\alpha) = \theta_{\boldsymbol{x}} \circ \alpha = \theta_{x_1} \circ \theta_{\tilde{\boldsymbol{x}}} \circ \alpha = \varphi^i \circ \bar{\psi}^{i-1}(\alpha) \tag{5.5.5}$$

the map ψ^i is therefore bijective for $i \leq n$. □

Chapter 9

Field Theories

9.1 Field extensions

We first deal with several basic notions in field theory, mostly inspired by easy linear algebra considerations. The keywords here are finite, simple, finitely generated, algebraic.

9.1.1 Basic definitions of field extensions

The study of fields is (of course) the study of the category **Fld** of fields, with ring homomorphisms as morphisms. The task is to understand what fields are and above all what they are in relation to one another. The place to start is a reminder from elementary ring theory: every ring homomorphisms from a field to a nonzero ring is injective. Indeed, the kernel of a ring homomorphism to a nonzero ring is a proper ideal (because a homomorphism maps 1 to 1 by definition and $1 \neq 0$ in nonzero rings), and the only proper ideal in a field is (0). In particular, every ring homomorphism of fields is injective (fields are nonzero rings by definition!); every morphism in **Fld** is a monomorphism.

The coarsest invariant of a field K is its **characteristic**. We have a unique ring homomorphisms $\iota : \mathbb{Z} \to K$ (recall that $\mathbb{Z}$ is initial in **Ring**: 1 must go to 1 by definition of homomorphism, and this fixes the value of $\iota(n)$ for all $n \in \mathbb{Z}$); the characteristic of K, $\mathrm{char}(K)$, is defined to be the nonnegative generator of the ideal $\ker \iota$; that is, $\mathrm{char}(K) = 0$ if ι is injective, and $\mathrm{char}(K) = p > 0$ if $\ker \iota = (p) \neq (0)$. Since $\iota(\mathbb{Z})$ must be an integral domain, (p) is a prime ideal in $\mathbb{Z}$. Therefore, the characteristic of a field is either 0 or a prime number.

Definition 9.1.1. *A field E containing a field K is called an **extension field of K** (or simply an **extension** of K, and we speak of an extension E/K). The dimension of E as an K-vector space is called the **degree of E over K**, and is denote by $[E : K]$. We say that E is **finite** over K when it has finite degree over K.*

Example 9.1.2 (Example of field extensions).

(a) The field of complex numbers $\mathbb{C}$ has degree 2 over $\mathbb{R}$, so $\mathbb{R} \subseteq \mathbb{C}$ is a extension of degree 2.

(b) The field of real numbers $\mathbb{R}$ has infinite degree over $\mathbb{Q}$: the field $\mathbb{Q}$ is countable, and so every finite-dimensional $\mathbb{Q}$-vector space is also countable, but a famous argument of Cantor shows that $\mathbb{R}$ is not countable.

(c) The field of Gaussian numbers

$$\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$$

has degree 2 over $\mathbb{Q}$.

(d) The field $K(X)$ has infinite degree over K; in fact, even its subspace $K[X]$ has infinite dimension over K.

Let K be a subfield of a field E, and let S be a subset of E. The intersection of all the subfields of E containing K and S is obviously the smallest subfield of E containing both K and S. We call it the **subfield of E generated by K and S** (or **generated over K by S**), and we denote it $K(S)$. It is the field of fractions of the ring $K[S]$ in E because this is a subfield of E containing K and S and contained in every other such field. When $S = \{\alpha_1, \dots, \alpha_n\}$, we write $K(\alpha_1, \dots, \alpha_n)$ for $K(S)$. Thus, $F[\alpha_1, \dots, \alpha_n]$ consists of all elements of E that can be expressed as polynomials in the α_i with coefficients in K, and $K(\alpha_1, \dots, \alpha_n)$ consists of all elements of E that can be expressed as a quotient of two such polynomials.

Let E and F be subfields of a field L. The intersection of the subfields of L containing both E and F is obviously the smallest subfield of L containing both E and F. We call it the **composite** of E and F in L, and we denote it by $E \cdot F$. It can also be described as the subfield of L generated over E by F, or the subfield generated over F by E:

$$E \cdot F = E(F) = F(E).$$

More generally, the composite $\bigvee E_i$ of a family $\mathcal{E} = \{E_i : i \in I\}$ of fields, all of which are contained in a single field L, is the smallest subfield of L containing all members of the family.

A **monomial** over a family $\mathcal{E} = \{E_i : i \in I\}$ of fields with $E_i \subseteq L$ is simply a product of a finite number of elements from the union $\bigcup_i E_i$. The set of all finite sums of monomials over $\mathcal{E}$ is the smallest subring R of L containing each field E_i and the set of all quotients of elements of R (the quotient field of R) is the composite $\bigvee E_i$. Thus, each element of $\bigvee E_i$ involves only a finite number of elements from the union $\bigcup_i E_i$ and is therefore contained in a composite of a finite number of fields from the family $\mathcal{E}$.

The collection of all subfields of a field L forms a complete lattice (under set inclusion), with meet being intersection and join being composite. The bottom element is the prime subfield of L and the top element is L itself.

9.1.1.1 Distinguished extensions

We will have much to say about towers of fields of the form $K \subseteq E \subseteq F$. Let us refer to such a tower as a **2-tower**, where E is the intermediate field, $K \subseteq E$ is the lower step, $E \subseteq F$ is the upper step and $K \subseteq F$ is the full extension.

Following Lang, we will say that a class $\mathcal{C}$ of field extensions is **distinguished** provided that it has the following properties

(1) (**The Tower Property**) For any 2-tower $K \subseteq E \subseteq F$, the full extension is in $\mathcal{C}$ if and only if the upper and lower steps are in $\mathcal{C}$. In symbols,

$$(K \subseteq F) \in \mathcal{C} \Leftrightarrow (K \subseteq E) \in \mathcal{C} \text{ and } (E \subseteq F) \in \mathcal{C}.$$

(2) (**The Lifting Property**) The class $\mathcal{C}$ is closed under lifting by an arbitrary field, that is,

$$(K \subseteq E) \in \mathcal{C} \text{ and } K \subseteq F \Rightarrow (F \subseteq EF) \in \mathcal{C}.$$

provided, of course, that EF is defined. The tower $F \subseteq EF$ is the **lifting** of $K \subseteq E$ by F.

(3) (**Closure under finite composites**) If EF is defined, then

$$(K \subseteq E) \in \mathcal{C} \text{ and } (K \subseteq F) \in \mathcal{C} \Rightarrow (K \subseteq EF) \in \mathcal{C}.$$

Note that if $\mathcal{C}$ satisfies (1) and (2), then it also satisfies (3). This follows from the fact that $K \subseteq EF$ can be decomposed into $K \subseteq F \subseteq EF$, and the first step is in $\mathcal{C}$, the second step is in $\mathcal{C}$ since it is the lifting of $K \subseteq E$ by F, and so the full extension is in $\mathcal{C}$. Therefore, to show a class $\mathcal{C}$ is distinguished, we noly need to check the properties (1) and (2).

If a class $\mathcal{C}$ of extensions has the property that

$$(K \subseteq E_i) \in \mathcal{C} \Rightarrow (K \subseteq \bigvee E_i) \in \mathcal{C}$$

for any family $\{E_i\}$ of fields (provided, as always, that the composite is defined), we say that $\mathcal{C}$ is **closed under arbitrary composites**. This property does not follow from closure under finite composites.

Here is a list of the common types of extensions and their distinguishedness. We will verify these statements in due course.

Distinguished	Nondistinguished
Algebraic extensions	Simple extensions
Finite extensions	Transcendental extensions
Finitely generated extensions	Normal extensions
Separable extensions	
Purely ineparable extensions	

9.1.2 Simple, finite, and algebraic extensions

9.1.2.1 Simple extensions

Definition 9.1.3. *A field extension E/K is **simple** if there exists an element $\alpha \in K$ such that $E = K(\alpha)$.*

Let $f(X) \in K[X]$ be a monic polynomial of degree n, and let $(f(X))$ be the ideal generated by f. Consider the quotient ring $K[X]/(f(X))$, and write α for the image of X in $K[X]/(f(X))$. The map $g(X) \mapsto g(\alpha)$ is a homomorphism from $K[X]$ to $K[\alpha]$ sending $f(X)$ to 0, so we have $f(X) = 0$. Moreover, the division algorithm shows that each element g of $K[X]/(f(X))$ is represented by a unique polynomial r of degree $< n$. Hence each element of $K[X]$ can be expressed uniquely as a sum

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}, \quad a_i \in K.$$

If in addition $f(X)$ is irreducible, then every nonzero in $K[\alpha]$ has an inverse, so $K[\alpha]$ becomes a field which extends K. From these observations, we conclude:

Proposition 9.1.4. *For a monic irreducible polynomial $f(X)$ of degree n in $K[X]$,*

$$E = K[X]/(f(X))$$

is a field of degree n over K.

It turns out that every simple extension is of the form mentioned above. To be precise, we have the following result.

Proposition 9.1.5. *Let $K \subseteq K(\alpha)$ be a simple extension. Consider the evaluation map $\epsilon : K[X] \to K(\alpha)$, defined by $f(X) \mapsto f(\alpha)$. Then we have the following:*

(i) ϵ is injective if and only if $K(\alpha)/K$ is an infinite extension. In this case, $K(\alpha)$ is isomorphic to the field of rational functions $K(X)$.

(ii) ϵ is not injective if and only if $K(\alpha)$ is finite. In this case there exists a unique monic irreducible nonconstant polynomial $p(X) \in K[X]$ of degree $n = [K(\alpha) : K]$ such that

$$K(\alpha) \cong \frac{K[X]}{(p(X))}$$

Via this isomorphism, α corresponds to the coset of x. The polynomial $p(X)$ is the monic polynomial of smallest degree in $K[X]$ such that $p(\alpha) = 0$ in $K(\alpha)$, it is called the ***minimal polynomial*** *of α over K.*

Proof. By the first isomorphism theorem, the image of $\epsilon : K[X] \to K(\alpha)$ is isomorphic to $K[X]/\ker\epsilon$. Since $K(\alpha)$ is an integral domain, so is $K[X]/\ker\epsilon$; hence $\ker(\epsilon)$ is a prime ideal in $K[X]$.

Assume $\ker\epsilon = 0$; that is, ϵ is an injective map from the integral domain $K[X]$ to the field $K(\alpha)$. By the universal property of fields of fractions, ϵ extends to a unique homomorphism

$$K(X) \to K(\alpha).$$

The (isomorphic) image of $K(X)$ in $K(\alpha)$ is a field containing K and α; hence it equals $K(\alpha)$ by definition of simple extension.

Since ϵ is injective, the powers $1, \alpha, \alpha^2, \cdots$ (that is, the images $\epsilon(X^i)$) are all distinct and linearly independent over K (because the powers $1, X, X^2, \cdots$ are linearly independent over K); therefore the extension $K \subseteq K(\alpha)$ is infinite in this case.

If $\ker\epsilon \neq 0$, then $\ker\epsilon = (p(X))$ for a unique monic irreducible nonconstant polynomial $p(X)$, which has smallest degree among all nonzero polynomials in $\ker\epsilon$. As $(p(X))$ is then maximal in $K[X]$, the image of ϵ is a subfield of $K(\alpha)$ containing $\alpha = \epsilon(X)$. By definition of simple extension, $K(\alpha)$ is the image of ϵ; that is, the induced homomorphism

$$\frac{K[X]}{(f(X))} \to K(\alpha)$$

is an isomorphism. In this case $[K(\alpha) : K] = \deg p(X)$, and in particular the extension is finite, as claimed. □

Example 9.1.6. Consider the extension $\mathbb{Q} \subseteq \mathbb{R}$. The polynomial $X^2 - 2 \in \mathbb{Q}[X]$ has roots in $\mathbb{R}$; therefore, there exists a homomorphism (hence a field extension)

$$\epsilon : \frac{\mathbb{Q}[X]}{(X^2 - 2)} \to \mathbb{R}$$

such that the image of (the coset of) x is a root α of $X^2 - 2$. Proposition 9.1.5 simply identifies the image of this homomorphism with $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$.

This is hopefully crystal clear; however, note that even this simple example shows that the induced morphism ϵ is not unique: because there are more than one root of $X^2 - 2$ in $\mathbb{R}$. Concretely, there are two possible choices for $\alpha : \alpha = +\sqrt{2}$ and $\alpha = -\sqrt{2}$. The choice of α determines the evaluation map ϵ and therefore the specific realization of $\mathbb{Q}[X]/(X^2 - 2)$ as a subfield of R.

Definition 9.1.7. *Let E/K be a field extension. The **group of automorphisms** of the extension, denoted $\mathrm{Aut}_K(E)$, is the group of field automorphisms $\sigma : E \to E$ such that $\sigma|_K = \mathrm{id}_K$.*

Corollary 9.1.8. *Let $K \subseteq E = K(\alpha)$ be a simple finite extension, and let $p(X)$ be the minimal polynomial of α over K. Then $|\mathrm{Aut}_K(E)|$ equals the number of distinct roots of $p(X)$ in K; in particular,*

$$|\mathrm{Aut}_K(E)| \leq [E : K]$$

with equality if and only if $p(X)$ factors over K as a product of distinct linear polynomials.

The class of simple extensions has all of the properties required of distinguished extensions except that the lower and upper steps being simple does not imply that the full extension is simple. That is, if each step in a 2-tower is simple

$$K \subseteq K(\alpha) \subseteq K(\alpha)(\beta) = K(\alpha, \beta).$$

this does not imply that the full extension is simple.

Example 9.1.9. Let u and v be independent variables and let p be a prime. In the tower

$$\mathbb{F}_p(u^p, v^p) \subseteq \mathbb{F}_p(u, v^p) \subseteq \mathbb{F}_p(u, v)$$

each step is simple but the full extension is not. We will prove this in due time.

On the other hand, if the full extension is simple: $K \subseteq K \subseteq K(\alpha)$, then the upper step is $K \subseteq K(\alpha)$, which is simple. Also, the lower step is simple, but the nontrivial proof requires us to consider the algebraic and transcendental cases separately. Here we give a proof about the algebraic case.

Proposition 9.1.10. *A finite extension E/K is simple if and only if the number of distinct intermediate fields $K \subseteq K \subseteq E$ is finite.*

Proof. Assume $E = K(\alpha)$ is simple and algebraic, and let $q(X)$ be the minimal polynomial of α over K. Embed E in an algebraic closure $\overline{K}$ of K. If K is an intermediate field, then $E = K(\alpha)$ is also a simple, algebraic extension; denote by $q_K(X)$ the minimal polynomial of α over K. Since $q_K(X) \in K[X]$ for all K and $q_K(\alpha) = 0$, we know that each $q_K(X)$ is a factor of $q_K(X)$. We claim

that K is in fact determined by $q_K(X)$. Since $q_K(X)$ has finitely many factors in K, this proves that there are only finitely many intermediate fields, that is, the only if part of the statement.

To verigy our claim, let K_0 be the field generated by the coefficients of $q_K(X)$. Then q_K has coefficients in K_0 and is irreducible over K_0 since it is irreducible over K. Hence the degree of α over K_0 is the same as the degree of α over K, and this implies $K = K_0$.

Assume that there is only a finite number of fields, intermediate between K and E. Let $\alpha, \beta \in E$. As c ranges over elements of K, we can only have a finite number of fields of type $K(c\alpha + \beta)$. Hence there exist elements $c_1, c_2 \in K$ with $c_1 \neq c_2$ such that

$$K(c_1\alpha + \beta) = K(c_2\alpha + \beta)$$

Note that $c_1\alpha + \beta$ and $c_2\alpha + \beta$ are in the same field, whence so is $(c_1 - c_2)\alpha$, and hence so is α. Thus β is also in that field, and we see that $K(\alpha, \beta)$ can be generated by one element.

Proceeding inductively, if $E = K(\alpha_1, \ldots, \alpha_n)$ then there will exist elements $c_1, \ldots, c_n \in K$ such that

$$E = K(c_1\alpha_1 + \cdots + c_n\alpha_n).$$

This proves our claim. □

In view of the previous theorem, it is clear that if $K \subseteq E \subseteq K(\alpha)$, where α is *algebraic*, then the lower step $K \subseteq E$ is also simple. (Note that $K \subseteq E$ is a finite extension and therefore finitely generated by the elements of a basis for E over K, whose elements are algebraic over K.)

9.1.2.2 Finite and algebraic extensions

Now we consider more complicated cases. The finite extension and algebraic extension defined below will be of our main consideration.

Definition 9.1.11. *Let E/K be a field extension, and let $\alpha \in E$. Then α is **algebraic** over K of degree n if $n = [K(\alpha) : K]$ is finite; α is **transcendantal** over K otherwise. The extension E/K is **algebraic** if every $\alpha \in E$ is algebraic over K.*

By Proposition 9.1.5, $\alpha \in E$ is algebraic over K if and only if there exists a nonzero polynomial $f(X) \in K[X]$ such that $f(\alpha) = 0$. The minimal polynomial of α is the monic polynomial of smallest degree satisfying this condition; as we have seen, it is necessarily irreducible. Also note that if α is algebraic over K, then every element of $K(\alpha)$ may in fact be written as a polynomial with coefficients in K.

It is clear that a finite extension must be algebraic.

Proposition 9.1.12. *Let E/K be a finite extension. Then every $\alpha \in E$ is algebraic over K, with degree less than $[E : K]$.*

Proof. Since $K \subseteq K(\alpha) \subseteq E$, the dimension of $K(\alpha)$ as a K-vector space is bounded by $\dim_K E = [E : K]$. □

Concretely, if E/K is finite and $\alpha \in E$, then the powers $1, \alpha, \alpha^2, \ldots$ are necessarily *linearly dependent*; and any nontrivial linear dependence relation among them provides us with a nonzero polynomial $f(X) \in K[X]$ such that $f(\alpha) = 0$.

The literal converse of the claim that finite extensions are algebraic is not true; we will see an example in a moment. However, something along these lines holds; understanding the situation requires a more careful look at finiteness conditions.

First of all, compositions of finite extensions are finite extensions, and the degree behaves nicely with respect to this operation:

Proposition 9.1.13 (Multiplicativity of Degrees). *Consider fields $K \subseteq E \subseteq F$. Then F/K is of finite degree if and only if F/E and E/K are both of finite degree, in which case*

$$[F : K] = [F : E][E : K].$$

Proof. If F is finite over K, then it is certainly finite over E; moreover, E, being a subspace of a finite-dimensional K-vector space, is also finite-dimensional.

Thus, assume that F/E and E/K are of finite degree, and let $\{e_1, \dots, e_m\}$ be a basis for E as an K-vector space and let $\{f_1, \dots, f_n\}$ be a basis for F as an E-vector space. To complete the proof of the proposition, it suffices to show that $\{e_i f_j : 1 \leq i \leq m, 1 \leq j \leq n\}$ is a basis for F over K, because then F will be finite over K of the predicted degree.

First, $\{e_i f_j\}$ spans F: let $\gamma \in F$, then because $\{f_j\}$ spans F as an E-vector space, we have

$$\gamma = \sum_j \alpha_j f_j$$

for some $\alpha_j \in E$. Because $\{e_i\}$ spans E as an K-vector space, for each j there exist $a_{ij} \in K$ such that

$$\alpha_j = \sum_i a_{ij} e_i.$$

On putting these together, we find that

$$\gamma = \sum_{i,j} a_{ij} e_i f_j.$$

Second, $\{e_i f_j\}$ is linearly independent. A linear relation $\sum_{ij} a_{ij} e_i f_j = 0$, $a_{ij} \in K$, can be rewritten into $\sum_j (\sum_i a_{ij} e_i) f_j = 0$. The linear independence of the f_j's now shows that $\sum_i a_{ij} e_i = 0$ for each j, and the linear independence of the e_i's shows that each $a_{ij} = 0$. □

As in the case of groups, we draw the immediate (but powerful) consequence, reminiscent of Lagrange's theorem:

Corollary 9.1.14. *Let L/K be a finite extension, and let E be an intermediate field (that is, $K \subseteq E \subseteq L$). Then both $[L : E]$ and $[E : K]$ divide $[L : K]$.*

Example 9.1.15. Let E/K be a field extension, and let $\alpha \in E$ be an algebraic element over K, of odd order. Then we claim that α may be written as a polynomial in α^2, with coefficients in K. Indeed, $K(\alpha^2)$ is intermediate between K and $K(\alpha)$:

$$K \subseteq K(\alpha^2) \subseteq K(\alpha)$$

Let $d = [K(\alpha) : K(\alpha^2)]$. Since α satisfies the polynomial $X^2 - \alpha^2 \in K(\alpha^2)[X]$, we get $d \leq 2$. On the other hand, d divides $[K(\alpha) : K]$ by Corollary 9.1.14, and $[K(\alpha) : K]$ is odd, so $d \neq 2$.

Therefore $d = 1$, proving $K(\alpha) = K(\alpha^2)$, and in particular $\alpha \in K(\alpha^2)$, which is the claim.

Here is something else that should evoke fond memories for the reader. An algebra is **finite** over the base ring if it is finitely generated as a *module*, that is, if it admits an onto homomorphism (of modules) from a finitely generated free module; a commutative algebra is of **finite type** if it admits an onto homomorphism (of algebras) from a polynomial ring in finitely many variables.

Something along the same lines is going to occur here. First, it is easy to see that an extension E/K is finite if and only if $\dim_K E$ is finite, that is, if and only if E is a finite K-algebra. The other finiteness condition takes the following form.

Definition 9.1.16. *A field extension E/K is **finitely generated** if there exist $\alpha_1, \dots, \alpha_n \in K$ such that*

$$E = K(\alpha_1, \alpha_2, \dots, \alpha_n).$$

Coming back to the issue of finite vs. algebraic, these two notions do coincide for finitely generated extensions.

Proposition 9.1.17. *Let $K \subseteq E = K(\alpha_1, \dots, \alpha_n)$ be a finitely generated field extension. Then the following are equivalent:*

(i) E/K is a finite extension.

(ii) E/K is an algebraic extension.

(iii) Each α_i is algebraic over K.

If these conditions are satisfied, then

$$[E : K] \leq \prod_{i=1}^{n} [K(\alpha_i) : K].$$

Proof. Proposition 9.1.12 show that $(i) \Rightarrow (ii)$, $(ii) \Rightarrow (iii)$ tivially, so we prove the implication $(iii) \Rightarrow (i)$. Assume that each α_i is algebraic over K, and let d_i be the degree of α_i over K. By definition, $K \subseteq K(\alpha_i)$ is finite, of degree d_i. Since each extension

$$K(\alpha_1, \dots, \alpha_{i-1}) \subseteq K(\alpha_1, \dots, \alpha_i)$$

is finite, of degree $\leq d_i$, Applying Corollary 9.1.14 to the composition of extensions

$$K \subseteq K(\alpha_1) \subseteq K(\alpha_1, \alpha_2) \subseteq \cdots \subseteq K(\alpha_1, \dots, \alpha_n) = E$$

proves that E/K is finite and $[E : K] \leq d_1 \cdots d_n$, as needed. □

While rather straightforward, Proposition 9.1.17 has always seemed remarkable to us: it says (in particular) that if α and β are algebraic over a field K, then so are $\alpha \pm \beta, \alpha\beta, \alpha\beta^{-1}$ and any other rational function of α and β. One immediate consequence of this observation is that the set of algebraic elements of any extension forms a field:

Corollary 9.1.18. *Let E/K be a field extension. Let*

$$\overline{K} = \{\alpha \in E : \alpha \text{ is algebraic over } K\}.$$

Then $\overline{K}$ is a field.

Example 9.1.19. Let $\overline{\mathbb{Q}} \subseteq \mathbb{C}$ be the set of complex numbers that are algebraic over $\mathbb{Q}$; then $\overline{\mathbb{Q}}$ is a field, and the extension $\mathbb{Q} \subseteq \overline{\mathbb{Q}}$ is (tautologically) algebraic. Note that $\mathbb{Q} \subseteq \overline{\mathbb{Q}}$ is not a finite extension, because in it there are elements of arbitrarily high degree over $\mathbb{Q}$: indeed, there exist irreducible polynomials in $\mathbb{Q}[X]$ of arbitrarily high degree.

Corollary 9.1.20. *If E is algebraic over K, then every subring of E containing K is a field.*

Proof. Let A be a ring with $K \subseteq A \subseteq E$. If $\alpha \in A$, then $K[\alpha] \subseteq A$. But $K[\alpha]$ is a field because α is algebraic, and so A contains α^{-1}. This implies A is a field. □

Another consequence of Proposition 9.1.17 is the important fact that compositions of algebraic extensions are algebraic (whether finitely generated or not):

Corollary 9.1.21. *Let $K \subseteq E \subseteq F$ be field extensions. Then F/K is algebraic if and only if both F/E and E/K are algebraic.*

Proof. If F/K is algebraic, then every element of F is algebraic over K, hence over E, and every element of E is algebraic over K; thus F/K and E/K are algebraic.

Conversely, assume F/E and E/K are both algebraic, and let $\alpha \in F$. Since α is algebraic over E, there exists a polynomial

$$f(X) = X^n + e_{n-1}X^{n-1} + \cdots + e_0 \in E[X]$$

such that $f(\alpha) = 0$. This implies that α is already algebraic over the subfield $K(e_0, \ldots, e_{n-1})$; therefore,

$$K(e_0, \ldots, e_{n-1}) \subseteq K(e_0, \ldots, e_{n-1}, \alpha)$$

is a finite extension. On the other hand, since each e_i is in E and therefore algebraic over K, the extension

$$K \subseteq K(e_0, \ldots, e_{n-1})$$

is finite by Proposition 9.1.17. By Proposition 9.1.13 the extension

$$K \subseteq K(e_0, \ldots, e_{n-1}, \alpha)$$

is finite. This implies that α is algebraic over K. □

Theorem 9.1.22. *Let E be an extension of K and X a subset of E such that $E = K(X)$ and every element of X is algebraic over K. Then E is an algebraic extension of K. If X is a finite set, then E is a finite extension of K.*

Proof. If $\beta \in E$, then $\beta \in K(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_1, \ldots, \alpha_n \in X$. By Proposition 9.1.17, since $K(\alpha_1, \ldots, \alpha_n)$ is finitely generated, we conclude that it is finite. Hence by Proposition 9.1.12 β is algebraic over K. □

We will essentially deal only with finitely generated extensions, and Proposition 9.1.17 will simplify our work considerably. Also, since finitely generated extensions are compositions of simple extensions, the reader should expect that we will give a careful look at automorphisms of such extensions.

It may in fact come as a surprise that, in many cases, finitely generated extensions turn out to be simple to begin with; we will prove a precise statement to this effect in due time. The reader already has enough tools to contemplate easy (but interesting) examples, such as the following. This should serve as an encouragement to look at many more.

Example 9.1.23. Consider the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. This is a finite extension, of degree at most 4, thus any five elements in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ must be linearly dependent over $\mathbb{Q}$. We consider the powers of $(\sqrt{2} + \sqrt{3})$:

$$1, \quad (\sqrt{2} + \sqrt{3}), \quad (\sqrt{2} + \sqrt{3})^2, \quad (\sqrt{2} + \sqrt{3})^3, \quad (\sqrt{2} + \sqrt{3})^4.$$

These elements must be linearly dependent, and we find

$$q_0 + q_1(\sqrt{2} + \sqrt{3}) + q_2(\sqrt{2} + \sqrt{3})^2 + q_3(\sqrt{2} + \sqrt{3})^3 + (\sqrt{2} + \sqrt{3})^4 = 0$$

is satisfied when $q_0 = 1, q_1 = 0, q_2 = -10, q_3 = 0$: that is, $(\sqrt{2} + \sqrt{3})$ is the root of

$$f(X) = X^4 - 10X^2 + 1.$$

It follows that $\sqrt{2} + \sqrt{3}$ has degree 4 over $\mathbb{Q}$, therefore $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$.

Consider the composition of extensions

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

By Corollary 9.1.14, we have

$$4 = [\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] \leq [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}],$$

thus we conclude that $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2} + \sqrt{3})]$, and it follows that

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3}).$$

Staring now at the composition

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}),$$

Corollary 9.1.14 tells us that $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$. That is, a side-effect of the computation carried out above is that the polynomial $t^2 - 3$ must be irreducible over $\mathbb{Q}(\sqrt{2})$.

The fact that the other roots of the minimal polynomial of $\sqrt{2} + \sqrt{3}$ looked so much like $\sqrt{2} + \sqrt{3}$ is not surprising. Indeed, since $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3})$ is a simple extension, we know that there is an automorphism of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ fixing $\mathbb{Q}(\sqrt{2})$ and swappint $\sqrt{3}$ and $-\sqrt{3}$. Similarly, there is an automorphism fixing $\mathbb{Q}(\sqrt{3})$ and swapping $\sqrt{2}$ and $-\sqrt{2}$. These automorphisms must act on the set of roots of $f(X)$: applying them and their composition to $\sqrt{2} + \sqrt{3}$ produces the other three roots of $f(X)$.

In fact, at this point we know that $G = \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}, \sqrt{3}))$ must consist of 4 elements and has at least two elements of order 2 (both automorphisms found above have order 2). This is enough to conclude that G is not a cyclic group, and hence it must be isomorphic to the group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

9.1.3 Algebraic closure

Recall that a field K is **algebraically closed** if all irreducible polynomials in $K[X]$ have degree 1, that is, if every polynomial in $K[X]$ factors completely as a product of linear terms. Equivalently every maximal ideal in $K[X]$ is of the form $(X - c)$, for $c \in K$. The following lemma is immediate from the definition.

Lemma 9.1.24. *For a field K, the following are equivalent:*

- *K is algebraically closed.*
- *K has no nontrivial algebraic extensions.*
- *If L is any extension of K and $\alpha \in L$ is algebraic over K, then $\alpha \in K$.*

Definition 9.1.25. *An **algebraic closure** of a field K is an algebraic extension $K \subseteq \Omega$ such that Ω is algebraically closed.*

We can now easily establish the existence of algebraic closures.

Theorem 9.1.26. *Let K be a field. Then there is an extension Ω of K that is algebraically closed.*

Proof. The following proof is due to Emil Artin. The first step is to construct an extension field K_1 of K, with the property that all nonconstant polynomials in $K[X]$ have a root in K_1.

To do this, consider a set $\mathscr{T} = \{t_f\}$ in bijection with the set of nonconstant monic polynomials $f(X) \in K[X]$, and let $K[\mathscr{T}]$ be the corresponding polynomial ring in all the indeterminates t_f. Let $I \subseteq K[\mathscr{T}]$ be the ideal generated by all polynomials $f(t_f)$. Then I is a proper ideal. Indeed, otherwise we could write

$$1 = \sum_{i=1}^{n} a_i f_i(t_{f_i}) \tag{1.3.1}$$

where $a_i \in K[\mathscr{T}]$. We claim that this cannot be done: indeed, we can construct an extension E/K where the polynomials $f_1, \ldots, f_n$ have roots $\alpha_1, \ldots, \alpha_n$, respectively; view (1.3.1) as an identity in $F[\mathscr{T}]$, and plug in $t_{f_i} = \alpha_i$, obtaining

$$1 = \sum_{i=1}^{n} a_i f(\alpha_i) = \sum_{i=1}^{n} a_i \cdot 0 = 0$$

which is nonsense.

Since I is proper, it is contained in a maximal ideal $\mathfrak{m}$ containing I. Thus, we obtain a field extension

$$K \subseteq K_1 := K[\mathscr{T}]/\mathfrak{m}.$$

By construction every nonconstant monic (and hence every nonconstant) polynomial $f(X)$ has a root in K_1, namely the coset of t_f.

Using the same technique, we may define a tower of field extensions

$$K \subseteq K_1 \subseteq K_2 \subseteq \cdots$$

such that each nonconstant polynomial $f(X) \in K_i[X]$ has a root in K_{i+1}. The union $\Omega = \bigcup_i K_i$ is an extension field of K. Moreover, any polynomial $f(X) \in \Omega[X]$ has all of its coefficients in K_i for some i and so has a root in K_i, hence in Ω. It follows that every polynomial in $\Omega[X]$ splits over Ω. Hence Ω is algebraically closed. □

We can now easily establish the existence of algebraic closures.

Theorem 9.1.27. *Let $K \subseteq L$ be a field extension where L is algebraically closed. Let*

$$\overline{K} = \{\alpha \in L : \alpha \text{ is algebraic over } K\}.$$

Then $\overline{K}$ is the only algebraic closure of K that is contained in L. Thus, any field has an algebraic closure.

Proof. By Corollary 9.1.18, $\overline{K}$ is a field, and the extension $K \subseteq \overline{K}$ is tautologically algebraic. To verify that $\overline{K}$ is algebraically closed, let α be algebraic over $\overline{K}$; then

$$K \subseteq \overline{K} \subseteq \overline{K}(\alpha)$$

is a composition of algebraic extensions, so $\overline{K} \subseteq \overline{K}(\alpha)$ is algebraic, and in particular α is algebraic over K. But then $\alpha \in \overline{K}$, by definition of the latter. It follows that $\overline{K}$ is algebraically closed, by Lemma 9.1.24.

As to uniqueness, if $K \subseteq E \subseteq L$ with E an algebraic closure of K, then since $K \subseteq E$ is algebraic, we have $E \subseteq \overline{K}$. But if the inclusion is proper, then there is an $\alpha \in \overline{K} \setminus E$. It follows that $\min(\alpha, E)$ does not split over E, a contradiction to the fact that E is algebraically closed. Hence $\overline{K} = E$. The final statement comes from Theorem 9.1.26. □

We will show a bit later that all algebraic closures of a field K are isomorphic, which is one reason why the notation $\overline{K}$ is (at least partially) justified.

Here is a characterization of algebraic closures.

Proposition 9.1.28. *Let $K \subseteq E$ be a field extension. The following are equivalent.*

(i) E is an algebraic closure of K.

(ii) E is a maximal algebraic extension of K, that is, $K \subseteq E$ is algebraic, and if $E \subseteq F$ is algebraic then $F = E$.

(iii) E is a minimal algebraically closed extension of K, that is, if $K \subseteq E' \subseteq E$ where E' is algebraically closed, then $E' = E$.

(iv) $K \subseteq E$ is algebraic and every nonconstant polynomial in $K[X]$ splits over E.

Proof. To see that (i) implies (ii), suppose that E is an algebraic closure of K. Then E/K is algebraic by definition. If $E \subseteq F$ is another algebraic extension, then by Lemma 9.1.24 we have $F = E$. Therefore E is a maximal algebraic extension of K. Conversely, let E be a maximal algebraic extension of K and let $f(X) \in E[X]$. Let L be the splitting field for $f(X)$ over E. Then

$K \subseteq E \subseteq L$ is an algebraic tower, since L is generated over E by the finite set of roots of $f(X)$. Hence, the maximality of E implies that $E = L$, and so $f(X)$ splits in E, which says that E is algebraically closed and therefore an algebraic closure of K.

To see that (i) implies (iii), suppose that E is an algebraic closure of K and $K \subseteq E' \subseteq E$, where E' is algebraically closed. Since $E' \subseteq E$ is algebraic, it follows that $E' = E$, by Lemma 9.1.24. Conversely, suppose that E is a minimal algebraically closed extension of K. Let $\overline{K}$ be the algebraic closure of K in E. Thus, $K \subseteq \overline{K} \subseteq E$, with $K \subseteq \overline{K}$ algebraic. By hypothesis, since $\overline{K}$ is algebraic closed, we conclude $\overline{K} = E$, so E is an algebraic closure of K.

Finally, it is clear that (i) implies (iv). If (iv) holds, then E/K is algebraic and if $K \subseteq E \subseteq L$ is algebraic, then let $\alpha \in L \setminus E$ have minimal polynomial $f(X)$ over K. This polynomial splits over E and so $\alpha \in E$, which implies that $E = L$, whence E is a maximal algebraic extension of K and so (ii) holds. □

9.1.4 Embeddings and their extensions

Homomorphisms between fields play a key role in the theory. Since a field has no nontrivial ideals, any homomorphism between fields is actually an embedding. In this part we study the general properties of embedding of fields and the extension of embeddings.

Let $\sigma : K \to L$ be an embedding of K into L and let E be an extension of K. An embedding $\bar{\sigma} : E \to L$ for which $\bar{\sigma}|_K = \sigma$ is called an **extension** of σ to E. An embedding of E that extends the identity map on K is called an **embedding over K**, or **K-embedding**. The set of all embeddings of K into L is denoted by $\mathrm{Hom}(K, L)$; the set of all embeddings of E into L that extend σ is denoted by $\mathrm{Hom}_\sigma(E, L)$ and the set of all embeddings over F is denoted by $\mathrm{Hom}_K(E, L)$.

Embeddings play a central role in Galois theory, and it is important to know when a given embedding $\sigma : K \to L$ can be extended to a larger field E, and how many such embeddings are possible. We will discuss the former issue here, and the latter issue in the next section.

First we establish some basic properties of embeddings. If $f(X) = \sum_i a_i X^i \in K[X]$ and if $\sigma : K \to E$ is an embedding, the polynomial $\sum_i \sigma(a_i) X^i$ is denoted by $f^\sigma(X)$.

Proposition 9.1.29 (Properties of embeddings).

(i) (***Embeddings preserve factorizations and roots***) *If $\sigma : K \to L$ is an embedding and $f(X)$, $p(X)$, $q(X)$ are polynomials in $K[X]$, then $f(X) = p(X)q(X)$ if and only if $f^\sigma(X) = p^\sigma(X)q^\sigma(X)$. Also, $\alpha \in K$ is a root of $f(X)$ if and only if $\sigma(\alpha)$ is a root of $f^\sigma(X)$.*

(ii) (***Embeddings preserve the lattice structure***) *If $\sigma : F \to L$ is an embedding and $\{E_i : i \in I\}$ is a family of subfields of F, then*

$$\sigma\Big(\bigcap_i E_i\Big) = \bigcap_i \sigma(E_i), \quad \sigma\Big(\bigvee_i E_i\Big) = \bigvee_i \sigma(E_i).$$

(iii) (***Embeddings preserve adjoining***) *If $\sigma : E \to F$ is an embedding and if $K \subseteq E$ and $S \subseteq E$, then*

$$\sigma(K(S)) = \sigma(K)(\sigma(S)).$$

(iv) (***Embeddings preserve being algebraic***) *Let $\sigma : K \to L$ is an embedding and let E/K be an algebraic extension. If $\bar{\sigma} : E \to L$ is an extension of σ, then $\sigma(K) \subseteq \bar{\sigma}(E)$ is algebraic.*

(v) (***Embeddings preserve algebraic closures***) *Let $\sigma : K \to L$ and let E be an algebraic closure of K. If $\bar{\sigma} : E \to L$ is an extension of σ, then $\bar{\sigma}(E)$ is an algebraic closure of $\sigma(K)$.*

Proof. Part (i) is easy to prove, and part (ii) follows from the following observation

$$\begin{aligned}\sigma\Big(\bigvee E_i\Big) &= \bigcap\{\sigma(H) : E_i \subseteq H \subseteq F \text{ for all } i \in I\}\\ &= \bigcap\{H' : \sigma(E_i) \subseteq H' \subseteq \sigma(F) \text{ for all } i \in I\} = \bigvee \sigma(E_i).\end{aligned}$$

Also, part (iii) follows from (ii).

For (iv), let $\alpha \in E$, then α is algebraic over K, so there is a polynomial $f(X) \in K[X]$ such that $f(\alpha) = 0$. By (i) we know that $\bar{\sigma}(\alpha)$ is a root of $f^{\bar{\sigma}}$, so it is algebraic over $\sigma(K)$, since α is arbitrary, this implies $\bar{\sigma}(E)$ is algebraic over $\sigma(K)$. Finally we prove (v). Since E/K is algebraic, by (iv) the extension $\bar{\sigma}(E)$ is algebraic over $\sigma(K)$. Let f^{σ} be a polynomial in $\sigma(K)[X]$. Then $f(X) \in K[X]$ so $f(X)$ split in E, since E is algebraic closed. It follows that f^{σ} split in $\bar{\sigma}(E)$, in view of (i), and therefore $\bar{\sigma}(E)$ is an algebraic closure of $\sigma(K)$, by Proposition 9.1.28. □

Even though the next result has a simple proof, the result is of major importance.

Theorem 9.1.30. *If $K \subseteq E$ is algebraic and $\sigma : E \to E$ is a K-embedding, then σ is an automorphism. In other words,*

$$\mathrm{Hom}_K(E, E) = \mathrm{Aut}_K(E).$$

Proof. Let $\alpha \in E$ and let R be the set of roots of the minimal polynomial of α that lie in E. Then $\sigma|_R$ is an injection on R and so is bijective. Therefore there is a $\beta \in S$ for which $\sigma(\beta) = \alpha$. Hence, σ is surjective and thus an automorphism of E. □

Now we proceed the construction of extension of embeddings. We first consider simple extensions. Suppose that $\sigma : K \to L$, where L is algebraically closed. Let α be algebraic over K. We can easily extend σ to $K(\alpha)$, using the minimal polynomial of α over K.

Proposition 9.1.31. *Let $K \subseteq E$ and let $\alpha \in E$ be algebraic over K with minimal polynomial $f(X)$. Let $\sigma : K \to L$ be an embedding, where L is algebraically closed.*

(i) *If β is any root of f^{σ} in L, then σ can be extended to an embedding $\bar{\sigma} : K(\alpha) \to L$ for which $\bar{\sigma}(\alpha) = \beta$. Moreover, any extension of σ to $K(\alpha)$ must have this form.*

(ii) *The number of extensions of σ to $K(\alpha)$ is equal to the number of distinct roots of $f(X)$ in L.*

Proof. The key point is that any extension $\bar{\sigma}$ of σ is completely determined by its value on α and this value must be a root β of $f^{\sigma}(X)$. In fact, we must have

$$\bar{\sigma}(f(\alpha)) = f^{\sigma}(\beta)$$

for any $f \in K[X]$. This prove (i), and (ii) follows from (i). □

The simple case above, together with Zorn's lemma, is just what we need to prove that if $\sigma : K \to L$, with L algebraically closed and if E/K is algebraic, then there is at least one extension of σ to E.

Theorem 9.1.32. *Let $K \subseteq E$ be an algebraic extension. Then any embedding $\sigma : K \to L$, where L is algebraically closed, can be extended to an embedding $\bar{\sigma} : E \to L$. Moreover, if $\alpha \in E$, $f(X) = \min(\alpha, K)$, and β is a root of $f^{\sigma}(X)$, then we can choose $\bar{\sigma}$ so that $\bar{\sigma}(\alpha) = \beta$.*

Proof. Consider the set $\mathcal{E}$ of homomorphisms $\tau \in \mathrm{Hom}_{\sigma}(K, L)$ such that $\tau(\alpha) = \beta$, where K is an intermediate field; $\mathcal{E}$ is nonempty, since the extension $\sigma_{\beta} : K(\alpha) \subseteq L$ defined by $\sigma_{\beta}(\alpha) = \beta$ gives an element of $\mathcal{E}$. We give a poset structure to $\mathcal{E}$ by defining

$$\tau \preceq \tau'$$

if $K \subseteq K' \subseteq E$ and τ' restricts to τ on K. If $\mathcal{K} = \{\tau_i : K_i \to L\}$ is a chain in $\mathcal{E}$, the map $\tau : \bigcup K_i \to L$ defined by the condition $\tau|_{K_i} = \tau_i$ is an upper bound for $\mathcal{K}$ in $\mathcal{E}$. Zorn's lemma implies the existence of a maximal extension $\tau : K \to L$. We contend that $K = E$, for if not, there is an element $\gamma \in E \setminus K$. But γ is algebraic over K and so we may extend τ to $K(\gamma)$, contradicting the maximality. □

As a corollary, we can establish the essential uniqueness of algebraic closures.

Theorem 9.1.33. *Every field K admits an algebraic closure $K \subseteq \overline{K}$; this extension is unique up to isomorphism.*

Proof. We only need to show the second point. Let L_1 and L_2 be algebraic closures of K. The identity map $\mathrm{id} : K \to K$ can be extended to an embedding $\tau : L_1 \to L_2$. Since L_1 is algebraically closed so is $\sigma(L_1)$ (Proposition 9.1.29). But L_2 is an algebraic extension of $\sigma(L_1)$ and so $\sigma(L_1) = L_2$. Hence, σ is an isomorphism. □

To conclude, we introduce the independence of embedding and prove a very useful result. We choose a somewhat more general setting, however. A **monoid** is a nonempty set M with an associative binary operation and an identity element. If M and N are monoids, a homomorphism of M into N is a map $\varphi : M \to N$ such that $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$ and $\varphi(1) = 1$.

Definition 9.1.34. *Let M be a monoid and let K be a field. A homomorphism $\chi : M \to K^{\times}$, where $K^{\times}$ is the multiplicative group of all nonzero elements of K, is called a **character** of M in K.*

Note that an embedding $\sigma : E \to L$ of fields is a character, when restricted to $E^{\times}$.

Theorem 9.1.35 (E. Artin)**.** *Any set $\mathcal{T}$ of distinct characters of M in K is linearly independent over K.*

Proof. Suppose that we have a nontrivial relation

$$\sum_{i=1}^{n} a_i \chi_i = 0$$

for some $\chi_i \in \mathcal{T}$ and $a_i \in K$. Look among all such nontrivial linear combinations of the χ_i's for one with the fewest number of nonzero coefficients and, by relabeling if necessary, assume that these coefficients are $a_1, \ldots, a_r$. Thus,

$$a_1\chi_1(g) + \cdots + a_r\chi_r(g) = 0 \tag{1.4.1}$$

for all $g \in M$ and this is the "shortest" such nontrivial equation (hence $a_i \neq 0$ for all i). Note that since $\chi_i(g) \in K^\times$, we have $\chi_i(g) \neq 0$ for all $g \in M$. Hence, $r > 1$.

Let us find a shorter relation. Since χ_1 is a character, $\chi_1(f) \neq 0$ for all $f \in M$. Multiplying by $\chi_1(f)$ gives

$$a_1\chi_1(f)\chi_1(g) + a_2\chi_1(f)\chi_2(g) + \cdots + a_r\chi_1(f)\chi_r(g) = 0.$$

On the other hand, replacing g by fg in (1.4.1) gives

$$a_1\chi_1(f)\chi_1(g) + a_2\chi_2(f)\chi_2(g) + \cdots + a_r\chi_r(f)\chi_r(g) = 0.$$

Subtracting the two equations cancels the first term, and we get

$$a_2[\chi_1(f) - \chi_2(f)]\chi_2(g) + \cdots + a_r[\chi_1(f) - \chi_r(f)]\chi_r(g) = 0.$$

Now, since $\chi_1 \neq r$, there is an $f \in M$ for which $\chi_1(f) - \chi_r(f) \neq 0$ and we have a shorter nontrivial relation of the form (1.4.1). This contradiction proves the theorem. □

Corollary 9.1.36 (Dedekind independence theorem). *Let E and F be fields. Any set of distinct embeddings of E into F is linearly independent over F.*

9.1.5 Splitting fields and normal extensions

we have constructed the algebraic closure $\overline{K}$ of any given field K: every polynomial in $K[X]$ factors as a product of linear terms (that is, *splits*) in $\overline{K}[X]$, and $\overline{K}$ is the smallest extension of K satisfying this property.

Here is an analogous, but more modest, requirement: given a subset $\mathcal{F} \subseteq K[X]$ of polynomials, construct an extension E/K such that every polynomial in $\mathcal{F}$ splits as a product of linear terms over E, and require E to be as small as possible with this property. We then call E the *splitting field* for $\mathcal{F}$. To be precise, we make the following definition.

Definition 9.1.37. *Let K be a field, and let $\mathcal{F}$ be a family of polynomials in $K[X]$. The **splitting field** for $\mathcal{F}$ over K is an extension E of K such that each polynomial in $\mathcal{F}$ splits in E and that E is generated by the set of all roots of the polynomials in $\mathcal{F}$.*

The next theorem says that splitting fields not only exist, but are essentially unique.

Theorem 9.1.38. *Let $\mathcal{F}$ be a family of polynomials over K.*

(i) In any algebraic closure $\overline{K}$ of K, there is a unique splitting field for $\mathcal{F}$.

(ii) If $K \subseteq E_1 \subseteq L_1$ and $K \subseteq E_2 \subseteq L_2$ are algebraic, where E_1 is the splitting field for $\mathcal{F}$ in L_1 and E_2 is the splitting field for $\mathcal{F}$ in L_2, then any embedding $\sigma : L_1 \to L_2$ over K maps E_1 onto E_2.

(iii) Any two splitting fields for $\mathcal{F}$ are isomorphic over K.

Proof. For part (i), if $\mathcal{F}$ is a family of polynomials over K, then every member of $\mathcal{F}$ splits in $\overline{K}$ and so $\overline{K}$ contains the field E generated over K by the roots in $\overline{K}$ of the polynomials in $\mathcal{F}$, that is, $\overline{K}$ contains a splitting field for $\mathcal{F}$. It is clear that this splitting field is unique in $\overline{K}$, because any splitting field in $\overline{K}$ must be generated, in $\overline{K}$, by the roots of all polynomials in $\mathcal{F}$.

For part (ii), if R is the family of roots of $\mathcal{F}$ contained in L_1 then $E_1 = K(R)$ and so

$$\sigma(E_1) = \sigma(K(R)) = K(\sigma(R)).$$

But $\sigma(R)$ is precisely the set of roots of $\mathcal{F}$ in L_2 and so $K(\sigma(R))$ is the splitting field for $\mathcal{F}$ in L_2, that is, $\sigma(E_1) = E_2$. Part (iii) follows immediately from part (ii). □

Example 9.1.39. The splitting field of $X^8 - 1$ over $\mathbb{Q}$ is generated by $\zeta := e^{2\pi i}/8$: indeed, the roots of $X^8 - 1$ are all the 8-th roots of 1, and all of them are powers of ζ. In fact, ζ is a root of the polynomial $X^4 + 1$, which is irreducible over $\mathbb{Q}$; therefore $E = \mathbb{Q}(\zeta)$ is already the splitting field of $X^4 + 1$. The degree of E over $\mathbb{Q}$ is

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = 4.$$

To understand this splitting field better, note that $i = \zeta^2$ is in E, and so is $\sqrt{2} = \zeta + \bar{\zeta} = \zeta + \zeta^{-1}$; thus E contains $\mathbb{Q}(i, \sqrt{2})$. Conversely, $\zeta = \frac{\sqrt{2}}{2}(1 + i) \in \mathbb{Q}(i, \sqrt{2})$. Therefore, the splitting field of $X^4 + 1$ is $\mathbb{Q}(i, \sqrt{2})$. Analyzing $\mathbb{Q} \subseteq \mathbb{Q}(i, \sqrt{2})$ shows that its group of automorphisms over $\mathbb{Q}$ is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Example 9.1.40. The polynomial $X^4 - 1$ factors over $\mathbb{Q}$:

$$X^4 - 1 = (X^2 + 1)(X + 1)(X - 1)$$

and it follows that the splitting field is the same as for $X^2 + 1$, that is, just $\mathbb{Q}(i)$.

Example 9.1.41. Now consider the polynomial $X^4 + 2$ over $\mathbb{Q}$. The overoptimistic reader may now hope that the difference between the splitting fields of $X^4 + 1$ vs. $X^4 - 1$ over $\mathbb{Q}$ is just due to the fact that the first polynomial is irreducible over $\mathbb{Q}$ and the second is not. This example will nip any such guess in the bud. With notation as above, the roots of $X^4 + 2$ are

$$\sqrt[4]{2}\zeta, \quad \sqrt[4]{2}\zeta^3, \quad \sqrt[4]{2}\zeta^5, \quad \sqrt[4]{2}\zeta^7$$

Therefore, with $E = \mathbb{Q}(\sqrt[4]{2}\zeta, \sqrt[4]{2}\zeta^3, \sqrt[4]{2}\zeta^5, \sqrt[4]{2}\zeta^7)$ the splitting field of $X^4 + 2$,

$$E \subseteq \mathbb{Q}(\zeta, \sqrt[4]{2}) = \mathbb{Q}(i, \sqrt{2}, \sqrt[4]{2}) = \mathbb{Q}(i, \sqrt[4]{2}).$$

On the other hand,

$$\sqrt{2} = \frac{(\sqrt[4]{2}\zeta)^3}{\sqrt[4]{2}\zeta^3}, \quad i = \frac{(\sqrt[4]{2})^2}{\sqrt{2}}, \quad \zeta = \frac{\sqrt{2}}{2}(1 + i), \quad \sqrt[4]{2} = \frac{\sqrt[4]{2}\zeta}{\zeta}.$$

Therefore, $\mathbb{Q}(i, \sqrt[4]{2}) \subseteq E$, and the conclusion is that the splitting field of $X^4 + 2$ equals $E = \mathbb{Q}(i, \sqrt[4]{2})$. A simple degree computation shows $[E : \mathbb{Q}] = 8$ and in particular the splitting field of $X^4 + 2$ is certainly not isomorphic to the splitting field of $X^4 + 1$.

Example 9.1.42. Consider the polynomial $X^6 + X^3 + 1$ over $\mathbb{Q}$. Let $\omega := (-1 + \sqrt{3}i)/2$. The solutions of $X^2 + X + 1$ are ω, ω^2, so the solutions of $X^6 + X^3 + 1$ are

$$\sqrt[3]{\omega}, \quad \omega\sqrt[3]{\omega}, \quad \omega^2\sqrt[3]{\omega}, \quad \sqrt[3]{\omega^2}, \quad \omega\sqrt[3]{\omega^2}, \quad \omega^2\sqrt[3]{\omega^2}.$$

So the splitting field of $X^6 + X^3 + 1$ is $\mathbb{Q}(\omega^{1/3})$, which has degree 9 over $\mathbb{Q}$.

Splitting fields will play an important role in the rest of the story. They are even more special than they may appear to be at first: it turns out that not only do they split the given polynomial, but they also automatically split any irreducible polynomial which dares touch them with a root. To make this property crystal clear, we introduce the following terminology.

Suppose that $K \subseteq E \subseteq \overline{K}$ is algebraic and that $\sigma : E \to \overline{K}$ is an embedding over K of E into the algebraic closure $\overline{K}$. Then E is said to be ***σ*-invariant** if $\sigma(E) \subseteq E$. However, since E/K is algebraic, any embedding of E into itself is an automorphism of E (Theorem 9.1.30) and so E is σ-invariant if and only if $\sigma(E) = E$, that is, if and only if σ is an automorphism of E.

If the field E is σ-invariant for all embeddings $\sigma : E \to \overline{K}$ over K, then it is not hard to see that any irreducible polynomial $f(X)$ over K that has one root α in E must split over K. For if β is also a root of $f(X)$ in $\overline{K}$, then there is an embedding $\sigma \in \mathrm{Hom}_K(E, \overline{K})$ for which $\sigma(\alpha) = \beta$. Hence, the σ-invariance of E implies that $\beta \in E$. Put another way, we can say that E is the splitting field for the family

$$\min(E, K) := \{\min(\alpha, K) : \alpha \in E\}.$$

We now formulate the observation above into the following theorem.

Theorem 9.1.43. *Let $K \subseteq E \subseteq \overline{K}$, where $\overline{K}$ is an algebraic closure of K. The following are equivalent.*

(i) E is a splitting field for a family $\mathcal{F}$ of polynomials over K.

(ii) E is invariant under every embedding $\sigma : E \to \overline{K}$ over K.

(iii) Every irreducible polynomial over E having one root in E splits in E.

Proof. We have already see the implications $(ii) \Rightarrow (iii) \Rightarrow (i)$. Now we prove $(i) \Rightarrow (ii)$. Suppose that E is a splitting field of a family $\mathcal{F}$ of polynomials over K. Thus, $E = K(R)$, where R is the set of roots of the polynomials in $\overline{K}$. But any embedding $\sigma : E \to \overline{K}$ over K sends roots to roots and so sends R to itself. Hence,

$$\sigma(E) = \sigma(K(R)) = K(\sigma(R)) = K(R) = E.$$

Since σ is an embedding of E into itself over K and $K \subseteq E$ is algebraic, it follows that σ is an automorphism of E. Thus the claim follows. □

Definition 9.1.44. *An algebraic extension $K \subseteq E$ that satisfies any (and hence all) of the conditions in the previous theorem is said to be a **normal extension**. We also say that E is **normal** over K and write $K \lhd E$.*

Corollary 9.1.45. *If E/K is a finite normal extension, then E is the splitting field of a finite family of irreducible polynomials.*

Proof. Let $E = K(\alpha_1, \ldots, \alpha_n)$. Since E/K is normal, each minimal polynomial $\min(\alpha_i, K)$ splits in E. Clearly, E is generated by the roots of the finite family $\mathcal{F} = \{\min(\alpha_i, K) : i = 1, \ldots, n\}$ and so E is the splitting field of $\mathcal{F}$. □

Note that the extension $K \subseteq \overline{K}$ is normal, since any nonconstant polynomial $f(X) \in K[X]$ splits in $\overline{K}$.

Example 9.1.46. If a complex root of an irreducible polynomial $p(X) \in \mathbb{Q}[X]$ may be expressed as a polynomial in i and $\sqrt[4]{2}$ with rational coefficients, then all roots of $p(X)$ may be expressed likewise in terms of i and $\sqrt[4]{2}$. Indeed, we have checked that $\mathbb{Q}(i, \sqrt[4]{2})$ is a splitting field over $\mathbb{Q}$; hence it is a normal extension of $\mathbb{Q}$.

Example 9.1.47. Let E/K be a degree 2 extension. Let $\alpha \in E \setminus K$, then the minimal polynomial of α over K must have degree 2, and therefore $E = K(\alpha)$. It follows that $\alpha^2 \in K$, and so $X^2 - \alpha^2$ is a polynomial in $K[X]$. Clearly this is the minimal polynomial of α. Since it splits in E, it follows that E is normal over K.

9.1.5.1 Normal extensions are not distinguished

As it happens, the class of normal extensions is not distinguished, but it does enjoy some of the associated properties.

Example 9.1.48. The extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2})$ is not normal since $\mathbb{Q}(\sqrt[4]{2})$ contains exactly two of the four roots of the irreducible polynomial $X^4 - 2$. On the other hand,

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$$

has each step of degree 2 and therefore each step is normal.

Here is what we can say on the positive side.

Proposition 9.1.49 (Properties of normal extensions).

(a) (***Full extension normal implies upper step normal***) *Let $K \subseteq E \subseteq F$. If F is normal over K then F is normal over E.*

(b) (***Lifting of a normal extension is normal***) *If E is normal over K and $K \subseteq F$, then EF is normal over F.*

(c) (***Arbitrary composites and intersections of normal are normal***) *If $\{E_i\}$ is a family of fields, and each E_i is normal over K, then $\bigvee E_i$ and $\bigcap E_i$ are both normal over K.*

Proof. Part (a) follows from the fact that a splitting field for a family of polynomials over K is also a splitting field for the same family of polynomials over E.

For (b), let E be a splitting field for a family $\mathcal{F}$ of polynomials over K and let R be the set of roots in E of all polynomials in $\mathcal{F}$. Then $E = K(R)$. Hence, $EF = F(K(R)) = F(R)$, which shows that EF is a splitting field for the family $\mathcal{F}$, thought of as a family of polynomials over F. Hence, EF is normal over F.

For (c), let $\sigma : \bigvee E_i \to \overline{K}$ be an embedding over K. Then σ is an embedding when restricted to each E_i and so $\sigma(E_i) = E_i$, whence

$$\sigma\Big(\bigvee E_i\Big) = \bigvee \sigma(E_i) = \bigvee E_i,$$

and so σ is an automorphism of $\bigvee E_i$. Similarly, if $\sigma : \bigcap E_i \to \overline{K}$ over K, then

$$\sigma\Big(\bigcap E_i) = \bigcap \sigma(E_i) = \bigcap E_i.$$

This proves the claim. □

9.1.5.2 Normal closures

If the extension E/K is not normal, then there is a smallest extension N of E (in a given algebraic closure $\overline{K}$) for which N is normal over K. Perhaps the simplest way to see this is to observe that $K \subseteq \overline{K}$ is normal and the intersection of normal extensions is normal, so

$$N = \bigcap \{F \subseteq \overline{K} : F \text{ contains } E \text{ and the extension } F/K \text{ is normal}\}.$$

Definition 9.1.50. *Let $K \subseteq E \subseteq \overline{K}$. The **normal closure** of E over K in $\overline{K}$ is the smallest subfield of $\overline{K}$ containing E for which F/K is normal. The normal closure is denoted by $\langle E/K \rangle$.*

Theorem 9.1.51. *Let $K \subseteq E \subseteq \overline{K}$ be algebraic extensions, with normal closure $N = \langle E/K \rangle$.*

(b) N is the composition of the image of E under $\mathrm{Hom}_K(E, \overline{K})$.

(c) N is the splitting field in $\overline{K}$ of the family $\min(E, K)$.

(d) If $E = K(S)$, where $S \subseteq E$, then N is the splitting field in $\overline{K}$ of the family $\min(S, K)$.

(e) If E/K is finite, then N/K is also finite.

Proof. Let N' be the composition field in (a). If $\sigma \in \mathrm{Hom}_K(E, \overline{K})$ then σ can be extended to a K-embedding of N to $\overline{K}$, denoted by $\bar{\sigma}$. Since N normal, we have $\bar{\sigma}(N) = N$, and thus

$$\sigma(E) = \bar{\sigma}(E) \subseteq \bar{\sigma}(N) = N.$$

This shows $N' \subseteq N$. Conversely, we show that N'/K is normal, so that $N \subseteq N'$.

Let $\tau : N' \to \overline{K}$ be an K-embedding. Then by Theorem 9.1.32 τ extends to an automorphism φ of $\overline{K}$. Both of the inclusions of N' into $\overline{K}$ are K-embeddings, so φ must be a K-automorphism. Now for $\sigma \in \mathrm{Hom}_K(E, \overline{K})$, we see $\varphi \circ \sigma \in \mathrm{Hom}_K(E, \overline{K})$, therefore

$$\varphi(N') = \varphi(\bigvee_{\sigma \in \mathrm{Hom}_K(E,\overline{K})} \sigma(E)) = \bigvee_{\sigma \in \mathrm{Hom}_K(E,\overline{K})} \varphi(\sigma(E)) \subseteq N'.$$

Since φ coincides with τ on N', it follows that $\tau(N') = N'$ and thus N' is normal. This completes the proof of (a). The rest part are easy. □

9.1.6 Separable extensions and linearly disjointness

Our intuition may lead us to think that if a polynomial factors as a product of linear factors and we are not *purposely* repeating one of the factors (as in $(X-1)^2(X-2)$), then these will be *distinct*. For example, surely irreducible polynomials necessarily split as products of distinct factors in an algebraic closure, right? Wrong.

Example 9.1.52. Let p be a prime, and consider the field $\mathbb{F}_p(X)$ of rational functions over $\mathbb{F}_p$. Then the polynomial

$$X^p - t \in \mathbb{F}_p(t)[X]$$

is irreducible: by Eisenstein's criterion it is irreducible in $\mathbb{F}_p[t][X]$ (since (t) is prime in $\mathbb{F}_p[t]$), hence in $\mathbb{F}_p(t)[X]$ by Proposition 5.4.11. Let α be a root of this polynomial in an extension L

of $\mathbb{F}_p(X)$ (for example L could be the algebraic closure of $\mathbb{F}_p(X)$, or more modestly a splitting field for the polynomial). Then

$$X^p - t = (X - \alpha)^p$$

in $L[X]$; that is, α has multiplicity p as a root of $f(X)$.

In other words, the minimal polynomial over $\mathbb{F}_p(X)$ of $\alpha \in L$ vanishes p times at α, and there is nothing to do about this: no smaller power of $(X - \alpha)$ than $(X - \alpha)^p = X^p - t$ has coefficients in $\mathbb{F}_p(X)$ (a smaller power would give a nontrivial factor of $X^p - t$, and $X^p - t$ is irreducible).

We have always found this example difficult to visualize, because of intuition developed in characteristic 0, and as we will see, no such pathology can occur in characteristic 0.

9.1.6.1 Separable polynomials

Definition 9.1.53. *Let K be a field. A polynomial $f(X) \in K[X]$ is **separable** if it has no multiple factors over its splitting field; $f(X)$ is **inseparable** if it has multiple factors over its splitting field.*

The first, somewhat surprising, observation about separability is that we can in fact detect it without leaving the field of coefficients of $f(X)$. This fact uses a notion borrowed from calculus: for a polynomial

$$f(X) = a_0 + a_1 X + \cdots + a_n X^n$$

we denote by $f'(X)$ the derivative

$$f'(X) = a_1 + 2a_2 X + \cdots + n a_n X^{n-1}.$$

Of course this is a purely formal operation; no limiting process is at work over arbitrary fields. Still, all expected properties of derivatives hold, as the reader should check: for example, $(fg)' = f'g + fg'$ as usual.

Proposition 9.1.54. *Let K be a field, and let $f(X) \in K[X]$. Then $f(X)$ is separable if and only if $f(X)$ and $f'(X)$ are relatively prime.*

By definition, $f(X)$ and $f'(X)$ are relatively prime precisely when the greatest common divisor of $f(X)$ and $f'(X)$ is 1. Note that if E/K, the gcd of $f(X)$ and $f'(X)$ is the same whether it is considered in $K[X]$ or in $E[X]$: for example because it can be computed by applying the Euclidean algorithm, and this proceeds in exactly the same way whether it is performed in $K[X]$ or in $E[X]$.

Proof. Over a splitting field E for $f(X)$, we have

$$f(X) = (X - \alpha_1)^{e_1}(X - \alpha_2)^{e_2} \cdots (X - \alpha_n)^{e_n}$$

where the α_i's are distinct. It is easy to see that $f(X)$ and $f'(X)$ have no nontrivial common factors over E if and only if $e_i = 1$ for all i. □

For example, the polynomial $X^p - t$ may be seen to be inseparable without invoking splitting fields: the derivative of $X^p - t$ equals $pX^{p-1} = 0$ in characteristic p, and $\gcd(X^p - t, 0) = X^p - t \neq 1$. This example captures one of the key features of inseparability:

Corollary 9.1.55. *Let K be a field, and let $f(X) \in K[X]$ be an irreducible polynomial. Then $f(X)$ is separable if and only if $f'(X) \neq 0$.*

Proof. Since $\deg(f'(X)) < \deg(f(X))$ and f is irreducible, it follows that $f(X)$ and $f'(X)$ are relatively prime if and only if $f'(X) = 0$. □

Corollary 9.1.56. *All irreducible polynomials over a field of characteristic 0 are separable.*

In fact, Corollary 9.1.55 gives us a precise picture of what inseparable irreducible polynomials must look like. If

$$f(X) = \sum_{i=0}^{n} a_i X^i$$

is irreducible and inseparable, then the characteristic of the field must be a positive prime p, and by Corollary 9.1.55 we must have

$$f'(X) = \sum_{i=0}^{n} i a_i X^{i-1} = 0.$$

That is, $ia_i = 0$ for all i. Now $ia_i = 0$ is automatic if i is a multiple of p, and it implies $a_i = 0$ for all the indices i which are not multiples of p. Therefore, the only nonvanishing coefficients in $f(X)$ must be those corresponding to indices which are multiples of p:

$$f(X) = a_0 + a_p X^p + a_{2p} X^{2p} + \cdots,$$

therefore, $f(X)$ must in fact be a polynomial in X^p.

Corollary 9.1.57. *Let $\mathrm{char}(K) = p$. An irreducible polynomial $f(X)$ over K is inseparable if and only if $f(X)$ has the form*

$$f(X) = g(X^{p^d})$$

*where $d > 0$ and $g(X)$ is a nonconstant polynomial. In this case, the integer d can be chosen so that $g(X)$ is separable, in which case every root of $f(X)$ has multiplicity p^d. In this case, the number d is called the **radical exponent** of $f(X)$.*

Proof. As we mentioned, if $f(X)$ is inseparable then $f'(X) = 0$, which implies that $f(X) = q(X^p)$ for some polynomial $q(X)$. If $q(X)$ has no multiple roots, we are done. If not, then we may repeat the argument with the irreducible polynomial $q(X)$, eventually obtaining the equation $f(X) = g(X^{p^d})$, where $g(X)$ is separable.

For the converse, suppose that $f(X) = g(X^{p^d})$ for some $d > 0$. Let K be a field in which $f(X)$ and $g(X)$ split. Thus,

$$g(X) = (X - \alpha_1) \cdots (X - \alpha_K)$$

for $\alpha_i \in K$, and so

$$f(X) = (X^{p^d} - \alpha_1) \cdots (X^{p^d} - \alpha_k).$$

Since $f(X)$ splits in K, there exist roots $\beta_i \in K$ for each of the factors $(X^{p^d} - \alpha_i)$, and so $\beta_i^{p^d} = \alpha_i$. Hence,

$$f(X) = (X^{p^d} - \beta_1^{p^d}) \cdots (X^{p^d} - \beta_k^{p^d}) = (X - \beta_1)^{p^d} \cdots (X - \beta_k)^{p^d}.$$

This shows that $f(X)$ is inseparable. Finally, if $f(X) = g(X^{p^d})$, where $g(X)$ is separable, then the α_i's above are distinct and so are the β_i's. Hence, each root of $f(X)$ has multiplicity p^d. □

9.1.6.2 Separable extensions

The terminology examined in the previous part now extends to the language of field extensions.

Definition 9.1.58. *If E/K is an extension and $\alpha \in K$, we say that α is **separable over** K if the minimal polynomial of α over K is separable; otherwise, it is inseparable. Also, the **radical exponent** of α over K is the radical exponent of* $\min(\alpha, K)$. *An algebraic field extension E/K is **separable** if every $\alpha \in K$ is separable over K.*

In particular, algebraic extensions of $\mathbb{Q}$ (or any field of characteristic zero) and of every finite field are necessarily separable.

Before proceeding, we record a useful lemma. If E is a field and $S \subseteq E$ then S^n denotes the set $\{s^n : s \in S\}$.

Lemma 9.1.59. *Let E/K be algebraic with* $\mathrm{char}(K) = p \neq 0$ *and let $S \subseteq E$.*

(i) $K(S) = K(S^{p^n})$ holds for some $n \geq 1$ if and only if it holds for all $n \geq 1$.

(ii) $K = K^{p^n}$ holds for some $n \geq 1$ if and only if it holds for all $n \geq 1$.

Proof. For part (i), suppose that $K(S) = K(S^{p^n})$ holds for some $n \geq 1$. Since

$$K(S) = K(S^{p^n}) \subseteq K(S^p) \subseteq K(S).$$

it follows that $K(S^p) = K(S)$. Now, since $[K(S)]^p = K^p(S^p)$, we have for any $n \geq 1$,

$$[K(S)]^{p^n} = K^{p^n}(S^{p^n})$$

and so

$$K(S^{p^n}) = K(K^{p^n}(S^{p^n})) = K([K(S)]^{p^n}) = K([K(S^p)]^{p^n}) = K(K^{p^n}(S^{p^{n+1}})) = K(S^{p^{n+1}}).$$

Hence, $K(S) = K(S^{p^n})$ for all $n \geq 1$. The converse part is obvious.

For part (ii), we observe that $K^{p^n} \subseteq K^p \subseteq K$ and so $K = K^{p^n}$ holds for some $n \geq 1$ if and only if $K = K^p$, which holds if and only if $K = K^{p^n}$ for all $n \geq 1$. □

According to Proposition 9.1.31, the number of extensions of an embedding $\sigma : K \to L$ to $K(\alpha)$, where L is algebraically closed, is equal to the number of distinct roots of $\min(\alpha, K)$. Hence, as we remarked earlier, the size of $\mathrm{Hom}_\sigma(K(\alpha), K)$ does not depend on either σ or L. The same is true for extensions of σ to any algebraic extension.

Theorem 9.1.60. *If E/K is algebraic and $\sigma : K \to L$, where L is algebraically closed, then the cardinality of* $\mathrm{Hom}_\sigma(E, L)$ *depends only on the extension E/K and not on σ or L. In other words, if $\tau : K \to L'$, with L' algebraically closed, then*

$$|\mathrm{Hom}_\sigma(E, L)| = |\mathrm{Hom}_\tau(E, L')|$$

as cardinal numbers.

Proof. Since for any $\bar{\sigma} \in \mathrm{Hom}_\sigma(E, L)$, the image $\bar{\sigma}(E)$ is contained in an algebraic closure of $\sigma(K)$, we may assume that L is an algebraic closure of $\sigma(K)$, and similarly, that L' is an algebraic closure of $\tau(K)$.

Since $\tau \circ \sigma^{-1} : \sigma(K) \to \tau(K)$ is an isomorphism and $K \subseteq L$ is algebraic, the map $\tau \circ \sigma^{-1}$ can be extended to an embedding of L into L'. Since $\bar{\sigma}(K) \subseteq L$ is algebraic, so is its image under λ, which is $\tau(K) \subseteq L'$, and since $\lambda(L)$ is algebraically closed, we have $\lambda(L) = L'$, implying that λ is an isomorphism.

$$\begin{tikzcd}
L' & & L \arrow[ll, "\lambda=\overline{\tau\circ\sigma^{-1}}"'] \\
& E \arrow[ul, "\lambda\circ\bar{\sigma}"] \arrow[ur, "\bar{\sigma}"'] & \\
\tau(K) \arrow[uu] & K \arrow[l, "\tau"'] \arrow[r, "\sigma"] \arrow[u] & \sigma(K) \arrow[uu]
\end{tikzcd}$$

Now, if $\bar{\sigma} \in \mathrm{Hom}_\sigma(E, L)$, then the map $\lambda \circ \bar{\sigma}$ is an embedding of E into L' extending τ on K. This defines a function from $\mathrm{Hom}_\sigma(E, L)$ to $\mathrm{Hom}_\tau(E, L')$ given by $\bar{\sigma} = \lambda \circ \bar{\sigma}$. Moreover, if $\tau, \mu \in \mathrm{Hom}_\sigma(E, L)$ are distinct, then there is a $\beta \in E$ for which $\tau(\beta) \neq \mu(\beta)$ and since λ is injective, $\lambda(\tau(\beta)) = \lambda(\mu(\beta))$, which implies that the map $\bar{\sigma} \mapsto \lambda \circ \bar{\sigma}$ is injective. Hence,

$$|\mathrm{Hom}_\sigma(E, L)| \leq |\mathrm{Hom}_\tau(E, L')|.$$

By a symmetric argument, we have the reverse inequality and so equality holds. □

In view of Theorem 9.1.60, we may make the following definition.

Definition 9.1.61. *Let E/K be algebraic and let $\sigma : K \to L$, where L is algebraically closed. The cardinality of the set* $\mathrm{Hom}_\sigma(E, L)$ *is called the* ***separable degree*** *of E over K and is denoted by $[E : K]_s$.*

This new terminology allows us to rephrase the situation for simple extensions.

Theorem 9.1.62 (Separable degree of simple extensions). *Let E/K and let $\alpha \in E$ be algebraic over K, with minimal polynomial $f(X)$. Then*

(a) If α is separable then

$$[K(\alpha) : K]_s = [K(\alpha) : K].$$

(b) If α is inseparable with radical exponent d, then

$$[K(\alpha) : K]_s = \frac{1}{p^d}[K(\alpha) : K],$$

and then extension $K(\alpha^{p^d})$ is separable over K.

Proof. This comes from Proposition 9.1.31 and Corollary 9.1.57. □

We would like to recast separability of simple and finite extensions entirely in the light of separable degree. First of all, we need to establish that the separable degree is multiplicative.

Theorem 9.1.63. *Let $K \subseteq E \subseteq F$ be algebraic extensions. Then*

$$[F : K]_s = [F : E]_s[E : K]_s.$$

Proof. Let $\iota : K \to \bar{F}$ be the canonical inclusion map. Then the set $\mathrm{Hom}_\iota(E, \bar{F})$ consists of extensions of ι to an embedding $\bar{\iota} : E \to \bar{F}$ and has cardinality $[E : K]_s$. Each extension $\sigma \in \mathrm{Hom}_\iota(E, \bar{F})$ is an embedding of E into $\bar{F}$ and can be further extended to an embedding of F into $\bar{F}$. Since the resulting extensions, of which there are $[F : E]_s[E : K]_s$, are distinct extensions of ι to E, we have

$$[F : K]_s \geq [F : E]_s[E : K]_s.$$

On the other hand, if $\sigma \in \mathrm{Hom}_\iota(F, \bar{F})$ then $\sigma|_E$ is the extension of E to $\bar{F}$, hence an element of $\mathrm{Hom}_\iota(E, \bar{F})$. Since σ is an extension of $\sigma|_E$ to F, we see that σ is obtained by a double extension of $\iota : K \to \bar{F}$ and so equality holds in the inequality above. □

Proposition 9.1.64 (Separability of simple extensions). *Let E/K be algebraic, with* $\mathrm{char}(K) = p \neq 0$. *The following are equivalent.*

(i) *α is separable over K.*

(ii) *$K(\alpha)$ is a separable extension over K.*

(iii) $[K(\alpha) : K]_s = [K(\alpha) : K]$.

(iv) *There is a positive integer n for which $K(\alpha) = K(\alpha^{p^n})$, in which case $K(\alpha) = K(\alpha^{p^n})$ for all n.*

If α is inseparable with radical exponent d, then

$$[K(\alpha) : K]_s = \frac{1}{p^d}[K(\alpha) : K].$$

Proof. By Theorem 9.1.62 we now that $(i) \Leftrightarrow (iii)$. Let α be separable and $\beta \in K(\alpha)$, then we have the tower

$$K \subseteq K(\beta) \subseteq K(\alpha).$$

The separable degree and the ordinary (vector space) degree are multiplicative and, at least for simple extensions, the separable degree does not exceed the ordinary degree. Hence, $[K(\alpha) : K]_s = [K(\alpha) : K]$ implies that the same is true for each step in the tower, and so $[K(\beta) : K]_s = [K(\beta) : K]$, which means β is separable over K.

Now we prove $(i) \Rightarrow (iv)$. Assume that α is separable. Note that α is a root of the polynomial $f(X) = X^p - \alpha^p = (X - \alpha)^p$ over $K(\alpha^p)$, and so $\min(\alpha, K(\alpha^p))$ divides $(X - \alpha)^p$. Since α is separable over K, it is also separable over $K(\alpha^p)$, which the implies

$$\min(\alpha, K(\alpha^p)) = x - \alpha.$$

Hence $\alpha \in K(\alpha^p)$. By Lemma 9.1.59 we conclude that (iii) holds.

Conversely, assume that $K(\alpha^{p^n}) = K(\alpha)$ for all $n \geq 1$. Let d be the radical exponent of α, then $K(\alpha^{p^d}) = K(\alpha)$. But $K(\alpha^{p^d})$ is a separable extension, therefore α is separable. This completes the proof. □

Proposition 9.1.65 (Separability of finite extensions). *Let E/K be a finite extension. Then $[E : K]_s \leq [E : K]$, and the following are equivalent:*

(i) *$E = K(\alpha_1, \ldots, \alpha_r)$, where each α_i is separable over K.*

(ii) E/K *is separable.*

(iii) $[E : K] = [E : K]_s$.

(iv) If $E = K(S)$ *for a finite set* $S \subseteq E$*, then* $K(S) = K(S^{p^n})$ *for some* $n \geq 1$*, in which case* $K(S) = K(S^{p^n})$ *for all* $n \geq 1$.

If E/K *is not separable, then*

$$[E : K]_s = \frac{1}{p^e}[E : K]$$

for some integer $e \geq 1$.

Proof. Since E is finite over K, it is finitely generated. Let $F = K(\alpha_1, \ldots, \alpha_r)$. Then using Theorem 9.1.62, Theorem 9.1.63, and Proposition 9.1.17,

$$\begin{aligned}[E : K]_s &= [K(\alpha_1, \ldots, \alpha_{r-1})(\alpha_r) : K(\alpha_1, \ldots, \alpha_{r-1})]_s \cdots [K(\alpha_1) : K]_s \\ &\leq [K(\alpha_1, \ldots, \alpha_{r-1})(\alpha_r) : K(\alpha_1, \ldots, \alpha_{r-1})] \cdots [K(\alpha_1) : K] = [E : K].\end{aligned}$$

This proves the stated inequality.

First we show (i)⇒(iii). If each α_i is separable over K, then it is separable over the field $K(\alpha_1, \ldots, \alpha_{i-1})$, so the inequality above is an equality. For (iii)⇒(ii), assume $[E : K]_s = [E : K]$, and let $\alpha \in E$. We have $K \subseteq K(\alpha) \subseteq E$; hence by Theorem 9.1.63

$$[E : K(\alpha)]_s[K(\alpha) : K]_s = [E : K]_s = [E : K] = [E : K(\alpha)][K(\alpha) : K].$$

Since both separable degrees are less than or equal to their plain counterparts, the equality implies

$$[K(\alpha) : K]_s = [K(\alpha) : K]$$

proving that α is separable, by Theorem 9.1.62. Therefore the extension E/K is separable. Now if $[E : K]_s = [E : K]$ and $E = K(\alpha_1, \ldots, \alpha_n)$, then the inequality becomes an equality, and so each α_i is separable over K, so (i) holds.

Finnaly, we prove $(ii) \Leftrightarrow (iv)$. Let $E = K(S)$ where S is a finite set. If E is separable, then any $\alpha \in E$ is separable over K and so

$$K(\alpha) = K(\alpha^{p^n}) \subseteq K(S^{p^n}).$$

for any $n \geq 1$. Thus, $K(S) = K(S^{p^n})$, for any $n \geq 1$. Conversely, if $K(S^{p^n}) = K(S)$ for some $n \geq 1$, then Lemma 9.1.59 implies that $K(S) = K(S^{p^n})$ for all $n \geq 1$. Since S is a finite set, we can take p^n to be the maximum of the numbers p^d, where d varies over all radical exponents of the elements of S, in which case each α^{p^d} is separable, and so $K(S^{p^n})$ is separable. Since $K(S) = K(S^{p^d})$, it is also separable. □

Finally, we consider the separability of algebraic extensions.

Proposition 9.1.66 (Separability of algebraic extensions). *Let* E/K *be algebraic and* $\mathrm{char}(K) = p \neq 0$.

(a) E *is separable if and only if it is generated by separable elements over* K.

(b) If E is separable and $E = K(S)$, then $K(S) = K(S^{p^n})$ for all $n \geq 1$.

Proof. For part (a), if E/K is separable then E is generated by itself over K. For the converse, assume that $E = K(S)$ where each $\alpha \in S$ is separable over K and let $\beta \in E$. Then $\beta \in K(S_0)$ for some finite subset $S_0 \subseteq S$. Since $K(S_0)$ is finitely generated and algebraic, it is finite. Thus, Proposition 9.1.65 implies that $K(S_0)$ is separable. Hence β is separable over K and so E is separable. As to part (b), we have for any $\alpha \in S$ $n \geq 1$

$$K(\alpha) = K(\alpha^{p^n}) \subseteq K(S^{p^n})$$

which implies that $K(S) \subseteq K(S^{p^n})$ and so $K(S) = K(S^{p^n})$. □

Using our characterization of separable extensions, we may now establish that the class of separable extensions is distinguished.

Proposition 9.1.67. *The class of separable extensions is distinguished and is also closed under the taking of arbitrary composites.*

Proof. For the tower property, if the full extension in $K \subseteq E \subseteq F$ is separable, then by definition so is $K \subseteq E$. As for the extension $E \subseteq F$, for any $\alpha \in F$, we have

$$\min(\alpha, K) \mid \min(\alpha, E),$$

and so α separable over K implies α separable over E, hence $E \subseteq F$ is separable. Conversely, suppose now that $K \subseteq E$ and $E \subseteq F$ are separable and let $\alpha \in F$. Let $S \subseteq E$ be the set of coefficients of $\min(\alpha, E)$. Then $\min(\alpha, E) = \min(\alpha, K(S))$ and so α is separable over $K(S)$. It follows that each step in the tower $K \subseteq K(S) \subseteq K(S, \alpha)$ is finite and separable, implying that α is separable over K. Hence, F is separable.

For the lifting property, let $K \subseteq E$ be separable and let $K \subseteq F$. Since every element of E is separable over K, it is also separable over the larger field F. Hence $EF = F(E)$ is separably generated and is therefore separable (Proposition 9.1.66).

The fact that separable extensions are closed under the taking of arbitrary composites follows from the finitary property of arbitrary composites. That is, each element of an arbitrary composite involves elements from only a finite number of the fields in the composite and so is an element of a finite composite, which is separable. □

9.1.6.3 Perfect fields

It is intersecting to consider certain condition on fields that guarantees the inseparability of its extensions. We make the following definition.

Definition 9.1.68. *A field K is **perfect** if every irreducible polynomial over K is separable.*

The following property of perfect fields is immediate from definition.

Proposition 9.1.69. *A field K is perfect if and only if every algebraic extension of K is separable over K.*

Proof. It is clear from the definitions that if K is perfect then any algebraic extension of K is separable. Conversely, suppose that every algebraic extension of K is separable. If $f(X) \in K[X]$

is irreducible and α is a root of $f(X)$ in some extension of K, then $K \subseteq K(\alpha)$ is algebraic and so α is separable over K, that is, $f(X)$ is separable. Thus, K is perfect. □

It is clear that fields with characteristic zero must be perfect. Also, we will prove later that finite fields are all perfect. Therefore if K is not a perfect field, it must be infinite and have nonzero characteristic.

Definition 9.1.70. *Let K be a field of characteristic $p > 0$. The* ***Frobenius homomorphism*** *is the map $\sigma : K \to K$ defined by $x \mapsto x^p$.*

The Frobenius homomorphism may not look like a homomorphism of rings, but it is. It must be injective, as is every nontrivial ring homomorphism from a field; but it is not necessarily surjective. In fact, it is surjective if and only if the field is perfect.

Proposition 9.1.71. *Let K be a field with characteristic $p > 0$. The following are equivalent.*

(i) K is perfect.

(ii) $K = K^{p^n}$ for some $n \geq 1$.

(iii) The Frobenius homomorphism is an automorphism for K.

Proof. Suppose K is perfect. Let $\alpha \in K$ and consider the polynomial $f(X) = X^p - \alpha$. If β is a root of $f(X)$ in a splitting field then $\beta^p = \alpha$ and so

$$f(X) = X^p - \beta^p = (X - \beta)^p$$

Now, if $g(X) = (X - \beta)^e$ is an irreducible factor of $f(X)$ over K, then it must be separable and so $e = 1$. Thus $\beta \in K$, that is, $\alpha = \beta^p \in K^p$ and so $K \subseteq K^p$. Since the reverse inclusion is manifest, we have $K = K^p$. Then (ii) follows from Lemma 9.1.59.

Now assume that (ii) holds. Then Lemma 9.1.59 implies that $K = K^p$. Suppose that $f(X) \in K[X]$ is irreducible. If $f(X)$ is not separable, then

$$f(X) = g(X^p) = \sum_i a_i (X^p)^i = \sum_i b_i^p (X^i)^p = \sum_i (b_i X^i)^p$$

contradicting the fact that $f(X)$ is irreducible. Hence, every irreducible polynomial is separable and so K is perfect. Thus, (ii) implies (i). Since the Frobenius map is a monomorphism, statement (ii), which says that σ^n is surjective, is equivalent to statement (iii). □

Example 9.1.72. Let p be a prime. Then the field $\mathbb{F}_p$ is finite and hence perfect. However, if t is an independent variable, then the field $\mathbb{F}_p(t)$ is not perfect, as we have seen in Example 9.1.52.

While it is true that any algebraic extension of a perfect field is perfect, not all subfields of a perfect field need be perfect.

Proposition 9.1.73. *Let $K \subseteq E$ be an algebraic extension.*

(a) If K is perfect then E is also perfect.

(b) If E/K is finite and E is perfect, then K is perfect.

Proof. Part (a) follows from Proposition 9.1.69 and the fact that every algebraic extension of E is an algebraic extension of K.

For part (ii), let $p = \text{char}(K)$ and suppose first that $K \subseteq E$ is simple. Thus, $E = K(\alpha)$ is perfect and α is algebraic over K. Since $K(\alpha)$ is perfect, we have $K(\alpha) = [K(\alpha)]^p = K^p(\alpha^p)$. Consider the tower

$$K^p \subseteq K \subseteq K(\alpha) = K^p(\alpha^p).$$

If $f(X) = \sum_i a_i X^i$ is the minimal polynomial of α over K, then

$$0 = \Big(\sum_i a_i \alpha^i\Big)^p = \sum_i a_i^p \alpha^{pi}$$

and so $[K^p(\alpha^p) : K^p] \leq [K(\alpha) : K] = 1$. It follows that in the tower above, $[K : K^p] = 1$, that is, $K = K^p$, whence K is perfect. Since E is finitely generated by algebraic elements, the result follows by repetition of the previous argument. □

Note that we cannot drop the finiteness condition in part (b) of the previous theorem since, for example, the extension $K \subseteq \overline{K}$ is algebraic and $\overline{K}$ is perfect for any field K, even if K is not.

9.1.6.4 Purely inseparability

The antithesis of a separable element is a purely inseparable element.

Definition 9.1.74. *An element α algebraic over K is **purely inseparable** over K if its minimal polynomial has the form $(X - \alpha)^n$ for some $n \geq 1$. An algebraic extension E/K is **purely inseparable** if every element of E is purely inseparable over K.*

It is clear that for a purely inseparable element E, an element $\alpha \in K$ is separable if and only if $\min(\alpha, K) = x - \alpha$; that is, $\alpha \in K$. In particular, for extensions of fields of characteristic 0 or finite fields, there are no "interesting" purely inseparable elements.

Lemma 9.1.75. *Let E/K be a purely inseparable extension with $p = \text{char}(K) \neq 0$. If $\alpha \in E$ is inseparable over K and d is the radical exponent of α, then the minimal polynomial of α over K is $(X - \alpha)^{p^d}$.*

Proof. By definition, $\min(\alpha, K) = (X - \alpha)^n$ for some $n \geq 1$. For $\alpha \notin K$. Since the coefficient of X^{n-1} in $(X - \alpha)^n$ is $-n\alpha$, it follows that n must be a multiple of p, that is,

$$\min(\alpha, K) = (X - \alpha)^{mp^e}.$$

But $\min(\alpha, K) = g(X^{p^d})$, hence $e \geq d$ and we can write

$$\min(\alpha, K) = (X^{p^d} - \alpha^{p^d})^{mp^{e-d}}.$$

which implies that $g(X) = (X - \alpha^{p^d})^{mp^{e-d}}$, which is separable if and only if $m = 1$ and $e = d$. Thus,

$$\min(\alpha, K) = (X - \alpha)^{p^d}$$

where d is the radical exponent of α over K. □

Example 9.1.76. Let $\mathrm{char}(K) = p$. If t is transcendental over K, then t is purely inseparable over $K(t^p)$, since its minimal polynomial over $K(t^p)$ is $X^p - t^p = (X - t)^p$.

Example 9.1.77. Here we present an example of an element that is neither separable nor purely inseparable over a field K. Let $\mathrm{char}(K) = p$ and let $\alpha \in K$ be nonzero. Let t be transcendental over K and let

$$s = \frac{t^{p^2}}{t^p + \alpha}.$$

According to Proposition 9.4.15, $K(s) \subseteq K(t)$ is algebraic and has degree equal to p^2, and the monic polynomial

$$p(X) = X^{p^2} - sX^p - s\alpha$$

is the minimal polynomial for t over $K(s)$. Since $p(X) = q(X^p)$, we deduce that t is not separable over $K(s)$. On the other hand, if t were purely inseparable over $K(s)$, we would have

$$X^{p^2} - sX^p - s\alpha = (X - t)^{p^2} = X^{p^2} - t^{p^2}$$

which would imply that $s = 0$, which is not the case. Hence, t is neither separable nor purely inseparable over $K(s)$.

Definition 9.1.78. *Let E/K be a finite extension. Since $[E : K]_s \mid [E : K]$, we may write*

$$[E : K] = [E : K]_i [E : K]_s$$

*where $[E : K]_i$ is the **inseparable degree** of E over K.*

Note that while the separable degree is defined for arbitrary extensions, the inseparable degree is defined only for finite extensions.

Now we assemble some properties of the inseparable degree.

Proposition 9.1.79. *Let $K \subseteq E \subseteq F$ be a finite extensions with* $\mathrm{char}(K) = p \neq 0$.

(a) $[F : K]_i = [F : E]_i [E : K]_i$.

(b) E/K is separable if and only if $[E : K]_i = 1$.

(c) If $\alpha \in E$ then $[K(\alpha) : K] = p^d$, where d is the radical exponent of α over K.

(d) $\alpha \in E$ is purely inseparable if and only if $[K(\alpha) : K]_s = 1$, if and only if $[K(\alpha) : K]_i = [K(\alpha) : K]$.

(e) $[E : K]_i$ is a power of p.

Proof. The first three statements are clear. Also, (d) follows from the fact that α is purely inseparable if and only if its minimal polynomial has only one distinct root. But this is equivalent to saying that $\mathrm{Hom}_K(K(\alpha), \overline{K})$ has cardinality 1. Finally, (e) follows from the fact that E/K is finitely generated and the inseparable degree is multiplicative. □

We next characterize purely inseparable elements.

Proposition 9.1.80 (Purely inseparable elements). *Let* $\mathrm{char}(K) = p \neq 0$. *Let α be algebraic over K, with radical exponent d and let $f(X) = \min(\alpha, K)$. The following are equivalent.*

(i) α *is purely inseparable over* K.

(ii) $K \subseteq K(\alpha)$ *is a purely inseparable extension.*

(iii) $\alpha^{p^n} \in K$ *for some* $n \geq 1$.

Proof. If (i) holds and $\beta \in K(\alpha)$, then in the tower $K \subseteq K(\beta) \subseteq K(\alpha)$ the inseparable degree of the full extension is equal to the degree, and so the same holds for the lower step. Hence, β is purely inseparable over K and (ii) holds. Clearly, (ii) implies (i).

If (i) holds, then $\min(\alpha, K) = X^{p^d} - \alpha^{p^d}$, which implies (iii). If (iii) holds, then $\min(\alpha, K) = X^{p^n} = \alpha^{p^n}$ and, as we have seen, α is purely inseparable. □

One may translate our results into the following remark. Let α be element in E, then we have the following tower of extensions:

$$K(\alpha) \supseteq K(\alpha^p) \supseteq \cdots \supseteq K(\alpha^{p^n}) \supseteq \cdots \supseteq K.$$

Then Theorem 9.1.62 says that if α is separable, then this tower is trivial, with the field all being $K(\alpha)$; and if α is inseparable, then this tower is descending. Now Proposition 9.1.80 tells us α is purely inseparability condition if and only if this twoer arrives at K. Note that Example 9.1.77 shows that there are cases where the tower is descending but never arrives at K.

The following result is the analogue of Proposition 9.1.66.

Proposition 9.1.81 (Purely inseparable extensions). *Let* E/K *be algebraic. The following are equivalent.*

(i) E *is* ***purely inseparably generated****; that is, generated by purely inseparable elements.*

(ii) E/K *is* ***degreewise purely inseparable****, that is,* $[E : K]_s = 1$.

(iii) E/K *is a purely inseparable extension.*

Proof. To prove that (i) implies (ii), suppose that $E = K(I)$, where all elements of I are purely inseparable over K. Let $\sigma : K \to L$ be an embedding to an algebraic closed field L. Then any $\tau \in \mathrm{Hom}_\sigma(E, L)$ is uniquely determined by its values on the elements of I. But if $\alpha \in I$ then $\tau(\alpha)$ is a root of the minimal polynomial $\min(\alpha, K) = (X - \alpha)^n$ and so $\tau(\alpha) = \alpha$. Hence τ must be the identity and therefore $[E : K]_s = 1$.

To show that (ii) implies (iii), let $\alpha \in E$ and suppose that β is a root of $\min(\alpha, K)$ in $\overline{K}$. Then by Theorem 9.1.32 the identity on K can be extended to an embedding $\sigma : E \to \overline{K}$, for which $\sigma(\alpha) = \beta$. Since $[E : K]_s = 1$, we must have $\sigma = \mathrm{id}$ and so $\beta = \alpha$. Thus, $\min(\alpha, K)$ has only one distinct root in $\overline{K}$ and so E is purely inseparable. It is clear that (iii) implies (i). □

Similarly to separable extensions, We can show that the class of purely inseparable extensions is distinguished.

Proposition 9.1.82. *The class of purely inseparable extensions is distinguished. It is also closed under the taking of arbitrary composites.*

Proof. Let $K \subseteq E \subseteq F$ be finite extensions. Since pure inseparability is equivalent to degreewise pure inseparability and $[F : K]_i = 1$ if and only if $[E : K]_i = 1$ and $[F : E]_i = 1$, it is clear that the tower property holds. For lifting, suppose that $K \subseteq E$ is purely inseparable and $K \subseteq F$. Since

every element of E is purely inseparable over K, it is also purely inseparable over the larger field F. Hence $EF = F(E)$ is purely inseparably generated and therefore purely inseparable.

The fact that purely inseparable extensions are closed under the taking of arbitrary composites follows from the finitary property of arbitrary composites, as in the separable case. □

9.1.6.5 Separable and purely inseparable closures

Let $K \subseteq E$ be an extension. Recall that the algebraic closure of K in E is the set $\overline{K}$ of all elements of E that are algebraic over E. The fact that $\overline{K}$ is a field is a consequence of the fact that an extension that is generated by algebraic elements is algebraic.

We can do exactly the same analysis for separable and purely inseparable elements. To wit, if $\alpha, \beta \in E$ are separable over K, then $K(\alpha, \beta)$ is separable over K. It follows that $\alpha \pm \beta$, $\alpha\beta$ and $\alpha\beta^{-1}$ are separable over K. Hence, the set of all elements of E that are separable over K is a subfield of E. A similar statement holds for separable and purely inseparable elements.

Definition 9.1.83. *Let E/K be algebraic. The field*

$$K^{\text{sep}} = \{\alpha \in E : \alpha \text{ is separable over } K\}$$

*is called the **separable closure** of K in E. The field*

$$K^{\text{isep}} = \{\alpha \in E : \alpha \text{ is purely inseparable over } K\}$$

*is called the **purely inseparable closure** of K in E.*

The separable closure allows us to decompose an arbitrary algebraic extension into separable and purely inseparable parts.

Proposition 9.1.84. *Let E/K be algebraic.*

(a) In the tower $K \subseteq K^{\text{sep}} \subseteq E$, the first step is separable and the second step is purely inseparable.

(b) Any automorphism σ of E over K is uniquely determined by its restriction to K^{sep}.

Proof. For (a), if $\alpha \in E \setminus K$ has radical exponent d, then α^{p^d} has a separable minimal polynomial and is therefore in K^{sep}. Thus, Proposition 9.1.80 implies that α is purely inseparable over K^{sep}. For (b), let α be purely inseparable over K, then any automorphism σ of E must send α to a root of $\min(\alpha, K) = (X - \alpha)^n$, and so $\sigma|_{K^{\text{isep}}}$ is the identify. □

Corollary 9.1.85. *Let E/K be finite, then $[E : K]_s = [K^{\text{sep}} : K]$ and $[E : K]_i = [E : K^{\text{isep}}]$.*

Proof. The first equality follows from part (b) of Proposition 9.1.84, and the second follows from the definition of $[E : K]_i$. □

Corollary 9.1.86. *If E/K is normal, then K^{sep}/K is also normal.*

Proof. Let σ be an embedding of K^{sep} in $\overline{K}$ over K and extend σ to an embedding of E. Then σ is an automorphism of E by Theorem 9.1.30. Furthermore, $\sigma(K^{\text{sep}})$ is separable over K, hence is contained in K^{sep}. Hence $\sigma(K^{\text{sep}}) = K^{\text{sep}}$, as contended. □

Proposition 9.1.84 shows that any algebraic extension can be decomposed into a separable extension followed by a purely inseparable extension. In general, the reverse is not possible: an algebraic extension can not be decomposed into a purely inseparable extension followed by a separable extension. This is because, although $K \subseteq K^{\text{isep}}$ is purely inseparable, the elements of $E \setminus K^{\text{isep}}$ need not be separable over K^{isep}; they are simply not purely inseparable over K. However, we do have a characterization for the extension $K^{\text{isep}} \subseteq E$ to be separable. For this we need a lemma.

Lemma 9.1.87. *Let E, F be two finite extensions of K, and assume that E/K is separable, F/K is purely inseparable. Assume E, F are subfields of a common field. Then*

$$[EF : F] = [E : K] = [EF : K]_s, \quad [EF : E] = [F : K] = [EF : K]_i.$$

Proof. In fact, we have the following picture:

$$\begin{tikzcd}
 & EF \arrow[dl, dash, "\text{p isep}"'] \arrow[dr, dash, "\text{sep}"] & \\
E \arrow[dr, dash, "\text{sep}"'] & & F \arrow[dl, dash, "\text{p isep}"] \\
 & K &
\end{tikzcd}$$

Since separable and purely inseparable extensions are distinguished, the extension EF/E is purely insepara and EF/F is separable. Therefore, by Proposition 9.1.66 and Proposition 9.1.81, we have

$$[EF : K]_s = [EF : F]_s [F : K]_s = [EF : F]_s = [EF : F],$$

and the claim for inseparable degree can be proved similarly. □

Proposition 9.1.88. *Let E/K be an algebraic extension. Then the extension E/K^{isep} is separable if and only if we have $E = K^{\text{sep}} K^{\text{isep}}$.*

Proof. Consider the following diagram of extensions

$$\begin{tikzcd}
 & E \arrow[d, dash] & \\
 & K^{\text{sep}} K^{\text{isep}} \arrow[dl, dash, "\text{p isep}"'] \arrow[dr, dash, "\text{sep}"] & \\
K^{\text{sep}} \arrow[dr, dash, "\text{sep}"'] & & K^{\text{isep}} \arrow[dl, dash, "\text{p isep}"] \\
 & K &
\end{tikzcd}$$

We already know that E/K^{sep} is purely inseparable, and so $E/K^{\text{sep}} K^{\text{isep}}$ is also purely inseparable. If E/K^{isep} is separable, then $E/K^{\text{sep}} K^{\text{isep}}$ is also separable, hence we get $E = K^{\text{sep}} K^{\text{isep}}$. The converse is trivial from the diagram above. □

We can obtain further results in the setting of Proposition 9.1.88 when E/K is a normal extension, which includes the case $E = \overline{K}$. Let $G = \text{Aut}_K(E)$ be the set of all automorphisms of E over K. Since E is normal, G is also the set of all embeddings of E into $\overline{K}$ over K. We define

the **fixed field** of G in E by

$$E^G = \{\alpha \in E : \sigma(\alpha) = \alpha \text{ for all } \sigma \in G\}.$$

Proposition 9.1.89. *Let E be normal over K, G its group of automorphisms over K, and E^G the fixed field of G. Then $E^G = K^{\mathrm{isep}}$, the extension E/K^{isep} is separable, and we have $E = K^{\mathrm{sep}}K^{\mathrm{isep}}$.*

Proof. Let $\alpha \in E^G$. If $\beta \in \overline{K}$ is conjugate to α then there exists an embedding $\sigma : E \to \overline{K}$ over K for which $\sigma(\alpha) = \beta$. But $\sigma(\alpha) = \alpha$ by the definition of E^G, and so $\beta = \alpha$. Hence the minimal polynomial of α has only one root and $\alpha \in K^{\mathrm{isep}}$. On the other hand, if $\alpha \in K^{\mathrm{isep}}$ then any $\sigma \in G$ must map σ to itself (Proposition 9.1.84). Hence $\alpha \in E^G$. This proves that $E^G = K^{\mathrm{isep}}$.

Now let $\alpha \in E$ and $f(X) = \min(\alpha, E^G)$. Let $g(X) = \prod(X - r_i)$ where $R = \{r_1, \dots, r_n\}$ is the set of *distinct* roots of $f(X)$ in E. Since any $\sigma \in G$ is a permutation of R, we deduce that $g^\sigma(X) = g(X)$ and so the coefficients of $g(X)$ lie in E^G. Hence $f(X) = g(X)$ and α is separable over E^G. □

9.1.6.6 Existence of primitive elements

We wish now to describe conditions under which a finite extension is simple. The most famous result along these lines is the theorem of the primitive element, which states that a finite separable extension is simple.

Theorem 9.1.90 (Theorem of the primitive element).

(a) Any extension of the form

$$K \subseteq K(\alpha_1, \dots, \alpha_n, \beta)$$

where α_i is separable over K and β is algebraic over K is a simple extension. Moreover, if K is infinite, this extension has infinitely many primitive elements, of the form $c_1\alpha_1 + \cdots + c_n\alpha_n + \beta$, where $c_1, \dots, c_n \in K$.

(b) For any finite extension $K \subseteq E$, there exists a $\beta \in E$ such that

$$[K(\beta) : K] = [E : K]_s.$$

If K is infinite, there exist infinitely many such elements β.

(c) If $K \subseteq E$ is finite and separable, say

$$E = K(\alpha_1, \dots, \alpha_n)$$

where α_i is separable over K, then $K \subseteq E$ is simple. If K is infinite, there exist infinitely many primitive elements for E over K of the form $c_1\alpha_1 + \cdots + c_n\alpha_n$, where $c_i \in K$.

(d) If K has characteristic 0 or if K is a finite field then any finite extension of K is simple.

Proof. If K is a finite field, then so is E, since $[E : K]$ is finite. Hence $E^\times = \langle\beta\rangle$ is cyclic and $K \subseteq E = K(\beta)$ is simple. Let us now assume that K is an infinite field.

For (a), we show that if $E = K(\alpha, \beta)$, with α separable over K and β algebraic over K, then $E = K(\gamma)$, where γ is algebraic over K. The argument can be repeated to obtain a primitive element in the more general case.

Let $f(X) = \min(\alpha, K)$, $g(X) = \min(\beta, K)$, and suppose that the roots of $f(X)$ are $\alpha_1 = \alpha, \ldots, \alpha_s$ and the roots of $g(X)$ are $\beta_1 = \beta, \ldots, \beta_t$. Since $f(X)$ is separable, the roots of $f(X)$ are distinct. However, the roots of $g(X)$ need not be distinct. We wish to show that for infinitely many values of $c \in K$, the elements $c\alpha + \beta$ are primitive. To do this, we need only show that $\alpha \in K(c\alpha + \beta)$, for then $\beta \in K(c\alpha + \beta)$ and so $K(\alpha, \beta) = K(c\alpha + \beta)$.

The polynomial $h(X) = g(c\alpha + \beta - cx)$ has coefficients in $K(c\alpha + \beta)$ and has α as a root. Thus, $f(X)$ and $g(X)$ have the common factor $x - \alpha$ in some extension of K. Moreover, since α is separable, α is a simple root of $f(X)$ and so no higher power of $x - \alpha$ is a factor of $f(X)$. Therefore, if we can choose $c \in K$ so that $f(X)$ and $h(X)$ have no other common roots in any extension of K, then it would follow that $\gcd(f(X), h(X)) = x - \alpha$, which must therefore be a polynomial over $K(c\alpha + \beta)$. In particular, $\alpha \in K(c\alpha + \beta)$, as desired.

The roots of h are the values of x for which $c\alpha + \beta - cx \neq \beta_i$ and we need only choose c so that none of the roots $\alpha_2, \ldots, \alpha_s$ satisfy this equation, that is, we need only choose c so that

$$c \neq \frac{\beta_i - \beta}{\alpha - \alpha_j}$$

for $i = 2, \ldots, t$ and $j = 2, \ldots, s$. Since K is infinite, there are infinitely many $c \in K$ satisfying this condition.

Now (b) follows from (a) by considering the separable closure K^{sep} of E in K. Since $K \subseteq K^{\text{sep}}$ is separable, with $[K^{\text{sep}} : K] = [E : K]_s$, we can apply part (a) to the separable extension K^{sep}/K. Also, (c) is a direct consequence of (a), as is (d). □

Example 9.1.91. Consider the extension $\mathbb{Q} \subseteq \mathbb{Q}(i, \sqrt{2})$. Here we have

$$f(X) = \min(i, \mathbb{Q}) = X^2 + 1, \quad g(X) = \min(\sqrt{2}, \mathbb{Q}) = X^2 - 2.$$

and so $\alpha_1 = i, \alpha_2 = -i$, and $\beta_1 = \sqrt{2}, \beta_2 = -\sqrt{2}$. According to the previous theorem, $ci + \sqrt{2}$ is primitive provided that

$$c \notin \left\{ \frac{\beta_i - \beta}{\alpha - \alpha_2} : i = 1, 2 \right\} = \{0, \sqrt{2}i\}.$$

In particular, we can choose any nonzero $c \in \mathbb{Q}$.

Theorem 9.1.90 is a good illustration of why separability is a technically desirable condition. One may wonder if there is an example of nonsimple extension. To give an example of this, we first provide a nice criterion for simplicity of algebraic extensions.

Proposition 9.1.92. *Let E/K be a finite extension with $[E : K]_i = p^d$. Then E/K is simple if and only if d is the smallest nonnegative integer for which $E^{p^d} \subseteq K^{\text{sep}}$.*

Proof. We have seen that if $K \subseteq E$ is simple then d is the smallest such nonnegative integer. For the converse, note first that if K is a finite field then so is E, implying that $E^\times$ is cyclic and so E/K is simple. Let us assume that K is an infinite field and looK at the second step in the tower $K \subseteq K^{\text{sep}} \subseteq E$. This step is purely inseparable. Since $K^{\text{sep}} \subseteq E$ is finite, we have

$$E = K^{\text{sep}}(\beta_1, \ldots, \beta_n)$$

If for some $e \leq d$, we have $\beta_i^{p^e} \in K^{\text{sep}}$ for all i, then $E^{p^e} \subseteq K^{\text{sep}}$, contrary to the hypothesis.

Hence one of the β_i's, say β, satisfies

$$\beta^{p^d} \in K^{\text{sep}}, \quad \beta^{p^e} \notin K^{\text{sep}} \text{ for } e < d.$$

It follows that

$$[K^{\text{sep}}(\beta) : K^{\text{sep}}]_i = p^d = [E : K]_i \geq [E : K^{\text{sep}}]_i.$$

Since $K^{\text{sep}}(\beta) \subseteq E$, we conclude $[K^{\text{sep}}(\beta) : K^{\text{sep}}]_i = [E : K^{\text{sep}}]_i$, and since the extensions involved are purely inseparable, we get $[K^{\text{sep}}(\beta) : K^{\text{sep}}] = [E : K^{\text{sep}}]$. Hence $E = K^{\text{sep}}(\beta)$.

Our tower now has the form $K \subseteq K^{\text{sep}} \subseteq K^{\text{sep}}(\beta)$ where β is purely inseparable over K^{sep}. In addition, K^{sep}/K is finite and separable and therefore simple. Thus there exist $\alpha \in K^{\text{sep}}$ such that $K^{\text{sep}} = K(\alpha)$ and therefore $E = K(\alpha, \beta)$, where α is separable over K and β is purely inseparable over $K(\alpha)$. By Theorem 9.1.90, the extension $K \subseteq K(\alpha, \beta)$ is simple. □

Example 9.1.93. By Theorem 9.1.90, if we want to construct a nonsimple finite extension, we have to use inseparable elements. Consider the extension E/K, where

$$K = \mathbb{F}_p(u^p, v^p), \quad E = \mathbb{F}_p(u, v).$$

The minimal polynomial of s over K is $X^p - u^p$ and the minimal polynomial of t over $\mathbb{F}_p(u, v^p)$ is $y^p - v^p$, so it follows that E/K is purely inseparable and $[E : K]_i = [E : K] = p^2$. Since $E^p \subseteq \mathbb{F}_p(u, v) = K$, by Proposition 9.1.92 the extension E/K is not simple.

Note that E/K has infinitely many intermediate fields: if there are $c, c' \in K$ such that $K(cu + v) = K(c'u + v)$, then we may conclude that $K(u, v) = K(cu + v)$, and in particular

$$[K(cu + v) : K] = p^2.$$

But this is not the case, since $(cu + v)^p = c^p u^p + v^p \in K(u^p, v^p) = K$; hence the minimal polynomial of $cu + v$ over K has degree at most p. Since $K = \mathbb{F}_p(u^p, v^p)$ is infinite, there are infinitely many intermediate fields, and it follows that E is not a simple extension of K.

9.1.6.7 Linearly disjointness

Let E and F be two extensions of a field K. By a **composite extension** of E and F we refer to any triple (L, ϕ, ψ), where L is an extension of K, ϕ is a K-homomorphism of E into L and ψ is a K-homomorphism of F into L, and where the field L is generated by $\phi(E) \cup \psi(F)$.

$$\begin{tikzcd}
 & L & \\
E \arrow[ur, "\phi"] \arrow[dr] & & F \arrow[ul, "\psi"'] \arrow[dl] \\
 & K &
\end{tikzcd}$$

By an **isomorphism** of a composite extension (L, ϕ, ψ) of E and F onto a composite extension (L', ϕ', ψ') of E and F we mean a K-isomorphism σ of L onto L' such that $\phi' = \sigma \circ \phi$ and $\psi' = \sigma \circ \psi$.

Let (L, ϕ, ψ) be a composite extension of E and F. The K-linear mapping of $E \otimes_K F$ into L which sends $x \otimes y$ to $\phi(x)\psi(y)$ is a K-algebra homomorphism; in this part, we shall denote it

by $\phi * \psi$. Its image is the subring of L generated by $\phi(E) \cup \psi(F)$.

Proposition 9.1.94. *Let E and F be two extensions of K.*

(a) Let (L, ϕ, ψ) be a composite extension of E and F; then the kernel $\mathfrak{p}$ of the homomorphism $\phi * \psi$ of $E \otimes_K F$ into L is a prime ideal.

(b) Let $\mathfrak{p}$ be a prime ideal of $E \otimes_K F$; then there exists a composite extension (L, ϕ, ψ) of E and F such that $\mathfrak{p}$ is the kernel of $\phi * \psi$, and any two such composite extensions are isomorphic.

Proof. Assertion (a) follows from the fact that the kernel of a homomorphism of a ring into a field is a prime ideal. Let $\mathfrak{p}$ be a prime ideal of $E \otimes_K F$, A be the quotient ring $(E \otimes_K F)/\mathfrak{p}$ and L the field of fractions of A. For $x \in E$ (resp. $y \in F$) we denote by $\phi(x)$ (resp. $\psi(y)$) the residue class mod $\mathfrak{p}$ of $x \otimes 1$ (resp. $1 \otimes y$). Then ϕ (resp. ψ) is a K-homomorphism of E (resp. F) into L and $\phi(E) \cup \psi(F)$ generates A as a ring, hence L as a field. Therefore (L, ϕ, ψ) is a composite extension of E and F; we see at once that $\phi * \psi$ is the canonical homomorphism of $E \otimes_K F$ into L, and its kernel is thus equal to $\mathfrak{p}$.

Let (L', ϕ', ψ') be a composite extension of E and F such that the kernel of $\phi' * \psi'$ is equal to $\mathfrak{p}$. Since $\phi * \psi$ and $\phi' * \psi'$ have the same kernel, there exists an isomorphism σ of A onto the image A' of $\phi' * \psi'$, characterized by $\phi' * \psi' = \sigma \circ (\phi * \psi)$. But A' is the subring of L' generated by $\phi'(E) \cup \phi'(F)$, hence L' is the field of fractions of A'. Therefore σ extends to an homomorphism of L onto L' and it is clear that σ is an isomorphism of (L, ϕ, ψ) onto (L', ϕ', ψ'). □

Remark 9.1.1. If $\mathfrak{p}$ and $\mathfrak{p}'$ are two distinct prime ideals of $E \otimes_K F$, the corresponding composite extensions of E and F (constructed by the procedure of the above proof) are not isomorphic. However, they may nevertheless be isomorphic as extensions of K.

Corollary 9.1.95. *There exist composite extensions of E and F.*

Proof. For since the commutative ring $E \otimes_K F$ is not reduced to 0, it has prime ideals: Krull's theorem proves the existence of maximal ideals and every maximal ideal is prime. □

We can make this corollary more precise as follows. Let (E, ϕ) and (F, ψ) be two extensions of K; choose a maximal ideal $\mathfrak{m}$ of the commutative ring $E \otimes_K F$ and put $L = (E \otimes_K F)/\mathfrak{m}$; then L is an extension of K. For $x \in E$ write $\bar{\phi}(x)$ for the residue class of $x \otimes 1$ mod $\mathfrak{m}$ and similarly put $\bar{\psi}(y)$ for the residue class of $1 \otimes y$ mod $\mathfrak{m}$ for all $y \in F$. We then have a commutative diagram of field homomorphisms

$$\begin{tikzcd} & L & \\ E \arrow[ur, "\bar{\phi}"] & & F \arrow[ul, "\bar{\psi}"'] \\ & K \arrow[ul, "\psi"] \arrow[ur, "\phi"'] & \end{tikzcd}$$

By replacing $(L, \bar{\phi})$ by an isomorphic extension of E we may suppose that L contains E as subfield and that $\bar{\phi}$ is the canonical injection of E in L. By changing notation we thus obtain the following corollary:

Corollary 9.1.96. *Let K and E be two fields and ϕ a homomorphism of K into E. If K is a field containing K as subfield, there exists a field E' containing E as subfield and a homomorphism ϕ' of K' into E' extending ϕ.*

Let A and B be two sub-K-algebras of Ω. There exists an algebra homomorphism $\varphi : A \otimes_K B \to \Omega$ which maps $x \otimes y$ to xy. The image of φ is a subring C of Ω generated by $A \cup B$. Moreover, if (b_μ) is a basis of B over K and (a_λ) a basis of A over K, then C coincides with the set of linear combinations $\sum c_{\lambda\mu} a_\lambda b_\mu$ where $c_{\lambda\mu} \in K$.

We shall say that A and B are **linearly disjoint over K**, if φ is an isomorphism of $A \otimes_K B$ onto C. We then have $A \cap B = K$; every free subset of B (resp. A) with respect to K is then free with respect to A (resp. B) ; conversely, for A and B to be linearly disjoint over K, it is sufficient that there should exist one basis of B over K (for example) which is free with respect to A.

Consider particularly the case where A and B are subextensions of Ω, we have the following proposition.

Proposition 9.1.97. *Let E and F be two extensions of K contained in a field Ω.*

(a) If F has finite degree over K, then the subring of a generated by $E \cup F$ is a field, coinciding with EF and the degree of EF over E is finite; we have $[EF : E] \leq [F : K]$, with equality ifand only if E and F are linearly disjoint over K. In that case EF is E-isomorphic to $E \otimes_K F$.

(b) If E and F are both of finite degree over K, then EF is of finite degree over K. We have $[EF : K] \leq [E : K][F : K]$ with equality if and only if E and F are linearly disjoint over K.

9.1.7 Exercise

Exercise 9.1.1. Let R be an integral domain containing a subfield K (as a subring). If R is finite-dimensional when regarded as an K-vector space, then it is a field.

Proof. Let α be a nonzero element of R. The map $x \mapsto \alpha x$ is an injective linear map of finite-dimensional K-vector spaces, and is therefore surjective. In particular, there is an element $\beta \in R$ such that $\alpha\beta = 1$. Since α is arbitrary, we conclude that R is a field. □

Exercise 9.1.2. Let $K \subseteq K(\alpha)$ be a simple extension, with α transcendental over K. Let E be a subfield of $K(\alpha)$ properly containing K. Prove that $K(\alpha)$ is a finite extension of E.

Proof. Let a be an element in E, then

$$a = \frac{f(\alpha)}{g(\alpha)}, \quad f, g \in K[X]$$

Now in the polynomial ring $E[X]$,

$$h(X) := \frac{f(\alpha)}{g(\alpha)} g(X) - f(X) = a g(X) - f(X) \in E[X]$$

satisfies $h(\alpha) =$, hence $E \subseteq K(\alpha)$ is finite. □

Exercise 9.1.3. Let $f(X) \in K[X]$ be a polynomial over a field K of degree n, and let $r_1, \ldots, r_n$ be the roots of $f(X)$. For a subset $I \subseteq \{1, \ldots, n\}$, denote by r_I the sum $\sum_{i \in I} r_i$. Assume that $r_I \in K$ only for $I = \varnothing$ and $I = \{1, \ldots, n\}$. Prove that $f(X)$ is irreducible over K.

Proof. Let

$$p(X) = (X - r_{i_1}) \cdots (X - r_{i_d}) \in K[X]$$

be a factor of $f(X)$. Then the coefficient of X^{n-1} will be

$$(-1)^{d-1}(r_{i_1} + \cdots + r_{i_d}) = (-1)^{d-1} a_{i_1 \ldots i_d}$$

which belongs to K. This implies $d = n$, so $f(X)$ is irreducible. □

Exercise 9.1.4. Let K be a field. Prove that the ring of square $n \times n$ matrices $\mathcal{M}_n(F)$ contains an isomorphic copy of every extension of K of degree $\leq n$.

Proof. Assume K is an extension of K with degree n. For any element $\alpha \in K$. Multiplication by α defines a K-linear transformation on K, and since α has a minimal polynomial

$$m_\alpha(X) = t^n + r_{n-1}t^{n-1} + \cdots + r_0$$

we choose the basis $1, \alpha, \ldots, \alpha^{n-1}$, then the correponding matrix has the form

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -r_0 \\ 1 & 0 & 0 & \cdots & 0 & -r_1 \\ 0 & 1 & 0 & \cdots & 0 & -r_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & -r_{n-2} \\ 0 & 0 & 0 & \cdots & 1 & -r_{n-1} \end{pmatrix}$$

□

Exercise 9.1.5. Let E/K be a finite field extension, and let $p(X)$ be the characteristic polynomial of the K-linear transformation of K given by multiplication by α. Prove that $p(\alpha) = 0$.

This gives an effective way to find a polynomial satisfied by an element of an extension. Use it to find a polynomial satisfied by $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$.

Exercise 9.1.6. Let E/K be a finite field extension, and let $\alpha \in K$. The norm of α, $N_{E/K}(\alpha)$, is the determinant of the linear transformation of K given by multiplication by α.

Prove that the norm is multiplicative: for $\alpha, \beta \in f$,

$$N_{E/K}(\alpha\beta) = N_{E/K}(\alpha)N_{E/K}(\beta)$$

Compute the norm of a complex number viewed as an element of the extension $\mathbb{R} \subseteq \mathbb{C}$ (and marvel at the excellent choice of terminology). Do the same for elements of an extension $\mathbb{Q}(\sqrt{d})$ of $\mathbb{Q}$, where d is an integer that is not a square,

Proof. For an element α, assume

$$m_\alpha(X) = t^n + r_{n-1}t^{n-1} + \cdots + r_0$$

we choose $1, \alpha, \ldots, \alpha^{n-1}$, then the map $L_\alpha : x \mapsto \alpha x$ has the matrix:

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -r_0 \\ 1 & 0 & 0 & \cdots & 0 & -r_1 \\ 0 & 1 & 0 & \cdots & 0 & -r_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & -r_{n-2} \\ 0 & 0 & 0 & \cdots & 1 & -r_{n-1} \end{pmatrix}$$

from which we get $N_{E/K}(\alpha) = (-1)^n r_0$. The multiplicative comes from that of determinant.

Let $z = a + bi \in \mathbb{C}$, then z has minimal polynomial $X^2 - 2aX + a^2 + b^2$ in $\mathbb{R}$. Hence we have $N_{\mathbb{C}/\mathbb{R}}(z) = a^2 + b^2 = |z|^2$.

Finally, consider $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{d})$, then $m_{\sqrt{d}} = X^2 - d$, and $N(\sqrt{d}) = -d$. □

Exercise 9.1.7. Define the trace $\mathrm{tr}_{E/K}(\alpha)$ of an element α of a finite extension K of a field K by following the lead of Exercise above. Prove that the trace is additive:

$$\mathrm{tr}_{E/K}(\alpha + \beta) = \mathrm{tr}_{E/K}(\alpha) + \mathrm{tr}_{E/K}(\beta)$$

for $\alpha, \beta \in K$. Compute the trace of an element of an extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{d})$ for d an integer that is not a square.

Proof. For two matrix, $\mathrm{tr}(A + B) = \mathrm{tr}(A) + \mathrm{tr}(B)$. For the extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{d})$, $\mathrm{tr}(\sqrt{d}) = 0$. For α satisfying $m_\alpha(X) = t^n + r_{n-1}t^{n-1} + \cdots + r_0$, we have

$$N(\alpha) = (-1)^n r_0, \quad \mathrm{tr}(\alpha) = -r_{n-1}$$

□

Exercise 9.1.8. Let E/K be a finite extension, and let $\alpha \in E$. Assume $[E : K(\alpha)] = r$. Prove that

$$\mathrm{tr}_{E/K}(\alpha) = r\,\mathrm{tr}_{K(\alpha)/K}(\alpha), \quad N_{E/K}(\alpha) = N_{K(\alpha)/K}(\alpha)^r.$$

Proof. If $f_1, \ldots, f_r$ is a basis of E over $K(\alpha)$ and α has degree d over K, then $(f_i\alpha^j)$ is a basis of E over K by Proposition 9.1.13. The matrix corresponding to multiplication by α with respect to this basis consists of r identical square blocks. Hence we get the result from simple linear algebra. □

Exercise 9.1.9. Let p be a prime integer, and let $\alpha = \sqrt[p]{2} \in \mathbb{R}$. Let $g(X) \in \mathbb{Q}[X]$ be any nonconstant polynomial of degree $< p$. Prove that α may be expressed as a polynomial in $g(\alpha)$ with rational coefficients.

Prove that an analogous statement for $\sqrt[4]{2}$ is false.

Proof. Consider the extension

$$\mathbb{Q} \subseteq \mathbb{Q}(g(\alpha)) \subseteq \mathbb{Q}(\alpha).$$

Since $H(X) = g(X) - g(\alpha) \in \mathbb{Q}(g(\alpha))[X]$ satisfies $h(\alpha) = 0$, we see $[\mathbb{Q}(\alpha) : \mathbb{Q}(g(\alpha))] < p$. Since p is a prime, this implies $[\mathbb{Q}(\alpha) : \mathbb{Q}(g(\alpha))] = 1$ by Corollary 9.1.14, which means $\mathbb{Q}(\alpha) = \mathbb{Q}(g(\alpha))$. Now the claim follows.

For $\sqrt[4]{2}$, consider $g(X) = X^2$. Since any polynomial of $\sqrt{2}$ can be written into $a + b\sqrt{2}$. We see the claim is false in this case □

Exercise 9.1.10. Let $\xi = \sqrt{2+\sqrt{2}}$.

- Find the minimal polynomial of ξ over $\mathbb{Q}$, and show that $\mathbb{Q}(\xi)$ has degree 4 over $\mathbb{Q}$.
- Prove that $\sqrt{2-\sqrt{2}}$ is another root of the minimal polynomial of ξ.
- Prove that $\sqrt{2-\sqrt{2}} \in \mathbb{Q}(\xi)$.
- By Corollary 9.1.8, sending ξ to $\sqrt{2-\sqrt{2}}$ defines an automorphism of $\mathbb{Q}(\xi)$ over $\mathbb{Q}$. Find the matrix of this automorphism w.r.t. the basis $1, \xi, \xi^2, \xi^3$.
- Prove that $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\xi))$ is cyclic of order 4.

Proof.

- $(\xi^2-2)^2 = 2$, so $\xi^4 - 4\xi^2 + 2 = 0$, $m_\xi = X^4 - 4X^2 + 2 = (X^2-2)^2 - 2$, the roots of it are $\pm\sqrt{2 \pm \sqrt{2}}$.
- A simple computation:

$$\xi^2 = 2+\sqrt{2}, \quad \xi^3 = 2\sqrt{2+\sqrt{2}} + \sqrt{2}\sqrt{2+\sqrt{2}}, \quad \xi^4 = 6 + 4\sqrt{2}$$

  Note that

$$\sqrt{2+\sqrt{2}} \cdot \sqrt{2-\sqrt{2}} = \sqrt{4-2} = \sqrt{2}$$

  so we have $\sqrt{2-\sqrt{2}} = \sqrt{2}\xi^{-1}$. We can see from above that $\sqrt{2} \in \mathbb{Q}(\xi)$, so $\sqrt{2-\sqrt{2}} \in \mathbb{Q}(\xi)$.
- Compute: denote $\sqrt{2-\sqrt{2}} =: \xi'$, and the automorphism φ, then we have $\xi' = \sqrt{2}\xi^{-1}$, and from $\xi^4 - 4\xi^2 + 2 = 0$ we obtain $\xi^{-1} = 2\xi - \xi^3/2$.

$$\begin{aligned}
&\varphi(1) = 1\\
&\varphi(\xi) = \xi' = \sqrt{2}\xi^{-1} = (\xi^2-2)(2\xi - \xi^3/2) = \xi^3 - 3\xi\\
&\varphi(\xi^2) = \xi'^2 = 2 - \sqrt{2} = 4 - \xi^2\\
&\varphi(\xi^3) = \xi'^3 = (4-\xi^2)\xi' = (4-\xi^2)(\xi^3 - 3\xi) = 7\xi^3 - 12\xi - \xi^5 = 3\xi^3 - 10\xi
\end{aligned}$$

  so the matrix representation is

$$A = \begin{pmatrix} 1 & 0 & 4 & 0 \\ 0 & -3 & 0 & -10 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 3 \end{pmatrix}$$

- we know that $\mathbb{Q}(\xi) = \mathbb{Q}(-\sqrt{2+\sqrt{2}})$ and $\mathbb{Q}(-\sqrt{2-\sqrt{2}}) = \mathbb{Q}(\xi')$. And $\varphi^2 = id$. This means the extension is Galois, hence $|\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\xi))| = 4$.

  We should clarify that calculating the composition of automorphisms should be done in this way: Let choose φ as an example, φ maps ξ to $\xi' = \xi^3 - 3\xi$, so φ^2 maps ξ to

$\varphi(\xi^3 - 3\xi) = \xi'^3 - 3\xi' = (3\xi^3 - 10\xi) - 3(\xi^3 - 3\xi) = -\xi$. Now it is clear that $\varphi^4 = id$. So $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\xi))$ has an element with order 4, hence is isomorphic to $\mathbb{Z}/4\mathbb{Z}$.

By the way, the matrix corresponding to φ has order 4, that is, $\varphi^4 = I_4$. In fact we have

$$A^2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

□

9.2 Galois theory

9.2.1 Galois connections

The traditional Galois correspondence between intermediate fields of an extension and subgroups of the Galois group is one of the main themes of this chapter. We choose to approach this theme through a more general concept, however.

9.2.1.1 Definition of Galois connection

Definition 9.2.1. *Let P and Q be partially ordered sets. A **Galois connection** on the pair (P, Q) is a pair (Π, Ω) of maps $\Pi : P \to Q$ and $\Omega : Q \to P$, where we write $\Pi(p) = p^e$ and $\Omega(q) = q^c$, with the following properties:*

*(1) (**Order-reversing**) For all $p, q \in P$ and $r, s \in Q$,*

$$p \leq q \Rightarrow q^e \leq p^e, \quad r \leq s \Rightarrow s^c \leq r^c.$$

*(2) (**Extensive**) For all $p \in P$, $q \in Q$,*

$$p \leq p^{ec}, \quad q \leq q^{ce}.$$

Lurking within a Galois connection we find two closure operations.

Definition 9.2.2. *Let P be a partially ordered set. A map $p \mapsto \mathrm{cl}(p)$ on P is an (algebraic) **closure operation** if the following properties hold:*

*(1) (**Extensive**) For all $p \in P$, $p \leq \mathrm{cl}(p)$.*

*(2) (**Idempotent**) For all $p \in P$, $\mathrm{cl}(\mathrm{cl}(p)) = \mathrm{cl}(p)$.*

*(3) (**Isotone**) For all $p, q \in P$, $p \leq q \Rightarrow \mathrm{cl}(p) \leq \mathrm{cl}(q)$.*

*An element $p \in P$ is said to be **closed** if $\mathrm{cl}(p) = p$. The set of all closed elements in P is denoted by $\mathrm{Cl}(p)$.*

Theorem 9.2.3. *Let* (Π, Ω) *be a Galois connection on* (P, Q)*. Then the maps*

$$p \mapsto p^{ec}, \quad q \mapsto q^{ce}$$

are closure operations on P *and* Q*, respectively, and we write* $p^{ec} = \mathrm{cl}(p)$ *and* $q^{ce} = \mathrm{cl}(q)$*. Moreover,*

(a) $p^{ece} = p^e$*, that is,*

$$\mathrm{cl}(p^e) = \mathrm{cl}(p)^e = p^e.$$

(b) $q^{cec} = q^c$*, that is,*

$$\mathrm{cl}(q^c) = \mathrm{cl}(q)^c = q^c$$

Proof. Since $p \leq p^{ec}$, the order-reversing property of e gives

$$p^{ece} \leq p^e \leq (p^e)^{ce}.$$

and so $p^e = p^{ece}$, from which (a) follows. Part (b) is similar. □

Theorem 9.2.4. *The maps* $\Pi : P \to \mathrm{Cl}(Q)$ *and* $\Omega : Q \to \mathrm{Cl}(P)$ *are surjective and the restricted maps* $\Pi : \mathrm{Cl}(P) \to \mathrm{Cl}(Q)$ *and* $\Omega : \mathrm{Cl}(Q) \to \mathrm{Cl}(P)$ *are inverse bijections.*

Proof. Since $\mathrm{cl}(p^e) = p^e$, we see that p^e is closed, that is, Π maps P into $\mathrm{Cl}(P)$. Moreover, Π is surjective since if $q \in \mathrm{Cl}(Q)$, then $q = \mathrm{cl}(q) = (q^c)^e$. To see that Π is injective when restricted to closed elements, if $p, q \in \mathrm{Cl}(P)$ and $p^e = q^e$, then $p^{ec} = q^{ec}$, that is, $p = q$. Similar arguments apply to Ω. Finally, since

$$\Omega \circ \Pi(\mathrm{cl}(p)) = \mathrm{cl}(\mathrm{cl}(p)) = \mathrm{cl}(p)$$

we see that $\Omega \circ \Pi = \mathrm{id}$ on $\mathrm{Cl}(P)$ and similarly, $\Pi \circ \Omega = \mathrm{id}$ on $\mathrm{Cl}(Q)$. □

Now we give some examples of Galois connections.

Example 9.2.5. Let X and Y be nonempty sets and $P = \mathscr{P}(X)$ and $Q = \mathscr{P}(Y)$ be the corresponding power sets. Let $R \subseteq X \times Y$ be a relation on $X \times Y$. Then the maps

$$S \in \mathscr{P}(X) \mapsto S^e = \{y \in Y : (x, y) \in R \text{ for all } x \in S\},$$

and

$$T \in \mathscr{P}(Y) \mapsto T^c = \{x \in X : (x, y) \in R \text{ for all } y \in T\}$$

form a Galois connection on $(\mathscr{P}(X), \mathscr{P}(Y))$.

Example 9.2.6. Let $n \geq 1$ and let K be a field. Let $P = \mathscr{P}(K[X_1, \ldots, X_n])$ be the set of all subsets of polynomials over K in the variables $X_1, \ldots, X_n$. Let $Q = \mathscr{P}(K^n)$ be the set of all subsets of K^n, the set of all ordered n-tuples over K. Let $\Pi : \mathscr{P}(K[X_1, \ldots, X_n]) \to \mathscr{P}(K^n)$ be defined by

$$\Pi(S) = \{x \in K^n : f(X) = 0 \text{ for all } f \in S\}$$

and let $\Omega : \mathscr{P}(K^n) \to \mathscr{P}(K[X_1, \ldots, X_n])$ be defined by

$$\Omega(T) = \{f \in K[X_1, \ldots, X_n] : f(X) = 0 \text{ for all } x \in T\}$$

Then (Π, Ω) is a Galois connection on $(\mathscr{P}(K[X_1, \ldots, X_n]), \mathscr{P}(K^n))$.

In the examples given above, the partially ordered sets P and Q are both lattices. In this situation, we have the follwoing useful result.

Theorem 9.2.7. *Let* (Π, Ω) *be a Galois connection on a pair* (P, Q) *of lattices.*

(a) *If P is a complete lattice, then so is* $\mathrm{Cl}(P)$*, under the same meet as P. A similar statement holds for Q.*

(b) *De Morgan's laws hold in* $\mathrm{Cl}(P)$ *and* $\mathrm{Cl}(Q)$*, that is, for* $p, q \in \mathrm{Cl}(P)$ *and* $r, s \in \mathrm{Cl}(Q)$*,*

$$(p \wedge q)^e = p^e \vee q^e, \quad (p \vee q)^e = p^e \wedge q^e,$$

and

$$(r \wedge s)^c = r^c \vee s^c, \quad (r \vee s)^c = r^c \wedge s^c,$$

Proof. For (a), first, since $1 \in P$ has the property that $1 \geq \mathrm{cl}(1) \geq 1$, it follows that $1 \in \mathrm{Cl}(P)$. Suppose that $p_i \in \mathrm{Cl}(P)$. Then the meet $\bigwedge p_i$ exists in P and since $\bigwedge p_i \leq p_j$ for all j, we have

$$\mathrm{cl}(\bigwedge p_i) \leq \mathrm{cl}(p_j) = p_j$$

whence $\mathrm{cl}(\bigwedge p_i) \leq \bigwedge p_j$. Since the reverse inequality holds as well, equality holds and $\bigwedge p_i \in \mathrm{Cl}(P)$. Since joins can be defined in terms of meets, ($\bigvee T$ is the meet of all upper bounds of T), it follows that $\mathrm{Cl}(P)$ is a complete lattice under meet in P. A similar argument can be made for Q.

For (b), observe first that $p \wedge q \leq p$ and $p \wedge q \leq q$ imply that $(p \wedge q)^e \geq p^e$ and $(p \wedge q)^e \geq q^e$, whence $(p \wedge q)^e \geq p^e \vee q^e$. Furthermore, if $r \geq p^e$ and $r \geq q^e$ for $r \geq \mathrm{Cl}(Q)$, then $r^c \leq p$ and $r^c \leq q$, whence $r^c \leq p \wedge q$. Thus, $r \geq (p \wedge q)^e$. It follows by definition of join that $(p \wedge q)^e = p^e \vee q^e$. The other parts of De Morgan's laws are proved similarly. □

In many examples of Galois connections, P and Q have both top and bottom elements. The following remark on the closeness of them is useful.

Proposition 9.2.8. *Let* (Π, Ω) *be a Galois connection on* (P, Q)*, where P and Q have top and bottom elements. Then*

(a) 1_P *and* 1_Q *are closed, and we have*

$$1_P = \Omega(0_Q), \quad 1_Q = \Pi(0_P).$$

(b) 0_P *is closde if and only if* $0_P = \Omega(1_Q)$*, and* 0_Q *is closed if and only if* $0_Q = \Pi(1_P)$*.*

Proof. A top element is closed, since $1_P \leq \mathrm{cl}(1_P) \leq 1_P$, and similar for 1_Q. Also, note that a top element is the image of the corresponding bottom element (if it exists), for $1_P = \Omega(\Pi(p))$ is the image of $\Pi(p)$ and since $0_Q \leq \Pi(p)$, the image of 0_Q must be at least as large as $\Pi(p)$, and therefore equal to 1_P.

Now, since $\Pi(0_P) = 1_Q$, it is closed if and only if $0_P = \Omega(\Pi(0_P)) = \Pi(1_Q)$. Similar, since $\Omega(0_Q) = 1_P$, it is closed if and only if $0_Q = \Pi(\Omega(0_Q)) = \Pi(1_P)$. □

9.2.1.2 Indexed Galois connections

Let $\mathbb{Z}^+$ denote the set of positive integers. In the set $\mathbb{Z}^+ \cup \{\infty\}$, we observe some obvious understandings about ∞, in particular, $\infty \leq \infty$, $n \leq \infty$ for all $n \in \mathbb{Z}^+$, $n \cdot \infty = \infty$ for $n \in \mathbb{Z}^+$ and $\infty \leq n \leq \infty$ implies $n = \infty$.

Definition 9.2.9. *A Galois connection (Π, Ω) on (P, Q) is **indexed** if*

(a) For each $p, q \in P$ with $p \leq q$, there exists a number $(q, p) \in \mathbb{Z}^+ \cup \{\infty\}$, called the degree, or index of q over p.

(b) For each $r, s \in Q$ with $r \leq s$, there exists a number $(s, r) \in \mathbb{Z}^+ \cup \{\infty\}$, called the degree, or index of s over r.

Moreover, the following properties must hold:

*(1) (**Degree is multiplicative**) If $s_1, s_2, s_3 \in P$ or Q, then*

$$s_1 \leq s_2 \leq s_3 \Rightarrow (s_3 : s_1) = (s_3 : s_2)(s_2 : s_1).$$

*(2) (**Degree is nonincreasing**) If $p, q \in P$ then*

$$p \leq q \Rightarrow (p^e : q^e) \leq (q : p).$$

If $r, s \in Q$ then

$$r \leq s \Rightarrow (r^c : s^c) \leq (s : r).$$

*(3) (**Equality by degree**) If $s, t \in P$ or Q, then*

$$(s : t) = 1 \Leftrightarrow s = t$$

If $(s : t) < \infty$, then t is said to be a finite extension of s. If P has a top and bottom element then the index of P is $\mathrm{index}(P) := (1_P : 0_P)$*, and similarly for Q.*

From now on, when we write $(q : p)$, it is with the tacit assumption that $p \leq q$.

The importance of indexing is described in the next theorem. It says that if a Galois connection is indexed, then the connection preserves the index of closed elements and that any finite extension of a closed element is also closed.

Theorem 9.2.10. *Let (Π, Ω) be an indexed Galois connection on (P, Q).*

*(a) (**Degree-preserving on closed elements**) If $p, q \in \mathrm{Cl}(P)$ and $p \leq q$ then $(q : p) = (p^e : q^e)$.*

*(b) (**Finite extensions of closed elements are closed**) If $p \in \mathrm{Cl}(P)$ and $(q : p) < \infty$ then $q \in \mathrm{Cl}(P)$. In particular, if 0_P is closed and $(1_P : 0_P)$ is finite then all elements of P are closed.*

A similar statement holds for Q.

Proof. For (a), we have

$$(q : p) \geq (p^e : q^e) \geq (q^{ec} : q^{ec}) = (q : p).$$

so equality holds throughout.

For (b), if $p \in \mathrm{Cl}(P)$ and $(q : p) < \infty$, then

$$(q : p) \geq (p^e : q^e) \geq (q^{ec} : p^{ec}) = (q^{ec} : p) = (\mathrm{cl}(q) : q)(q : p).$$

and since $(q : p) < \infty$, we may cancel to get $(\mathrm{cl}(q) : q) = 1$, which shows that q is closed. □

Thus, in an indexed Galois connection, the maps are degree-preserving, order-reversing bijections between the collections of closed sets $\mathrm{Cl}(P)$ and $\mathrm{Cl}(Q)$.

Proposition 9.2.11. *Let (Π, Ω) be an indexed Galois connection on (P, Q). If $p, q \in P$, $\mathrm{cl}(p) \leq q$, and one of the following holds*

(a) $(q : p) = (p^e : q^e)$ *and* $(q : \mathrm{cl}(p)) < \infty$.

(b) $(q : p) = (p^e : q^e) < \infty$.

then p is closed.

Proof. Suppose that $(q : \mathrm{cl}(p)) < \infty$. Then q is closed by Theorem 9.2.10 and since $\mathrm{cl}(p)^e = p^e$, we have

$$(q : \mathrm{cl}(p)) = (p^e : q^e).$$

Now if $(p^e : q^e) = (q : p)$, then we have $(q : \mathrm{cl}(p)) = (q : p)$. This implies $(\mathrm{cl}(p) : p) = 1$ if either $(q : \mathrm{cl}(p)) < \infty$ or $(q : p) < \infty$, and so $p = \mathrm{cl}(p)$ is closed. □

The following nonstandard definition will come in handy.

Definition 9.2.12. *Let (Π, Ω) be a Galois connection on (P, Q), we say that P is* ***completely closed*** *if every element of P is closed, and similarly for Q. Also, the pair (P, Q) (or the connection) is* ***completely closed*** *if all elements of P and all elements of Q are closed.*

We have remarked that the top elements 1_P and 0_Q, if they exist, are always closed, but the bottom elements 0_P and 0_Q need not be closed. However, the most important example of a Galois connection, namely, the Galois correspondence of a field extension E/K, which is the subject of our investigations, has the property that 0_Q is closed. So let us assume that 0_Q is closed and see what we can deduce.

Theorem 9.2.13 (0_Q is closed). *Let (Π, Ω) be an indexed Galois connection on (P, Q), where P and Q have top and bottom elements. Assume that 0_Q is closed. Then*

$$\mathrm{index}(Q) \leq \mathrm{index}(P).$$

Also,

(a) If $\mathrm{index}(Q) < \infty$ *or* $\mathrm{index}(P) < \infty$, *then Q is completely closed.*

(b) If $\mathrm{index}(P) < \infty$ *and 0_P is closed, then (P, Q) is completely closed.*

Proof. Since 0_Q is closed, by Proposition 9.2.8 we have $1_P^e = 0_Q$, and therefore

$$\mathrm{index}(P) = (1_P : 0_P) \geq (0_P^e : 1_P^e) = (1_Q : 1_P^e) = (1_Q : 0_Q) = \mathrm{index}(Q)$$

it follows that if P has finite index, then so does Q. Hence, if either P or Q has finite index, then Q is completely closed.

Finally, if P has finite index and 0_P is also closed, then the connection is completely closed by Theorem 9.2.10. □

9.2.2 The Galois correspondence

Now we describe the main theme of this chapter.

Definition 9.2.14. *The **Galois group** of a field extension E/K, denoted by $\mathrm{Gal}(E/K)$, is the group $\mathrm{Aut}_K(E)$ of all automorphisms of E over K. The group $\mathrm{Gal}(E/K)$ is also called the Galois group of E over K.*

Note that when the extension E/K is algebraic, by Theorem 9.1.30

$$\mathrm{Gal}(E/K) = \mathrm{Aut}_K(E) = \mathrm{Hom}_K(E, E),$$

and when E is normal over K, by Theorem 9.1.43

$$\mathrm{Gal}(E/K) = \mathrm{Hom}_K(E, \bar{E}).$$

Let E/K be a field extension and let $\mathcal{F}$ be the complete lattice of all intermediate fields of $K \subseteq E$, ordered by set inclusion. Let $\mathcal{G}$ be the complete lattice of all subgroups of the Galois group $\mathrm{Gal}(E/K)$, ordered by set inclusion. We define two maps $\Pi : \mathcal{F} \to \mathcal{G}$ and $\Omega : \mathcal{G} \to \mathcal{F}$ by

$$\Pi(K) = \mathrm{Gal}(E/K), \quad \Omega(H) = E^H$$

where E^H is the **fixed field** of H.

Theorem 9.2.15. *Let E/K. The pair of maps*

$$(\Pi : K \mapsto \mathrm{Gal}(E/K), \Omega : H \mapsto E^H)$$

is a Galois connection on $(\mathcal{F}, \mathcal{G})$, called the Galois correspondence of the extension E/K.

Proof. It is clear from the definition that Π and Ω are inclusion-reversing. Also, any element of K is fixed by every element of $\mathrm{Gal}(E/K)$, that is, $K \subseteq E^{\mathrm{Gal}(E/K)}$. Finally, any $\sigma \in H$ fixes every element in E^H, that is, $H \subseteq \mathrm{Gal}(E/E^H)$. Thus the claim follows. □

Since $\mathcal{F}$ and $\mathcal{G}$ are complete lattices, Theorem 9.2.7 provides the following corollary.

Corollary 9.2.16. *The set $\mathrm{Cl}(\mathcal{F})$ of closed intermediate fields and the set $\mathrm{Cl}(\mathcal{G})$ of closed subgroups of $\mathrm{Gal}(E/K)$ are complete lattices, where meet is intersection. In particular, the intersection of closed intermediate fields is closed and the intersection of closed subgroups is closed.*

We would like to show that the Galois correspondence of an extension E/K is indexed, where $(K : L) = [K : L]$ is the degree of the extension K/L and $(H : J)$ is the index of the subgroup J in the group H. We know that the degrees are multiplicative and that

$$[K : L] = 1 \Leftrightarrow K = L, \quad [H : J] = 1 \Leftrightarrow H = J.$$

The next theorem shows that the map $\Pi : K \mapsto \mathrm{Gal}(E/K)$ is degree-nonincreasing.

Proposition 9.2.17. *For the tower $K \subseteq E \subseteq F \subseteq L$, we have*

$$[\mathrm{Gal}(L/E) : \mathrm{Gal}(L/F)] \leq [F : E]_s \leq [F : E]$$

as elements in $\mathbb{Z}^+ \cup \{\infty\}$.

Proof. Consider the function $\Phi : \mathrm{Gal}(L/E) \to \mathrm{Hom}_K(F, L)$ that maps $\sigma \in \mathrm{Gal}(L/E)$ to its restriction $\sigma|_F \in \mathrm{Hom}_K(F, L)$. Then $\Phi(\sigma) = \Phi(\tau)$ if and only if σ and τ agree on F, that is, if and only if $\sigma\mathrm{Gal}(L/F) = \tau\mathrm{Gal}(L/F)$. Hence Φ is constant on the cosets of $\mathrm{Gal}(L/F)$ in $\mathrm{Gal}(L/E)$ and so induces an injection on $\mathrm{Gal}(L/E)/\mathrm{Gal}(L/F)$, whence

$$[\mathrm{Gal}(L/E) : \mathrm{Gal}(L/F)] = |\operatorname{im}(\Phi)| \leq |\mathrm{Hom}_K(F, L)| \leq [F : K]_s.$$

This finishes the proof. □

Proposition 9.2.18. *Let E/K be an extension and let $J \subseteq H \subseteq \mathrm{Gal}(E/K)$. Then*

$$[E^J : E^H] \leq [H : J].$$

Proof. First, if $[H : J]$ is infinite, then there is nothing to prove, so let us assume that $[H : J] < \infty$, that is, $H/J = \{h_1J, \ldots, h_mJ\}$ is a finite set. Thus, $S = \{h_1, \ldots, h_m\}$ is a complete set of distinct coset representatives for H/J, and we may assume that $h_1 \in J$.

Let $E^{H/J}$ denote the set of all functions from H/J into E. Then $E^{H/J}$ is a vector space over E, where if $\sigma, \tau \in E^{H/J}$ and $a, b \in E$, then

$$(a\sigma + b\tau)(hJ) = a\sigma(hJ) + b\tau(hJ).$$

Moreover, since the functions $\epsilon_i : H/J \to E$ defined by $\epsilon_i(h_kJ) = \delta_{i,k}$ form a basis for $E^{H/J}$ over E, we have

$$\dim_E(E^{H/J}) = |H/J| = [H : J].$$

Thus, we have two vector spaces: E^J is a vector space over E^H of dimension $[E^J : E^H]$ and $E^{H/J}$ is a vector space over E of dimension $[H : J]$. We wish to show that $\dim_{E^H}(E^J) \leq \dim_E(E^{H/J})$.

To do this, we will show that $\alpha_1, \ldots, \alpha_n \in E^J$ are linearly independent over E^H if and only if the evaluation functions $\widetilde{\alpha}_1, \ldots, \widetilde{\alpha}_n \in E^{H/J}$, defined by

$$\widetilde{\alpha}_k(h_iJ) = h_i(\alpha_k)$$

are linearly independent over E. Note that if $h_1J = h_2J$ then $h_1^{-1}h_2 \in J$ and so

$$(h_1^{-1}h_2)(\alpha_k) = \alpha_k$$

(recall that $\alpha_k \in E^J$) which implies that $h_1(\alpha_k) = h_2(\alpha_k)$, that is, $\widetilde{\alpha}_k(h_1J) = \widetilde{\alpha}_k(h_2J)$. Hence, $\widetilde{\alpha}_k$ is well-defined.

Let $\widetilde{\alpha}_1, \ldots, \widetilde{\alpha}_n \in E^{H/J}$ be linear independent over E. If there are $e_1, \ldots, e_s \in E^H$ such that

$$e_1\alpha_1 + \cdots + e_s\alpha_s = 0$$

then we have

$$\begin{aligned}(e_1\widetilde{\alpha}_1 + \cdots + e_s\widetilde{\alpha}_s)(h_kJ) &= e_1h_k(\alpha_1) + \cdots + e_sh_k(\alpha_s)\\ &= h_k(e_1\alpha_1 + \cdots + e_s\alpha_s) = 0\end{aligned}$$

for all $h_k \in S$. Therefore $e_1\widetilde{\alpha}_1 + \cdots + e_s\widetilde{\alpha}_s = 0$, which implies $e_1 = \cdots = e_s = 0$ by linearly independence of $\widetilde{\alpha}_k$'s over E.

Now assume that $\alpha_1, \ldots, \alpha_n \in E^J$ are linearly independent over E^H and, by reindexing if necessary, let

$$e_1\widetilde{\alpha}_1 + \cdots + e_s\widetilde{\alpha}_s = 0$$

be a nontrivial linear combination over E that is shortest among all nontrivial linear combinations equal to 0. Thus, $e_i \neq 0$ for all i. Dividing by e_s if necessary, we may also assume that $e_s = 1$. Thus

$$e_1\widetilde{\alpha}_1 + \cdots + e_{s-1}\widetilde{\alpha}_{s-1} + \widetilde{\alpha}_s = 0. \tag{2.2.1}$$

Then applying this to h_kJ gives

$$e_1h_k(\alpha_1) + \cdots + e_{s-1}h_k(\alpha_{s-1}) + h_k(\alpha_s) = 0.$$

for all $h_k \in S$. Since the α_i's are fixed by any element of J, and any $h \in H$ has the form $h = h_kj$ for some $j \in J$, we deduce that

$$e_1h(\alpha_1) + \cdots + e_{s-1}h(\alpha_{s-1}) + h(\alpha_s) = 0 \tag{2.2.2}$$

for all $h \in H$. In particular, if $h = 1$, then

$$e_1\alpha_1 + \cdots + e_{s-1}\alpha_{s-1} + \alpha_s = 0. \tag{2.2.3}$$

which implies, owing to the independence of the α_i's over E^H, that not all of the e_i's can lie in E^H. Let us assume that $e_1 \notin E^H$. Hence, there is a $\tau \in H$ for which $\tau(e_1) \neq e_1$.

We can replace h by $\tau^{-1}h$ in (2.2.2) to get

$$e_1\tau^{-1}h(\alpha_1) + \cdots + e_{s-1}\tau^{-1}h(\alpha_{s-1}) + \tau^{-1}h(\alpha_)s = 0.$$

Applying τ gives

$$\tau(e_1)h(\alpha_1) + \cdots + \tau(e_{s-1})h(\alpha_{s-1}) + h(\alpha_s) = 0$$

for all $h \in H$ and so

$$(\tau e_1)\widetilde{\alpha}_1 + \cdots + (\tau e_{s-1})\widetilde{\alpha}_{s-1} + \widetilde{\alpha}_s = 0.$$

Finally, subtracting (2.2.1) from (2.2.3) gives

$$(\tau e_1 - e_1)\widetilde{\alpha}_1 + \cdots + (\tau e_{s-1} - e_{s-1})\widetilde{\alpha}_{s-1} = 0.$$

whose first coefficient is nonzero. But this is shorter than (2.2.1), a contradiction that completes the proof. □

Thus, the Galois correspondence of an extension E/K is indexed. We can now summarize our results in a famous theorem.

Theorem 9.2.19 (Fundamental Theorem of Galois Theory I). *The Galois correspondence (Π, Ω) of an extension E/K is an indexed Galois connection and the bottom group 0_Q is closed. The restrictions of Π and Ω to closed elements are order-reversing, degreepreserving inverse bijections as well as lattice anti-isomorphisms, that is, if K_i are closed intermediate fields and H_i are closed subgroups, then*

$$\mathrm{Gal}(E/\bigcap K_i) = \bigvee \mathrm{Gal}(E/K_i), \quad \mathrm{Gal}(E/\bigvee K_i) = \bigcap \mathrm{Gal}(E/K_i),$$

and

$$E^{\bigcap H_i} = \bigvee E^{H_i}, \quad E^{\bigvee H_i} = \bigcap E^{H_i}.$$

We should note that the joins in the previous theorem are joins in the corresponding lattices. Thus, for instance, $\bigvee \mathrm{Gal}(E/K_i)$ is the smallest closed subgroup of $\mathrm{Gal}(E/K)$ containing all of the subgroups $\mathrm{Gal}(E/K_i)$, and this need not be the smallest subgroup of $\mathrm{Gal}(E/K)$ containing these groups.

As a result of the closedness of $0_Q = \{1\} = \mathrm{Gal}(E/E)$, Theorem 9.2.13 gives the following.

Corollary 9.2.20. *Let (Π, Ω) be the Galois correspondence of E/K. Then*

$$|\mathrm{Gal}(E/K)| \leq [E : K].$$

Also,

(a) If $|\mathrm{Gal}(E/K)| < \infty$ or $[E : K] < \infty$, then $\mathcal{G}$ is completely closed.

(b) If $[E : K] < \infty$ and K is closed, then $\mathcal{F}$ and $\mathcal{G}$ are completely closed.

9.2.3 Closed elements in the Galois correspondence

We turn our attention to the question of which intermediate fields of an extension and which subgroups of the Galois group are closed. We know on general principles that top elements are always closed. Thus, E and $\mathrm{Gal}(E/K)$ are closed. Moreover, the bottom group $\{1\} = \mathrm{Gal}(E/E)$ is also closed. We also know that any finite extension of a closed element is closed.

Now we require a definition. A normal separable extension E/K is called a **Galois extension**, or simply **Galois**. The next theorem follows from the relevant properties of normal and separable extensions. We state it separably.

Proposition 9.2.21 (Properties of Galois extensions).

*(a) (**Full extension Galois implies upper step Galois**) Let $K \subseteq E \subseteq L$. If L/K is Galois then the upper step L/K is Galois.*

*(b) (**Closed under lifting**) The class of Galois extensions is closed under lifting.*

*(c) (**Closed under arbitary composites and intersections**) The class of Galois extensions is closed under arbitrary composites and intersections.*

The importance of Galois extension is revealed in the following theorem.

Theorem 9.2.22 (Fundamental Theorem of Galois Theory II). *Let E/K be algebraic and consider the Galois correspondence on E/K.*

*(1) (**Closed fields**) The closed intermediate fields are precisely the fixed fields, that is, the fields of the form E^H for some $H \subseteq \mathrm{Gal}(E/K)$.*

(a) An intermediate field K is closed if and only if E/K is Galois.

(b) Any extension of a closed intermediate field is closed.

(c) If E/K is a Galois extension, then $\mathcal{F}$ is completely closed.

*(2) (**Closed groups**) The closed subgroups of $\mathrm{Gal}(E/K)$ are precisely the Galois groups of E, that is, the subgroups of the form $\mathrm{Gal}(E/K)$, for some intermediate field K.*

(a) Any finite extension of a closed subgroup is closed.

(b) $\{1\}$ is closed and so any finite subgroup of $\mathrm{Gal}(E/K)$ is closed.

(c) When E/K is finite, so is $\mathrm{Gal}(E/K)$ and so $\mathcal{G}$ is completely closed.

(3) If E/K is a finite Galois extension, then the correspondence is completely closed.

Proof. First, suppose that K is closed and let $\alpha \in E \setminus K$. Then the finite extension $K(\alpha) \subseteq K$ of K is also closed and so

$$d := [\mathrm{Gal}(E/K) : \mathrm{Gal}(E/K(\alpha))] = [K(\alpha) : K] < \infty.$$

Let $S = \{\sigma_1, \ldots, \sigma_d\}$ be a representatives for the coset $\mathrm{Gal}(E/K)/\mathrm{Gal}(E/K(\alpha))$. Each element of S gives a distinct value on α, that is, a distinct root of $\min(\alpha, K)$, for if $\sigma_i(\alpha) = \sigma_j(\alpha)$, then $\sigma_i \circ \sigma_j^{-1} \in \mathrm{Gal}(E/K(\alpha))$, which is not possible for $i \neq j$. Hence, the d roots of $\min(\alpha, K)$ are $\{\sigma_1(\alpha), \ldots, \sigma_d(\alpha)\}$, which are distinct and lie in E. Thus, α is separable and $\min(\alpha, K)$ splits in E, implying that E/K is a Galois extension.

For the converse, suppose that E/K is Galois. If $\alpha \in \mathrm{cl}(K) = E^{\mathrm{Gal}(E/K)}$ has minimal polynomial $f(X) = \min(\alpha, K)$, then $f(X)$ can have no roots other than α. For if β is a root of $f(X)$ in some extension, then there is an embedding $\sigma : E \to \overline{K}$ over K for which $\sigma(\alpha) = \beta$. But since E is normal over K, it follows that $\sigma \in \mathrm{Gal}(E/K)$ and so $\beta = \sigma(\alpha) = \alpha$. Thus $f(X)$ has only one distinct root. Since E/K is separable, it must be linear, which implies that $\alpha \in K$. Thus, $\mathrm{cl}(K) = K$ and K is closed.

Now let K be a closed intermediate field, so that E/K is Galois. If L is an arbitrary extension of K (not necessarily finite), then by Proposition 9.2.21 the extension E/L is also Galois, and therefore L is closed. □

Now we give some examples of non Galois extensions to show that in the general algebraic case, not all subgroups need be closed.

Example 9.2.23. Consider the extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$. Since

$$[\mathbb{Q} : \mathbb{Q}(\sqrt[3]{2})] = 3$$

is prime, the only intermediate fields are $\mathbb{Q}$ and $\mathbb{Q}(\sqrt[3]{2})$ (by Corollary 9.1.14). Concerning $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}))$, since $\sqrt[3]{2} \in \mathbb{R}$, we have an extension $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$; since $\sqrt[3]{2}$ is the only cube root

of 2 in $\mathbb{R}$, we see that the minimal polynomial $X^3 - 2$ of $\sqrt[3]{2}$ has a single root in $\mathbb{Q}(\sqrt[3]{2})$. By Corollary 9.1.8, $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}))$ consists of a single element: it is trivial. Thus, in this example the Galois correspondence acts between a set with two elements and a singleton:

$$\{\mathbb{Q}, \mathbb{Q}(\sqrt[3]{2})\} \rightleftarrows \{\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}))\} = \{e\}$$

In particular, the function associating with each intermediate field the corresponding automorphism group is not injective.

Example 9.2.24. For this example, we shall use the fact that for any prime power p^d, there exists a unique finite field $\mathbb{F}_{p^d}$ of size p^d and $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^e}$ if and only if $d \mid e$. Let $K = \mathbb{F}_p$ and let $E = \overline{\mathbb{F}}_p$. Since K is a finite field, it is perfect and so E/K is separable. Since E is algebraically closed, E/K is normal. Hence E/K is a Galois extension and therefore K is closed. The extension E/K is not finite, however, since $[\mathbb{F}_{p^d} : \mathbb{F}_p] = d$ and $\mathbb{F}_p \subseteq \mathbb{F}_{p^d} \subseteq \overline{\mathbb{F}}_p$ for all $d \geq 1$.

Let $H = \langle \sigma \rangle$ be the subgroup of $\mathrm{Gal}(E/K)$ generated by the Frobenius homomorphism $\sigma : x \mapsto x^p$. The fixed field E^H is the set of all $\alpha \in E$ for which $\alpha = \alpha^p$, in other words, the roots in E of the polynomial $f(X) = X^p - X$. But $f(X)$ already has p roots in K, and so $E^H = K$. It then follows that

$$\mathrm{cl}(H) = \mathrm{Gal}(E/E^H) = \mathrm{Gal}(E/K).$$

Hence, all we need do is show that $H \neq \mathrm{Gal}(E/K)$ to conclude that H is not closed. The key is that any $\tau \in H$ has the form $\tau = \sigma^d$ for some $d \geq 1$ and so the fixed set of τ is

$$\{\alpha \in E : \sigma^d(\alpha) = \alpha\} = \{\alpha \in E : \alpha^{p^d} - \alpha = 0\} = \mathbb{F}_{p^d}$$

which is a finite set. Thus, it suffices show that there is an element of $\mathrm{Gal}(E/K)$ that fixes infinitely many elements of E. To this end, let q be another prime and consider the field

$$F = \mathbb{F}_{p^q} \cup \mathbb{F}_{p^{q^2}} \cup \mathbb{F}_{p^{q^3}} \cup \cdots$$

Then F is a proper subfield of E, since it does not contain, for instance, the subfield $\mathbb{F}_{p^{q+1}}$. Hence $[E : F] > 1$ and since E/F is Galois, the group $\mathrm{Gal}(E/F)$ is not trivial. But if $\tau \in \mathrm{Gal}(E/F)$, then τ fixes the infinite field F.

The Galois correspondence begins with a field extension E/K and the corresponding Galois group $\mathrm{Gal}(E/K)$. We may also begin with a field E and a subgroup G of $\mathrm{Aut}(E)$. Then we can form the fixed field

$$E^G = \{\alpha \in E : \sigma(\alpha) = \alpha \text{ for all } \sigma \in G\}$$

and consider the Galois correspondence of the extension E/E^G.

Proposition 9.2.25. *Let E be a field and let G be a group of automorphisms of E.*

(a) If E/E^G is algebraic, then it is Galois and all intermediate fields are closed.

(b) If E/E^G is finite, then all intemediate fields and all subgroups are closed.

(c) If G is closed (which happens if G is finite), then $G = \mathrm{Gal}(E/E^G)$ is the top group of the correspondence.

$$\begin{tikzcd}
E \arrow[dd, dash] & \mathrm{Gal}(E/E^G) \arrow[d, dash] \\
 & G \arrow[d, dash] \arrow[dl] \\
K = E^G \arrow[ur] & \{1\}
\end{tikzcd}$$

Proof. Suppose E/E^G is algebraic. Then since the base field E^G is closed, E/E^G is a Galois extension. If moreover $[E : E^G] < \infty$, then the correspondence is completely closed by Theorem 9.2.22. If G is closed, then $G = \mathrm{Gal}(E/E^G)$, so it is the top group. □

9.2.4 The Krull topology on Galois group

Let E/K be algebraic. The closure $\mathrm{cl}(H)$ of a subgroup H of the Galois group $\mathrm{Gal}(E/K)$ can be characterized in a useful way. The following nonstandard definition will help.

Definition 9.2.26. *Let E/K be algebraic. Let H be a subgroup of the Galois group $\mathrm{Gal}(E/K)$. A function $\tau : E \to E$ is a **limit point** of H if for any finite set $S \subseteq E$, we have $\tau|_S \in H|_S$, that is, τ agrees with some member of H on S. Let $\overline{H}$ denote the set of closure points of H.*

The name "limit point" is justified in the following proposition.

Proposition 9.2.27. *Let E/K be algebraic and let H be a subgroup of the Galois group $\mathrm{Gal}(E/K)$. Then $\mathrm{cl}(H)$ is the set of limit points of H. More specifically, the following are equivalent:*

(i) $\tau \in \mathrm{cl}(H)$,

(ii) for any finite set $S \subseteq E$, we have $\tau|_S \in H|_S$.

Consequently, a subgroup H of $\mathrm{Gal}(E/K)$ is closed if and only if it contains all of its closure points. In particular, any subgroup of the form $\mathrm{Gal}(E/K)$ contains all of its closure points.

Proof. First, note that a closure point τ of H is a member of the Galois group $\mathrm{Gal}(E/K)$, in fact, τ is in the closure of H, that is

$$\overline{H} \subseteq \mathrm{Gal}(E/E^H) = \mathrm{cl}(H).$$

Indeed, τ is a homomorphism because it agrees with a homomorphism on any finite set in E and it fixes each element of E^H because every member of $\mathrm{Gal}(E/E^H)$ fixes E^H.

We claim that $\overline{H} = \mathrm{cl}(H)$. Since $H \subseteq \overline{H} \subseteq \mathrm{cl}(H)$, the result would follow if H were closed, but of course, it may not be. However, given any finite set $S \subseteq E$, we need only work with the finite extension $E^H \subseteq E^H(S)$, whose Galois group is $\mathrm{Gal}(E^H(S)/E^H)$. In this case, all subgroups are closed. The problem is that we want $H|_{E^H(S)}$ to be in the Galois group and this requires that $E^H \subseteq E^H(S)$ be normal. No problem really: we just pass to a normal closure. Consider the extension

$$E^H \subseteq K = \langle E^H(S)/K \rangle$$

which is finite, normal, contains S and has Galois group $\mathrm{Gal}(K/E^H)$. Since all subgroups are closed, $H|_K$ is a closed subgroup of the Galois group $\mathrm{Gal}(K/E^H)$. Hence, in the Galois correspondence on $E^H \subseteq K$, we have

$$H|_K \subseteq \overline{H|_K} = \mathrm{cl}(H|_K) = \mathrm{Gal}(K/\mathrm{Inv}(H|_K)).$$

It follows that any $\sigma \in$ agrees with a member of $H|_K$ on S. But if $\tau \in \mathrm{cl}(H) = \mathrm{Gal}(E/E^H)$, then

$$\tau|_K \in \mathrm{Gal}(E/\mathrm{Inv}(H))|_K = \mathrm{Gal}(K/\mathrm{Inv}(H|_K))$$

and so $\tau|_K$ agrees with a member of $H|_K$ on S, that is, τ agrees with a member of H on S. Thus, $\overline{H} \in \mathrm{cl}(H)$, as desired. □

We now extend the definition of closure point to apply to any set of functions in E^E, not just subgroups of the Galois group. In particular, a function $\tau \in E^E$ is a closure point of $H \subseteq E^E$ if for any finite set $S \subseteq E$, we have $\tau|_S \in H|_S$.

It is not hard to show that the operation $H \mapsto \overline{H}$ is an algebraic closure operation. In addition, we have $\overline{\varnothing} = \varnothing$ and

$$\overline{H \cup K} = \overline{H} \cup \overline{K}$$

To see the latter, note that if $f \in \overline{H \cup K}$, then for any finite subset $S \subseteq E$, the function f agrees with an element of $H \cup K$ on S. But if $f \notin \overline{H}$, then there is a finite set $S \subseteq E$ for which f does not agree with any element of H on S. Similarly, if $f \notin \overline{K}$, then there is a finite set $R \subseteq E$ for which f does not agree with any element of K on R. However, $R \cup S$ is a finite set and so there must be some element $g \in H \cup K$ that agrees with f on $R \cup S$, and therefore on both R and S, that is, $f = g$ on R and $f = g$ on S. But $g \in H$ or $g \in K$, either one of which provides a contradiction.

It follows that the operation $H \mapsto \overline{H}$ is also a topological closure operation. Hence, the set of all complements of closed elements forms a toplology on E^E. This topology is actually quite famous.

Definition 9.2.28. *Let E^E be the set of all functions from E into E. The **finite topology** on E^E is defined by specifying as subbasis all sets of the form*

$$S_{u,v} = \{f : E \to E : f(u) = v\}$$

where $u, v \in E$. Thus, a basis for E^E consists of all sets of the form

$$\{f : E \to E : f(u_1) = v_1, \ldots, f(u_n) = v_n\}$$

where $u_i, v_i \in E$.

To show that the topology obtained from closure points is the finite topology, let A be any subset of E^E. If $f \in E^E$ is in the closure of A under the finite topology, then any basis set that containing f also contains an element of A. It follows that for any finite set $S \subseteq E$, there is a $g \in A$ for which $f|_S = g|_S$, that is, $f|_S \in A|_S$. In other words, f is a closure point of A.

On the other hand, if f is a closure point of A, then f agrees with some element of A on any finite set and so any basis element containing f must intersect A, showing that f is in the closure of A. Thus we may content us to write the closure $\overline{A}$ with no ambiguous.

Theorem 9.2.29. *Let E/K be algebraic. Then the Galois group* $\mathrm{Gal}(E/K)$ *is closed in the finite topology on E^E. Moreover, a subgroup $H \subseteq$* $\mathrm{Gal}(E/K)$ *is closed in the Galois correspondence if and only if it is closed in the finite subspace topology on* $\mathrm{Gal}(E/K)$.

The subspace topology of the finite topology inherited by $\mathrm{Gal}(E/K)$ is called the Krull topology on $\mathrm{Gal}(E/K)$. We may phrase the previous theorem as follows: A subgroup of $\mathrm{Gal}(E/K)$ is **Galois-closed** if and only if it is **Krull-closed**.

We must remark that the previous theorem just says that the subgroups of $\mathrm{Gal}(E/K)$ are closed with the Krull topology, but not the converse. In fact, there are many other closed subsets of $\mathrm{Gal}(E/K)$, for example the union $H \cup K$ of two subgroups of $\mathrm{Gal}(E/K)$, which is not a subgroup in general.

Since $\mathrm{Gal}(E/K)$ is also a group, we may wonder whether the Krull topology makes $\mathrm{Gal}(E/K)$ a topological group. This is indeed the case, as we will show now.

Proposition 9.2.30. *Let E/K be algebraic. Then $G := \mathrm{Gal}(E/K)$ is a topological group with the Krull topology, and a neighbourhood base of 1 in G is given by*

$$G_S = \{\sigma \in \mathrm{Gal}(E/K) : \sigma(s) = s \text{ for all } s \in S\} \tag{2.4.1}$$

where $S \subseteq E$ is a finite set.

Proof. Let $m : G \times G \to G$ denote the composition on G and $i : G \to G$ denote the inverse operation on G. We will prove that, for any subset $A \times B \subseteq G \times G$,

$$m(\overline{A \times B}) \subseteq \overline{m(A \times B)}, \quad i(\overline{A}) \subseteq \overline{i(A)}. \tag{2.4.2}$$

To do this, first let $(\tau, \sigma) \in \overline{A \times B}$. Then for any finite subset $S \subseteq E$, there exists $\gamma \in A$ and $\nu \in B$ such that

$$\sigma|_S = \nu|_S, \quad \tau|_{\nu(S)} = \gamma|_{\nu(S)},$$

which implies

$$(\tau \circ \sigma)|_S = (\gamma \circ \nu)|_S$$

and therefore $m(\tau, \sigma) = \tau \circ \sigma \in \overline{m(A \times B)}$.

Next let $\tau \in \overline{A}$. Then for any finite subset $S \subseteq E$, there exists $\eta \in A$ such that $\tau|_{\tau^{-1}(S)} = \eta|_{\tau^{-1}(S)}$, and therefore

$$\tau^{-1}|_S = \eta^{-1}|_S.$$

This implies $i(\tau) \in \overline{i(A)}$, and finishes the proof of (2.4.2).

Finally, we consider the neighbourhoods of 1 in G. Let

$$U = \{\sigma \in \mathrm{Gal}(E/K) : \sigma(u_1) = v_1, \ldots, \sigma(u_n) = v_n\}$$

be a basis of G. Then U contains 1 if and only if $u_i = v_i$ for all i, that is, U is the form of (2.4.1). □

Remark 9.2.1. Since a finite subextension F/K of E is determined by finitely many elements, a neighborhood basis of 1 in G is also given by

$$G_F : \{\sigma \in \mathrm{Gal}(E/K) : \sigma|_F = \mathrm{id}\}$$

where F is a subfield of E and F/K is a finite extension.

We now prove some topological properties for the group $\mathrm{Gal}(E/K)$.

Proposition 9.2.31. *The Galois group G of a Galois extension E/K is compact, Hausdorff, and totally disconnected.*

Proof. We first show that G is Hausdorff. If $\sigma \neq \tau$, then $\sigma^{-1}\tau \neq 1$, and so it moves some element of E, i.e., there exists an $\alpha \in E$ such that $\sigma(\alpha) \neq \tau(\alpha)$. For any S containing α, σG_S and τG_S are disjoint because their elements act differently on α. Hence they are disjoint open subsets of G containing σ and τ respectively.

We next show that G is compact. We first noted that, if S is a finite set stable under G, then G_S is a normal subgroup of G ($\sigma G_S \sigma^{-1} = G_{\sigma(S)} = G_S$), and it has finite index because

$$[G : G_S] = |S|$$

by the class formula. Since every finite set is contained in a stable finite set (each element of E is algebraic over K, and its orbit is the set of its conjugates, which is finite), the argument for the Hausdorffness of G shows that the map

$$G \to \prod_{S \text{ finite and stable}} G/G_S$$

is injective. When we endow G/G_S with the product topology, the induced topology on G is that for which the G_S form an open neighbourhood base of 1, i.e., it is the Krull topology. According to the Tychonoff theorem, $\prod G/G_S$ is compact, and so it remains to show that G is closed in the product. For each $S_1 \subseteq S_2$, there are continuous maps

$$\begin{tikzcd} \prod G/G_S \arrow[r] \arrow[dr] & G/G_{S_2} \arrow[d] \\ & G/G_{S_1} \end{tikzcd}$$

where $G/G_{S_2} \to G/G_{S_1}$ is the quotient map. Let $E(S_1, S_2)$ be the closed subset of $\prod G/G_S$ on which the two maps agree. Then $E(S_1, S_2)$ is closed. Since the image of G is exactly the intersection $\bigcap_{S_1 \subseteq S_2} E(S_1, S_2)$, it follows that G is closed in $\prod G/G_S$, and hence compact.

Finally, for each finite set S stable under G, G_S is a subgroup that is open and hence closed. Since $\bigcap G_S = \{1\}$, this shows that the connected component of G containing 1 is just $\{1\}$. By homogeneity, a similar statement is true for every element of G. □

Corollary 9.2.32. *Let G be the Galois group of a Galois extension E/K. Let $\mathcal{S}$ be the collection of finite subsets in E, then*

$$G \cong \varprojlim_{S \in \mathcal{S}} G/G_S.$$

Proof. This follows from the proof above, in view of the realization of the inverse limit. □

9.2.5 Normal subgroups and normal extensions

We now wish to discuss intermediate fields $K \subseteq E \subseteq L$ and their Galois groups $\mathrm{Gal}(E/K)$. We begin with a result concerning the conjugates of a Galois group.

Definition 9.2.33. *Let $K \subseteq E, F \subseteq L$. If there is a $\sigma \in \mathrm{Gal}(L/K)$ for which $\sigma(E) = F$, then E and F are said to be **conjugate**.*

Proposition 9.2.34 (Galois Group of Conjugations). *Let $K \subseteq E, F \subseteq L$ be extensions.*

(a) *For any* $\sigma \in \mathrm{Hom}_K(L, \bar{L})$, *we have*

$$\sigma \mathrm{Gal}(L/E)\sigma^{-1} = \mathrm{Gal}(\sigma(L)/\sigma(E)).$$

(b) *If* E *is normal over* K, *then for any* $\sigma \in \mathrm{Hom}_K(L, \bar{L})$, *we have*

$$\sigma \mathrm{Gal}(L/E)\sigma^{-1} = \mathrm{Gal}(\sigma(L)/E).$$

(c) *If* L *is normal over* K, *then for any* $\sigma \in \mathrm{Hom}_K(L, \bar{L})$, *we have*

$$\sigma \mathrm{Gal}(L/E)\sigma^{-1} = \mathrm{Gal}(L/\sigma(E)).$$

(d) *If* L/K *is Galois, then* E *and* F *are conjugate if and only if the Galois groups* $\mathrm{Gal}(L/E)$ *and* $\mathrm{Gal}(L/F)$ *are conjugate.*

Proof. We first prove (a). Let $\tau \in \mathrm{Gal}(\sigma(L)/\sigma(E))$. Then $\sigma^{-1}\tau\sigma$ is an automorphism of L. Moreover, since τ fixes $\sigma(E)$, we have for $\alpha \in E$,

$$\sigma^{-1}\tau\sigma(\alpha) = \sigma^{-1}\tau(\sigma(\alpha)) = \sigma^{-1}(\sigma(\alpha)) = \alpha,$$

and so $\sigma^{-1}\tau\sigma \in \mathrm{Gal}(L/E)$. Hence

$$\mathrm{Gal}(\sigma(L)/\sigma(E)) \subseteq \sigma \mathrm{Gal}(L/E)\sigma^{-1}.$$

For the reverse inclusion, let $\mu = \sigma\tau\sigma^{-1}$, where $\tau \in \mathrm{Gal}(L/E)$. Then μ is an automorphism of $\sigma(L)$ and if $\alpha \in E$, then $\tau(\alpha) = \alpha$ and so

$$\mu(\sigma(\alpha)) = \sigma\tau(\alpha) = \sigma(\alpha),$$

which shows that $\mu \in \mathrm{Gal}(\sigma(L)/\sigma(E))$.

Part (b) follows from (a), since if $K \lhd E$ then any $\sigma \in \mathrm{Hom}_K(E, \bar{E})$ satisfies $\sigma(E) = E$. Part (c) is similar. For (d), if $\sigma(E) = F$, then part (a) implies that

$$\sigma \mathrm{Gal}(L/E)\sigma^{-1} = \mathrm{Gal}(L/\sigma(E)) = \mathrm{Gal}(L/F).$$

Conversely, if $\sigma \mathrm{Gal}(L/E)\sigma^{-1} = \mathrm{Gal}(L/F)$ then (a) implies that $\mathrm{Gal}(L/\sigma(E)) = \mathrm{Gal}(L/F)$. Since $\sigma(E)$ and F are both closed, taking fixed field gives $\sigma(E) = F$. □

Theorem 9.2.35 (Fundamental Theorem of Galois Theory III). *Let* $K \subseteq E \subseteq L$ *be extensions and* $\Phi : \mathrm{Gal}(L/E) \to \mathrm{Hom}_K(E, L)$ *be the restriction map* $\sigma \mapsto \sigma|_E$.

(a) *If* $K \lhd E$ *then* $\mathrm{Gal}(L/E) \lhd \mathrm{Gal}(L/K)$ *and* Φ *induces an embedding*

$$\frac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(L/E)} \hookrightarrow \mathrm{Gal}(E/K),$$

which is an homeomorphism if $K \lhd L$.

(b) *If* $\mathrm{Gal}(L/E) \lhd \mathrm{Gal}(L/K)$, $K \lhd L$ *and* E *is closed (that is,* L/E *is Galois), then* $K \lhd E$ *and* Φ *induces*

an homeomorphism

$$\frac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(L/E)} \cong \mathrm{Gal}(E/K).$$

(c) *If L/K is Galois, then $K \lhd E$ if and only* $\mathrm{Gal}(L/E) \lhd \mathrm{Gal}(L/K)$.

Proof. The map Φ is continuous since for any finite subset $S \subseteq E$ we have

$$\Phi^{-1}(\mathrm{Gal}(E/K)_S) = \{\sigma \in \mathrm{Gal}(L/K) : (\sigma|_E)(s) = s \text{ for all } s \in S\} = \mathrm{Gal}(L/K)_S$$

which is open in $\mathrm{Gal}(L/K)$. Note that Φ is then closed, beging a continuous map from a compact space to a Hausdorff space.

If $K \lhd E$, then the restriction map Φ has image in $\mathrm{Hom}_K(E, E) = \mathrm{Gal}(E/K)$. Now, by Proposition 9.2.34, since E/K is normal, for any $\sigma \in \mathrm{Gal}(L/K)$ we have

$$\sigma\mathrm{Gal}(L/E)\sigma^{-1} = \mathrm{Gal}(\sigma(L)/\sigma(E)) = \mathrm{Gal}(L/\sigma(E)) = \mathrm{Gal}(L/E), \tag{2.5.1}$$

and therefore $\mathrm{Gal}(L/E)$ is normal in $\mathrm{Gal}(L/K)$. Since $\ker \Phi = \mathrm{Gal}(L/E)$, it induced an embedding

$$\frac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(L/E)} \hookrightarrow \mathrm{Gal}(E/K).$$

If L is also normal over K, then Φ is surjective, since any $\sigma \in \mathrm{Gal}(E/K)$ can be extended to an embedding of L into $\bar{L}$ over L, which must be an element of $\mathrm{Gal}(L/K)$. Hence the embedding is an isomorphism.

Conversely, if $\mathrm{Gal}(E/K) \lhd \mathrm{Gal}(L/K)$ and L/E is Galois, then taking fixed fields in (2.5.1) gives $\mathrm{cl}(\sigma(E)) = \mathrm{cl}(E)$. Thus, if E is closed, then $\sigma(E) \subseteq E$ for all $\sigma \in \mathrm{Gal}(L/K)$. If in addition $K \lhd L$, then $\sigma(E) \subseteq E$ for all $\sigma \in \mathrm{Hom}_K(L, \bar{L})$, that is, E is normal over K. □

Remark 9.2.2. There is a parallel between Galois theory and the theory of **covering spaces** in topology. In this analogy, Galois extensions correspond to **regular covers**; the Galois group of an extension corresponds to the group of **deck transformations**; and Theorem 9.2.35 corresponds to the fact that the quotient of a regular cover by a normal subgroup of the group of deck transformations is again a regular cover.

More general (connected) covers correspond to more general algebraic extensions. A space is **simply connected** if and only if it admits no nontrivial connected covers, so this notion corresponds in field theory to the condition that a field K admits no nontrivial algebraic extensions, that is, that K is **algebraically closed**. Viewing the fundamental group of a space as the group of deck transformations of its fundamental cover suggests that we should think of the Galois group of the algebraic closure $K \subseteq \bar{K}$ as the fundamental group of a field K.

In algebraic geometry this analogy is carried out to its natural consequences. A covering map of algebraic varieties $X \to Y$ determines a field extension $K(Y) \subseteq K(X)$, where $K(X)$, $K(Y)$ are the fields of rational functions (in the affine case, these are just the fields of fractions of the corresponding coordinate rings). One can then use Galois theory to transfer to the algebra-geometric environment notions such as the fundamental group, without appealing to topological notions (such as continuous maps from S^1), which would be problematic in e.g., positive characteristic.

Example 9.2.36 (Galois group of X^4-2). The extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2}, \mathrm{i})$ is a spliting field of X^4-2,

and has degree 8, as we have seen in Example 9.1.41. The roots of this polynomial are $\alpha = \sqrt[4]{2}$, $-\alpha$, $i\alpha$ and $-\mathrm{i}\alpha$, and so any member of the Galois group G is a permutation of these roots. One way to help find the Galois group is to look for an intermediate field N that is normal, because the elements of $\mathrm{Gal}(N/\mathbb{Q})$ are precisely the restrictions of the members of G. Now since any extension of degree 2 is normal, we have $\mathbb{Q} \lhd \mathbb{Q}(\mathrm{i})$; the elements of $\mathrm{Gal}(\mathbb{Q}(\mathrm{i})/\mathbb{Q})$ are the identity 1 and the map $\tau : \mathrm{i} \to -\mathrm{i}$. Since $[\mathbb{Q}(\alpha, \mathrm{i}) : \mathbb{Q}(\mathrm{i})] = 4$, we have $\min(\alpha, \mathbb{Q}(i)) = X^4 - 2$ and so each of the automorphisms 1 and τ can be extended to an element of G by sending α to any of the roots of $X^4 - 2$. This gives all elements of G:

The extensions of 1	The extensions of τ
$1 : \mathrm{i} \mapsto \mathrm{i}, \alpha \mapsto \alpha$	$\tau : \mathrm{i} \mapsto -\mathrm{i}, \alpha \mapsto \alpha$
$\sigma : \mathrm{i} \mapsto \mathrm{i}, \alpha \mapsto \mathrm{i}\alpha$	$\tau\sigma : \mathrm{i} \mapsto -\mathrm{i}, \alpha \mapsto -\mathrm{i}\alpha$
$\sigma^2 : \mathrm{i} \mapsto \mathrm{i}, \alpha \mapsto -\alpha$	$\tau\sigma^2 : \mathrm{i} \mapsto -\mathrm{i}, \alpha \mapsto -\alpha$
$\sigma^3 : \mathrm{i} \mapsto \mathrm{i}, \alpha \mapsto -\mathrm{i}\alpha$	$\tau\sigma^3 : \mathrm{i} \mapsto -\mathrm{i}, \alpha \mapsto \mathrm{i}\alpha$

Note that G can not be abelian, because otherwise any subgroup of G is normal, and thus any intermediate field of $\mathbb{Q} \subseteq \mathbb{Q}(\alpha, \mathrm{i})$ is normal. However, the extension $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$ is not normal. Since $|G| = 8$, this then implies $G = Q_8$ or $G = D_4$. Note that G has a normal subgroup $\langle\sigma\rangle = \{1, \sigma, \sigma^2, \sigma^3\}$ of order 4, and we have $\tau\sigma\tau = \sigma^3$. These together imply that $G \cong D_4$.

Now we want to determine all subgroups of G. All nontrivial subgroups of G have order 2 or 4. The subgroups of order 2 correspond to the elements of order 2:

$$\{1, \sigma^2\}, \quad \{1, \tau\}, \quad \{1, \tau\sigma\}, \quad \{1, \tau\sigma^2\}, \quad \{1, \tau\sigma^3\}.$$

The subgroups of order 4 are

$$\{1, \sigma, \sigma^2, \sigma^3\}, \quad \{1, \tau, \tau\sigma^2, \sigma^2\}, \quad \{1, \tau\sigma, \tau\sigma^3, \sigma^2\}.$$

Therefore the lattice of subgroups of G is

$$\begin{tikzcd}
 & & G \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & & \\
 & \{1, \tau, \tau\sigma^2, \sigma^2\} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \{1, \sigma, \sigma^2, \sigma^3\} \arrow[d, dash] & \{1, \tau\sigma, \tau\sigma^3, \sigma^2\} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\{1, \tau\} \arrow[drr, dash] & \{1, \tau\sigma^2\} \arrow[dr, dash] & \{1, \sigma^2\} \arrow[d, dash] & \{1, \tau\sigma\} \arrow[dl, dash] & \{1, \tau\sigma^3\} \arrow[dll, dash] \\
 & & \{1\} & &
\end{tikzcd}$$

Of course, the lattice of intermediate (fixed) fields is a reflection of this. To compute fixed fields, we use the fact that $\{1, \mathrm{i}\}$ is a basis for $\mathbb{Q}(\mathrm{i})$ over $\mathbb{Q}$ and $\{1, \alpha, \alpha^2, \alpha^3\}$ is a basis for $\mathbb{Q}(\mathrm{i}, \alpha)$ over $\mathbb{Q}(i)$ and so the products form a basis for $\mathbb{Q}(r, i)$ over $\mathbb{Q}$. Hence, each $\xi \in E = \mathbb{Q}(\alpha, \mathrm{i})$ has the form

$$\xi = a + b_1\alpha + b_2\alpha^2 + b_3\alpha^3 + d_1\mathrm{i} + d_2\mathrm{i}\alpha + d_3\mathrm{i}\alpha^2 + d_4\mathrm{i}\alpha^3.$$

Using this, the fixed fields are easy to compute:

$E^{\{1,\tau\}} = \mathbb{Q}(\alpha)$	$E^{\{1,\tau,\tau\sigma^2,\sigma^2\}} = \mathbb{Q}(\alpha^2)$
$E^{\{1,\tau\sigma^2\}} = \mathbb{Q}(\mathrm{i}\alpha)$	$E^{\{1,\sigma,\sigma^2,\sigma^3\}} = \mathbb{Q}(\mathrm{i})$
$E^{\{1,\sigma^2\}} = \mathbb{Q}(\alpha^2, \mathrm{i})$	$E^{\{1,\tau\sigma,\tau\sigma^3,\sigma^2\}} = \mathbb{Q}(\mathrm{i}\alpha^2)$
$E^{\{1,\tau\sigma\}} = \mathbb{Q}((1-\mathrm{i})\alpha)$	
$E^{\{1,\tau\sigma^3\}} = \mathbb{Q}((1+\mathrm{i})\alpha)$	

We collect these results into the following diagram

$$\begin{tikzcd}
 & & \mathbb{Q} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & & \\
 & \mathbb{Q}(\alpha^2) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \mathbb{Q}(\mathrm{i}) \arrow[d, dash] & \mathbb{Q}(\mathrm{i}\alpha^2) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\alpha) \arrow[drr, dash] & \mathbb{Q}(\mathrm{i}\alpha) \arrow[dr, dash] & \mathbb{Q}(\alpha^2, \mathrm{i}) \arrow[d, dash] & \mathbb{Q}((1+\mathrm{i})\alpha) \arrow[dl, dash] & \mathbb{Q}((1-\mathrm{i})\alpha) \arrow[dll, dash] \\
 & & \mathbb{Q}(\alpha, \mathrm{i}) & &
\end{tikzcd}$$

Note that in the diagram, $\mathbb{Q}(\alpha^2, \mathrm{i}) = \mathbb{Q}(\sqrt{2}, \mathrm{i}) = \mathbb{Q}(\sqrt{2} + \mathrm{i})$ is the spliting field of $X^4 - X^2 - 2$ over $\mathbb{Q}$. This justify the fact that $\mathrm{Gal}(\mathbb{Q}(\alpha, \mathrm{i})/\mathbb{Q}(\alpha^2, i)) = \langle \sigma^2 \rangle$ is a normal subgroup.

9.2.6 Galois groups of lifting and composites

We now examine the behavior of Galois groups under lifting and under composites. As usual, we assume that all composites mentioned are defined.

Let $K \subseteq E$ be normal and let $K \subseteq F$. Any $\sigma \in \mathrm{Gal}(EF/F)$, the Galois group of the lifting, is uniquely determined by what it does to E (since it fixes F) and so the restriction map $\sigma \mapsto \sigma|_E$ is an injection. Since E/K is normal, it follows that $\sigma|_E \in \mathrm{Gal}(E/K)$. But $\sigma|_E$ may fix more than K: It also fixes every element of E that is fixed by σ, that is,

$$\sigma|_E \in \mathrm{Gal}(E/E \cap EF^{\mathrm{Gal}(EF/F)}) = \mathrm{Gal}(E/E \cap \mathrm{cl}(F)).$$

Note that the restriction map is a homomorphism, and hence an embedding of $\mathrm{Gal}(EF/F)$ into $\mathrm{Gal}(E/E \cap \mathrm{cl}(F))$. We will show that this embedding is actually an isomorphism and

$$\mathrm{Gal}(EF/F) \cong \mathrm{Gal}(E/E \cap \mathrm{cl}(F)).$$

Proposition 9.2.37. *Let $K \subseteq E$ be normal and let $K \subseteq F$. The restriction map*

$$\Phi : \mathrm{Gal}(EF/F) \to \mathrm{Gal}(E/E \cap \mathrm{cl}(F))$$

defined by $\Phi(\sigma) = \sigma|_E$ is a homeomorphism.

Proof. We first prove that the map is continuous. For any finite set S of elements of E, we have

$$\Phi^{-1}(\mathrm{Gal}(E/E \cap \mathrm{cl}(F))_S) = \mathrm{Gal}(EF/F)_S,$$

which is open. Therefore Φ is continuous by homogeneity.

We next show that the map is an isomorphism of groups (neglecting the topology). Since Φ is injective, we only need to show it is also surjective. To avoid confusion, let us use the

notation Inv_E for the fixed field with respect to the Galois correspondence on E/K, and Inv_{EF} for the fixed field with respect to the Galois correspondence on EF/F. Let $H := \operatorname{im}\Phi$, then we observe that

$$\begin{aligned}\mathrm{Inv}_E(H) &= \{\alpha \in E : \tau(\alpha) = \alpha \text{ for all } \tau \in \operatorname{im}\Phi\}\\ &= \{\alpha \in E : (\sigma|_E)(\alpha) = \alpha \text{ for all } \sigma \in \mathrm{Gal}(EF/F)\}\\ &= \{\alpha \in E : \sigma(\alpha) = \alpha \text{ for all } \sigma \in \mathrm{Gal}(EF/F)\}\\ &= E \cap \mathrm{Inv}_{EF}(\mathrm{Gal}(EF/F)) = E \cap \mathrm{cl}(F),\end{aligned}$$

Therefore $\overline{H} = \mathrm{Gal}(E/E \cap \mathrm{cl}(F))$, which implies H is dense in $\mathrm{Gal}(E/E \cap \mathrm{cl}(F))$. But H is closed, being a continuous image of a compact space in a Hausdorff space, so $H = \mathrm{Gal}(E/E \cap \mathrm{cl}(F))$.

Finally, since Φ is a continuous bijection, it is a homeomorphism, since $\mathrm{Gal}(EF/F)$ is a compact space and $\mathrm{Gal}(E/E \cap \mathrm{cl}(F))$ is Hausdorff. □

For a Galois extension E/K, the previous theorem simplifies a bit.

Proposition 9.2.38 (The Galois group of a lifting). *Suppose $K \subseteq E$ is a Galois extension and $K \subseteq F$ is an arbitrary extension. Then the lifting $F \subseteq EF$ is a Galois extension. Moreover, the restriction map $\mathrm{Gal}(EF/F) \to \mathrm{Gal}(E/E \cap F)$ defined by $\sigma \mapsto \sigma|_E$ is an isomorphism. Also,*

(a) $E \cap F = K$ implies $\mathrm{Gal}(EF/F) \cong \mathrm{Gal}(E/K)$.

(b) If $K \subseteq E$ is finite, then $\mathrm{Gal}(EF/F) \cong \mathrm{Gal}(E/K)$ implies $E \cap F = K$.

$$\begin{tikzcd}[column sep=small]
 & EF \arrow[dl, dash] \arrow[dr, dash, "\mathrm{Gal}"] & \\
E \arrow[dr, dash, "\mathrm{Gal}"'] & & F \arrow[dl, dash] \\
 & E \cap F \arrow[d, dash] & \\
 & K &
\end{tikzcd}$$

Proof. If E/K is Galois, then EF/F is Galois, implying that F is closed. Therefore the statement in Proposition 9.2.37 simplifies to (a). As for (b), since all is finite, if $\mathrm{Gal}(E/K) = \mathrm{Gal}(E/E \cap F)$ then taking fixed fields gives the claim. □

Corollary 9.2.39. *Suppose that $K \subseteq E_i$ is a finite Galois extension for $i = 1, \ldots, n-1$ and $K \subseteq E_n$ is a finite extension. then*

$$[E_1 \cdots E_n : K] = \prod_{i=1}^{n} [E_i : E_i \cap (E_{i+1} \cdots E_n)] = \frac{\prod_{i=1}^{n} [E_i : K]}{\prod_{i=1}^{n} [E_i \cap (E_{i+1} \cdots E_n) : K]},$$

where $E_n \cap (E_{n+1}) := K$.

Proof. The case $n = 2$ comes from Proposition 9.2.38, and the general case follows by induction. □

Corollary 9.2.40. *Let E and F be field extensions of K and let L be an algebraically closed field containing K. Moreover let E/K be Galois. If $\rho : E \to L$ and $\sigma : F \to L$ are K-homomorphisms such that $\rho|_{E\cap F} = \sigma|_{E\cap F}$, then there exists an K-homomorphism τ such that $\tau|_E = \rho$ and $\tau|_F = \sigma$.*

Proof. By Theorem 9.1.32, σ can be extended to a K-homomorphism $\widetilde{\sigma} : EF \to L$. As $\widetilde{\sigma}|_{E\cap F} = \rho|_{E\cap F}$, we have

$$\rho^{-1} \circ (\widetilde{\sigma}|_E) =: \epsilon \in \mathrm{Gal}(E/E \cap F).$$

According to Proposition 9.2.38, there exists a unique $\eta \in \mathrm{Gal}(EF/F)$ such that $\epsilon = \eta|_E$. Define $\tau = \widetilde{\sigma} \circ \eta^{-1}$, we see that $\tau : EF \to L$ is a K-homomorphism such that $\tau|_E = \rho$ and $\tau|_F = \sigma$. □

Example 9.2.41. We have studied cyclotomic fields $\mathbb{Q}(\zeta_n)$ as extensions of $\mathbb{Q}$; $\mathbb{Q}(\zeta_n)$ is the splitting field of $X^n - 1$, so these extensions are Galois; we have proved (Proposition 9.3.40) that $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is isomorphic to the group of units in $\mathbb{Z}/n\mathbb{Z}$.

Now let K be any field of characteristic zero. The splitting field of $X^n - 1$ over K is the composite $K(\zeta_n)$ of K and $\mathbb{Q}(\zeta_n)$. By Proposition 9.2.38 the extension $K \subseteq K(\zeta_n)$ is Galois, and $\mathrm{Aut}_K(K(\zeta_n))$ is isomorphic to a subgroup of the group of units of $\mathbb{Z}/n\mathbb{Z}$.

Example 9.2.42. We return to Example 9.2.24, where we consider the extension $\mathbb{F}_p \subseteq \overline{\mathbb{F}}_p$ and found a dense proper subgroup in $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$: the subgroup H generated by the Frobenius homomorphism σ. We now use this to determine the structure of G.

Recall that $\widehat{\mathbb{Z}}$ is the limit ring of the homomorphisms $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ for $m \mid n$. It is isomorphic to the direct product of p-adic intergers, where p is a positive prime. Let $\alpha \in \widehat{\mathbb{Z}}$ be represented by the sequence (a_i). Since $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ if $m \mid n$, it is easy to see how to define the automorphism $\sigma^\alpha \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$: Just let σ^α be $(\sigma|_{\mathbb{F}_{p^n}})^{a_n}$ on $\mathbb{F}_{p^n}$. If $m \mid n$, since $\sigma|_{\mathbb{F}_{p^m}}$ has order m and $a_m \equiv a_n \bmod n$, we see that

$$(\sigma|_{\mathbb{F}_{p^n}})^{a_n}|_{\mathbb{F}_{p^m}} = (\sigma|_{\mathbb{F}_{p^m}})^{a_n} = (\sigma|_{\mathbb{F}_{p^m}})^{a_m}$$

so this is well-defined. The map $\sigma \mapsto \sigma^\alpha$ gives an isomorphism from $\widehat{\mathbb{Z}}$ to $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$.

We now turn to the Galois group of a composite. Let $K \lhd E$ and $K \lhd F$. Then any $\sigma \in \mathrm{Gal}(EF/K)$ is completely determined by its action on E and F, that is, by its restrictions $\sigma|_E$ and $\sigma|_F$, or put another way, by the element

$$(\sigma|_E, \sigma|_F) \in \mathrm{Gal}(E/K) \times \mathrm{Gal}(F/K)$$

Indeed, the map $\Phi : \mathrm{Gal}(EF/K) \to \mathrm{Gal}(E/K) \times \mathrm{Gal}(F/K)$ is an embedding of groups. Moreover, as we will see, in the finite case, if the fields enjoy a form of independence ($E \cap F = K$), then the embedding is an isomorphism.

Proposition 9.2.43 (The Galois group of a composite).

(a) Let $\mathcal{E} = \{E_i : i \in I\}$ be a family of fields, with $K \lhd E_i$ for all $i \in I$. Let $G = \prod \mathrm{Gal}(E_i/K)$ be the direct product of the Galois groups $\mathrm{Gal}(E_i/K)$ and let π_i be projection onto the i-th coordinate. Then the map

$$\Phi : \mathrm{Gal}(\bigvee E_i/K) \to \prod \mathrm{Gal}(E_i/K), \quad \sigma \mapsto (\sigma|_{E_i})$$

is an embedding of groups, and Φ is an isomorphism if

$$E_j \cap \Big(\bigvee_{i \neq j} E_i\Big) = K$$

for all $j \in I$.

(b) *If $\mathcal{E} = \{E_1, \dots, E_n\}$ is a finite family of finite Galois extensions, then the map Φ is an isomorphism if and only if*

$$E_i \cap (E_{i+1} \dots E_n) = K$$

for all $i = 1, \dots, n$.

Proof. Since $K \lhd E_i$, by Theorem 9.2.35, each individual restriction map $\Phi_j : \sigma \mapsto \sigma|_{E_j}$ is a surjective homomorphism from $\mathrm{Gal}(\bigvee E_i/K)$ onto $\mathrm{Gal}(E_j/K)$, with kernel $\mathrm{Gal}(\bigvee E_i/E_j)$. Hence, Φ is a homomorphism from $\mathrm{Gal}(\bigvee E_i/K) \to \prod \mathrm{Gal}(E_i/K)$. As to the kernel of Φ, if $\Phi(\sigma) = 1$, then

$$\sigma|_{E_j} = \Phi_j(\sigma) = \pi_j(\Phi(\sigma)) = 1$$

and so $\sigma = 1$ on each E_j, which implies that $\sigma = 1$. Hence, $\ker \Phi = \{1\}$ and Φ is an embedding. If moreover $E_j \cap (\bigvee_{i \neq j} E_j) = K$, then by Proposition 9.2.38 we have

$$\mathrm{Gal}(E_j/K) \cong \mathrm{Gal}(\bigvee E_i / \bigvee_{i \neq j} E_i),$$

where the isomorphism is given by restriction. This implies the direct summand $\mathrm{Gal}(E_j/K)$ is contained in $\operatorname{im} \Phi$. Since this holds for all j, it follows that Φ is surjective, and hence an isomorphism.

When $\mathcal{E}$ is a finite family of finite Galois extensions, all Galois groups are finite and all subgroups and intermediate fields are closed. Since Φ is injective, we have

$$|\operatorname{im} \Phi| = |\mathrm{Gal}(E_1 \cdots E_n/K)| = [E_1 \cdots E_n : K] = \frac{\prod_{i=1}^n [E_i : K]}{\prod_{i=1}^n [E_i \cap (E_{i+1} \cdots E_n) : K]}$$

and also

$$\left| \prod \mathrm{Gal}(E_i/K) \right| = \prod_{i=1}^n |\mathrm{Gal}(E_i/K)| = \prod_{i=1}^n [E_i : K].$$

Therefore Φ is surjective if and only if $E_i \cap (E_{i+1} \cdots E_n) = K$ for all $i = 1, \dots, n$. □

If $K \subseteq E$ is a finite Galois extension whose Galois group is a direct product $G_1 \times \cdots \times G_n$, then we may wish to find intermediate fields E_i whose Galois groups (over K) are isomorphic to the individual factors G_i in the direct product.

Corollary 9.2.44. *Suppose that $K \subseteq E$ is a Galois extension with Galois group of the form*

$$\mathrm{Gal}(E/K) = G_1 \times \cdots \times G_n.$$

If

$$H_i = G_1 \times \cdots \times \{1\} \times \cdots \times G_n$$

where $\{1\}$ is in the i-th coordinate and if $E_i = E^{H_i}$, then

(a) *$K \subseteq E_i$ is Galois, with Galois group $\mathrm{Gal}(E/E_i) \cong G_i$.*

(b) *$E = E_1 \vee \cdots \vee E_n$.*

(c) *$E_i \cap (E_{i+1} \cdots E_n) = K$ for all $i = 1, \dots, n$.*

Proof. Since $G_i \lhd G$, $K \subseteq E$ is normal, and $E_i = E^{H_i}$ is closed, it follows from Theorem 9.2.35(b) that $K \lhd E_i$ and

$$\mathrm{Gal}(E_i/K) \cong \frac{\mathrm{Gal}(E/K)}{\mathrm{Gal}(E/E_i)} = \frac{G}{H_i} \cong G_i.$$

In addition, $E_1 \cdots E_n/K$ is Galois and since

$$\mathrm{Gal}(E/\bigvee E_i) = \bigcap \mathrm{Gal}(E/E_i) = \bigcap H_i = \{1\} = \mathrm{Gal}(E/E)$$

taking fixed fields gives $E = \bigvee E_i$. Hence,

$$\mathrm{Gal}(\bigvee E_i/K) = \mathrm{Gal}(E/K) = \prod G_i \cong \prod \mathrm{Gal}(E_i/K)$$

and Proposition 9.2.43 implies that $E_i \cap (E_{i+1} \cdots E_n) = K$ for all $i = 1, \ldots, n$. □

9.2.7 Exercise

Exercise 9.2.1. Prove that quadratic extensions are Galois.

Proof. Let $K \subseteq E$ be a quadratic extension, and $\alpha \in K$. Let $f(X)$ be the minimal polynomial of α, then $\deg f > 1$, since $\alpha \notin K$. But $\deg f \leq [E : K] = 2$, this shows that $\deg f = 2$, hence $E = K(\alpha)$. Now if $f(X)$ is not separable, then $f(X) = (X - \alpha)^2 = X^2 - 2a + a^2$. Which means $a \in K$, a contradiction. □

Exercise 9.2.2.

- Prove that $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2+\sqrt{2}})$ is Galois, with cyclic Galois group.
- Prove that $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3+\sqrt{5}})$ is Galois and its Galois group is isomorphic to $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.
- Prove that $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{1+\sqrt{2}})$ is not Galois, and compute its Galois closure $\mathbb{Q} \subseteq K$. Prove that $\mathrm{Aut}_{\mathbb{Q}}(F) \cong D_4$.

Proof.

- The minimal polynomial of $\zeta := \sqrt{3+\sqrt{5}}$ is $X^4 - 6X^2 + 4$. The roots of it are

  $$\pm\sqrt{3 \pm \sqrt{5}}$$

  Note that

  $$\sqrt{3+\sqrt{5}}\sqrt{3-\sqrt{5}} = \sqrt{9-5} = 2$$

  so the extension is Galois.

- The minimal polynomial of $\zeta := \sqrt{1+\sqrt{2}}$ is $X^4 - 2X^2 - 1$. The roots of it are

  $$\pm\sqrt{1 \pm \sqrt{2}}$$

  We also find that

  $$\sqrt{1+\sqrt{2}}\sqrt{1-\sqrt{2}} = \sqrt{1-2} = i$$

so the extension is not Galois.

□

Exercise 9.2.3. Let E/K be a Galois extension of degree n, and let E be an intermediate field. Assume that $[E : K]$ is the smallest prime dividing n. Prove $K \subseteq E$ is Galois.

Proof. This comes from the corresponding result in group theory. □

Exercise 9.2.4. Let E/K be a Galois extension of degree 75. Prove that there exists an intermediate field F, with $K \subsetneq F \subsetneq E$, such that the extension $K \subseteq F$ is Galois.

Proof. $75 = 3 \cdot 5^2$. So a group of order 75 has a unique 5-Sylow sugroup, which is therefore normal. □

Exercise 9.2.5. Find two algebraic extensions $K \subseteq E$, $K \subseteq F$ and embeddings $K \subseteq \overline{K}$, $\sigma_1 : F \subseteq \overline{K}$, $\sigma_2 : F \subseteq \overline{K}$ extending $K \subseteq \overline{K}$ such that the composites $E\sigma_1(F)$, $E\sigma_2(F)$ are not isomorphic.

Prove that no such example exists if E and F are Galois over K.

Proof. Consider $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2})$ and $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$. Embedding $\mathbb{Q}(\sqrt[4]{2})$ as $F_1 = \mathbb{Q}(\sqrt[4]{2})$ and $F_2 = \mathbb{Q}(\sqrt[4]{2}i)$. Then

$$\mathbb{Q}(\sqrt{2})F_1 = \mathbb{Q}(\sqrt{2}), \quad \mathbb{Q}(\sqrt{2})F_2 = \mathbb{Q}(\sqrt{2}i)$$

they are not isomorphic. □

Exercise 9.2.6. Let E/K be a Galois extension, and let $\alpha \in K$. Prove that

$$N_{E/K}(\alpha) = \prod_{\sigma \in \mathrm{Aut}_K(F)} \sigma(\alpha), \quad \mathrm{tr}_{E/K}(\alpha) = \sum_{\sigma \in \mathrm{Aut}_K(F)} \sigma(\alpha).$$

Exercise 9.2.7. Use Hilbert's theorem 90 to find all rational roots a, b of the equation $a^2 + b^2 d = 1$, where d is a positive integer that is not a square.

Proof. Consider the extension $D = \mathbb{Q}(\sqrt{d}i)$, then by Exercise 9.2.6, we know that

$$N_{D/\mathbb{Q}}(a + b\sqrt{d}) = (a + \sqrt{d}i)(a - \sqrt{d}i) = a^2 + db^2$$

Then

$$a^2 + db^2 = 1 \Leftrightarrow N_{D/\mathbb{Q}}(a + b\sqrt{d}i) = 1 \Leftrightarrow a + b\sqrt{d} = \beta/\varphi(\beta)$$

where $\varphi(a + b\sqrt{d}i) = a - b\sqrt{d}i$. So we conclude that

$$a^2 + db^2 = 1 \Leftrightarrow a + b\sqrt{d} = \frac{x + y\sqrt{d}i}{x - y\sqrt{d}i} = \frac{x^2 - dy^2}{x^2 + dy^2} + \frac{2xy\sqrt{d}i}{x^2 + dy^2}$$

□

9.3 Applications of Galois theory

In this section, we pass from the highly theoretical material of the previous section to the somewhat more concrete, where we apply the results to some special Galois correspondences.

9.3.1 The Galois group of a polynomial

The **Galois group of a polynomial** $f(X) \in K[X]$, denoted by $\mathrm{Gal}_K(f(X))$, is defined to be the Galois group of a splitting field E of $f(X)$ over K. If

$$f(X) = p_1(X)^{e_1} p_2^{e_2}(X) \cdots p_s(X)^{e_s}$$

is a factorization of $f(X)$ into powers of distinct irreducible polynomials over K, then E is also a splitting field for the polynomial $g(X) = p_1(X) \cdots p_s(X)$. Moreover, the extension E/K is separable (and hence Galois) if and only if each $p_i(X)$ is a separable polynomial. To see this, let E_i be the splitting field for $p_i(X)$ satisfying $K \subseteq E_i \subseteq E$. Then if $K \subseteq E$ is separable, so is the lower step $K \subseteq E_i$ and therefore so is $p_i(X)$. Conversely, if each factor $p_i(X)$ is separable over K, then E is separably generated over K and so $K \subseteq E$ is separable.

Let $\{\alpha_1, \ldots, \alpha_n\}$ be the set of roots of $f(X)$, then $\mathrm{Gal}_K(f)$ consists exactly of the permutations σ of $\{\alpha_1, \ldots, \alpha_n\}$ such that, for $P \in K[X_1, \ldots, X_n]$,

$$P(\alpha_1, \ldots, \alpha_n) = 0 \Leftrightarrow P(\sigma(\alpha_1), \ldots, \sigma(\alpha_n)) = 0. \tag{3.1.1}$$

To see this, note that the kernel of the map

$$K[X_1, \ldots, X_n] \to E_f, \quad X_i \mapsto \alpha_i \tag{3.1.2}$$

consists of the polynomials $P(X_1, \ldots, X_n)$ such that $P(\alpha_1, \ldots, \alpha_n) = 0$. Let σ be a permutation of the α_i's satisfying the condition (3.1.1). Then the map

$$K[X_1, \ldots, X_n] \to E_f, \quad X_i \mapsto \sigma(\alpha_i)$$

factors through the map (3.1.2), and defines an K-isomorphism $E_f \to E_f$, i.e., an element of the Galois group. This shows that every permutation satisfying the condition (3.1.1) extends uniquely to an element of $\mathrm{Gal}_K(f)$, and it is obvious that every element of $\mathrm{Gal}_K(f)$ arises in this way.

9.3.1.1 Symmetric polynomials

In this part, we discuss the relationship between the roots of a polynomial and its coefficients. It is well known that the constant coefficient of a polynomial $f(X)$ is the product of its roots and the linear term of $f(X)$ is the negative of the sum of the roots. We wish to expand considerably on these statements.

We first introduce the general polynomial and elementary symmetric functions. If K is a field and $t_1, \ldots, t_n$ are algebraically independent over K, the polynomial

$$g(X) = \prod_{i=1}^{n} (X - t_i)$$

is referred to as a general polynomial over K of degree n. Since the roots $t_1, \ldots, t_n$ of the general polynomial $g(X)$ are algebraically independent, this polynomial is, in some sense, the most general polynomial of degree n. It can be shown by induction that the general polynomial

can be written in the form

$$g(X) = X^n - s_1 X^{n-1} + \cdots + (-1)^n s_n$$

where the coefficients are given by

$$s_1 = \sum_i t_i, \quad s_2 = \sum_{i<j} t_i t_j, \quad \ldots \quad , s_n = \prod_{i=1}^n t_i$$

and are called the **elementary symmetric polynomials** in the variables t_i.

As an example of what can be gleaned from the general polynomial, we deduce immediately the following lemma.

Lemma 9.3.1. *Let $f(X) \in K[X]$. The coefficients of $f(X)$ are, except for sign, the elementary symmetric polynomials of the roots of $f(X)$. In particular, if*

$$f(X) = X^n - s_1 X^{n-1} + \cdots + (-1) s_n$$

has roots $r_1, \ldots, r_n$ in a splitting field, then

$$s_k = \sum_{i_1 < \cdots < i_k} r_{i_1} \cdots r_{i_k}.$$

Proposition 9.3.2. *The elementary symmetric polynomials $s_1, \ldots, s_n$ are algebraically independent over K.*

Proof. Since $K \subseteq K(s_1, \ldots, s_n) \subseteq K(t_1, \ldots, t_n)$, where the upper step is algebraic (each t_i is a root of the general polynomial, which has coefficients in $K(s_1, \ldots, s_n)$), Theorem 9.4.9 implies that $S = \{s_1, \ldots, s_n\}$ contains a transcendental basis for $K(t_1, \ldots, t_n)$ over K. But $\{t_1, \ldots, t_n\}$ is a transcendental basis and so tr. deg$(K(t_1, \ldots, t_n)/K) = n$. Hence, S is a transcendental basis. □

Let us compute the Galois group G of $K(t_1, \ldots, t_n)$ over $K(s_1, \ldots, s_n)$. Since $K(t_1, \ldots, t_n)$ is a splitting field for $g(X)$ over $K(s_1, \ldots, s_n)$, and since has $g(X)$ no multiple roots, the extension

$$K(s_1, \ldots, s_n) \subseteq K(t_1, \ldots, t_n)$$

is finite and Galois and so

$$|G| = [K(t_1, \ldots, t_n) : K(s_1, \ldots, s_n)] \leq n!$$

We claim that G is isomorphic to the symmetric group $\mathfrak{S}_n$.

Proposition 9.3.3. *Let $t_1, \ldots, t_n$ be algebraically independent over K and let $s_1, \ldots, s_n$ be the elementary symmetric polynomials in $t_1, \ldots, t_n$.*

(a) The extension $K(s_1, \ldots, s_n) \subseteq K(t_1, \ldots, t_n)$ is Galois of degree $n!$, with Galois group G isomorphic to the symmetric group $\mathfrak{S}_n$.

(b) Inv$(G) = K(s_1, \ldots, s_n)$, *that is, any rational function in $t_1, \ldots, t_n$ that is fixed by the maps in G is a rational function in $s_1, \ldots, s_n$.*

(c) *The general polynomial $g(X)$ is irreducible over $K[s_1, \dots, s_n]$.*

Proof. Let $\sigma \in \mathfrak{S}_n$, we defined a map

$$\sigma^* : K(t_1, \dots, t_n) \to K(t_1, \dots, t_n), \quad f(t_1, \dots, t_n) \mapsto f(t_{\sigma(1)}, \dots, t_{\sigma(n)}).$$

Since the t_i's are algebraically independent over K, this is a well-defined automorphism of $K(t_1, \dots, t_n)$ over K, which fixes the elementary symmetric polynomials s_i's. Thus, σ^* is an automorphism of $K(t_1, \dots, t_n)$ over $K(s_1, \dots, s_n)$, that is, $\sigma^* \in G$. Moreover, each σ^* is distinct, since if $\sigma^* = \tau^*$, then $t_{\sigma(i)} = t_{\tau(i)}$ for all i and so $\sigma = \tau$. It follows that G is isomorphic to $\mathfrak{S}_n$ and

$$[K(t_1, \dots, t_n) : K(s_1, \dots, s_n)] = n!.$$

Since the extension is Galois, the field $K(s_1, \dots, s_n)$ is closed, so $\mathrm{Inv}(G) = K(s_1, \dots, s_n)$. To prove (c), observe that if $g(X)$ were equal to $p(X)q(X)$ where $\deg p = d > 0$ and $\deg q = e > 0$, then the Galois group of $g(X)$ would have size at most $d!e! < (d+e)! = n!$. Hence $g(X)$ is irreducible. □

Now we are ready to define symmetric polynomials (and rational functions).

Definition 9.3.4. *A rational function $f(t_1, \dots, t_n) \in K(t_1, \dots, t_n)$ is* ***symmetric*** *in $t_1, \dots, t_n$ if*

$$f(t_{\sigma(1)}, \dots, t_{\sigma(n)}) = f(t_1, \dots, t_n)$$

for all permutations $\sigma \in \mathfrak{S}_n$, that is, if $f \in \mathrm{Inv}(G) = K(s_1, \dots, s_n)$, where G is the Galois group of the extension $K(s_1, \dots, s_n) \subseteq K(t_1, \dots, t_n)$.

A famous theorem of Isaac Newton describes the symmetric polynomials.

Theorem 9.3.5 (Newton's Theorem). *Let $t_1, \dots, t_n$ be algebraically independent over K and let $s_1, \dots, s_n$ be the elementary symmetric polynomials in $t_1, \dots, t_n$.*

(a) *A polynomial $f(X) \in K[t_1, \dots, t_n]$ is symmetric in $t_1, \dots, t_n$ if and only if it is a polynomial in $s_1, \dots, s_n$, that is, if and only if*

$$f(t_1, \dots, t_n) = p(s_1, \dots, s_n)$$

for some polynomial $p(t_1, \dots, t_n)$ over K. Moreover, if $f(t_1, \dots, t_n)$ has integer coefficients, then so does $p(s_1, \dots, s_n)$.

(b) *Let $f(X) \in K[X]$. Then the set of symmetric polynomials over K in the roots of $f(X)$ is equal to the set of polynomials over K in the coefficients of $f(X)$. In particular, any symmetric polynomial over K in the roots of $f(X)$ is an element of K.*

(c) *Let $f(X) \in \mathbb{Z}[X]$ be a polynomial with integer coefficients. Then the set of symmetric polynomials over $\mathbb{Z}$ in the roots of $f(X)$ is equal to the set of polynomials over $\mathbb{Z}$ in the coefficients of $f(X)$. In particular, any symmetric polynomial over $\mathbb{Z}$ in the roots of $f(X)$ is an integer.*

Proof. Statements (b) and (c) follow from statement (a) and Lemma 9.3.1. If $f(t_1, \dots, t_n)$ has the form $p(s_1, \dots, s_n)$, then it is clearly symmetric. For the converse, the proof consists of a

procedure that can be used to construct the polynomial $p(t_1, \ldots, t_n)$. Unfortunately, while the procedure is quite straightforward, it is recursive in nature and not at all practical.

We use induction on n. The theorem is true for $n = 1$, since $s_1 = t_1$. Assume that the theorem is true for any number of variables less than n and let $f(t_1, \ldots, t_n)$ be symmetric. By collecting powers of t_n, we can write

$$f(t_1, \ldots, t_n) = a_0 + a_1 t_n + \cdots + a_d t_n^d.$$

where each a_i is a polynomial in $t_1, \ldots, t_{n-1}$. Since f is symmetric in $t_1, \ldots, t_{n-1}$ and $t_1, \ldots, t_n$ are independent, each of the coefficients a_i is symmetric in $t_1, \ldots, t_{n-1}$. By the inductive hypothesis, we may express each a_i as a polynomial in the elementary symmetric polynomials on $t_1, \ldots, t_{n-1}$. If these elementary symmetric polynomials are denoted by $u_1, \ldots, u_{n-1}$, then

$$f(t_1, \ldots, t_n) = p_0 + p_1 t_n + \cdots + p_d t_n^d$$

where each p_i is a polynomial in $u_1, \ldots, u_{n-1}$, with integer coefficients if f has integer coefficients.

Note that the symmetric functions s_i can be expressed in terms of the symmetric functions u_i as follows

$$\begin{aligned} s_1 &= u_1 + t_n \\ s_2 &= u_2 + u_1 t_n \\ &\vdots \\ s_{n-1} &= u_{n-1} + u_{n-2} t_n \\ s_n &= u_{n-1} t_n \end{aligned} \tag{3.1.3}$$

These expressions can be solved for the u_i's in terms of the s_i's, giving

$$\begin{aligned} u_1 &= s_1 - t_n \\ u_2 &= s_2 - u_1 t_n = s_2 - s_1 t_n + t_n^2 \\ u_3 &= s_3 - u_2 t_n = s_3 - s_2 t_n + s_1 t_n^2 - t_n^3 \\ &\vdots \\ u_{n-1} &= s_{n-1} - u_{n-2} t_n = s_{n-1} - s_{n-2} t_n + \cdots + (-1)^{n-1} t_n^{n-1}. \end{aligned} \tag{3.1.4}$$

and from the last equation in (3.1.3),

$$0 = s_n - u_{n-1} t_n = s_n - s_{n-1} t_n + \cdots + (-1)^n t_n^n. \tag{3.1.5}$$

Substituting these expressions for the u_i's, and gather together powers of t_n, we get

$$f(t_1, \ldots, t_n) = r_0 + r_1 t_n + \cdots + r_m t_n^m$$

where each r_i is a polynomial in $s_1, \ldots, s_{n-1}$, with integer coefficients if f has integer coefficients. If $m \geq n$, we may reduce the degree in t_n by using (3.1.5), which also introduces the

term s_n. Hence,

$$f(t_1, \dots, t_n) = g_0 + g_1 t_n + \cdots + g_{n-1} t_n^{n-1} \tag{3.1.6}$$

where each g_i is a polynomial in $s_1, \dots, s_n$, with integer coefficients if $f(X)$ has integer coefficients. Since the left side of (3.1.6) is symmetric in the s_i's, we may interchange t_n and t_i, for each $i = 1, \dots, n-1$, to get

$$f(t_1, \dots, t_n) = g_0 + g_1 t_i + \cdots + g_{n-1} t_i^{n-1}$$

valid for all $i = 1, \dots, n$. Hence, the polynomial

$$P(X) = g_0 + g_1 X + \cdots + g_{n-1} X^{n-1} - f(t_1, \dots, t_n)$$

has degree (in X) at most $n-1$ but has n distinct roots $t_1, \dots, t_n$, whence it must be the zero polynomial. Thus, $g_i = 0$ for $i > 0$ and $f(t_1, \dots, t_n) = g_0 = g_0(s_1, \dots, s_n)$ as desired. □

Example 9.3.6. Let $g(X) = X^n - s_1 X^{n-1} + \cdots + (-1)^n s_n$ be the general polynomial with algebraically independent roots $r_1, \dots, r_n$. Let

$$p_i(r_1, \dots, r_n) = r_1^i + \cdots + r_n^i$$

Since the p_i's are symmetric polynomials in the roots of $g(X)$, Theorem 9.3.5 implies that they can be expressed as symmetric polynomials in the elementary symmetric polynomials $s_1, \dots, s_n$. Newton's identities are

$$p_k s_0 - p_{k-1} s_1 + p_{k-2} s_2 + \cdots + (-1)^{k-1} p_1 s_{k-1} + (-1)^k k s_k = 0 \tag{3.1.7}$$

valid for $k \geq 1$, where $s_0 = 1$ and $s_i = 0$ for $i > n$. For $k > n$, this equality is easy to prove by considering the sum

$$\begin{aligned} 0 = \sum_{i=1}^n r_i^{k-n} g(r_i) &= \sum_{i=1}^n (r_i^k - s_1 r_i^{k-1} + \cdots + (-1)^n r_i^{k-n} s_n) \\ &= \sum_{i=1}^n r_i^k - s_1 \sum_{i=1}^n r_i^{k-1} + \cdots + (-1)^n s_n \sum_{i=1}^n r_i^{k-n} \\ &= p_k - p_{k-1} s_1 + \cdots + (-1)^k p_{k-n} s_k \end{aligned}$$

and an similar argument prove the case $k = n$. For $1 \leq k < n$, we proceed by induction on n. Let $N_k^{(n)}(r_1, \dots, r_n)$ denote the left-sider of (3.1.7). Then we can see

$$N_k^{(n)}(r_1, \dots, r_{n-1}, 0) = N_k^{(n-1)}(r_1, \dots, r_{n-1}).$$

This implies $r_n \mid N_k^{(n)}(r_1, \dots, r_{n-1}, 0)$, and hence $s_n = r_1 \cdots r_n \mid N_k^{(n)}(r_1, \dots, r_n)$ by symmetricity on $r_1, \dots, r_n$. But this is impossible for $k < n$, since $p_{k-i} s_i$ does not contain the term $r_1 \dots r_n$ for $i < n$. This implies $N_k^{(k)}(r_1, \dots, r_n) = 0$.

Example 9.3.7.

9.3.1.2 The discriminant of a polynomial

We have seen that the Galois group $\mathrm{Gal}_K(f(X))$ of a polynomial of degree n is isomorphic to a subgroup of the symmetric group $\mathfrak{S}_n$ and that the Galois group of a general polynomial is isomorphic to $\mathfrak{S}_n$ itself. A special symmetric function of the roots of $f(X)$, known as the discriminant, provides a tool for determining whether the Galois group is isomorphic to a subgroup of the alternating group $\mathfrak{A}_n$.

Let $f(X)$ be a polynomial over K, with roots $r_1, \ldots, r_n$ in a splitting field E. Let

$$\Delta = \prod_{i<j}(r_i - r_j)$$

The **discriminant** of $f(X)$ is $D = \Delta^2$, which is clearly symmetric in the roots.

Proposition 9.3.8. *Let $f(X) \in K[X]$ have degree n and splitting field E. Let $\sqrt{D}$ be any square root of the discriminat D of $f(X)$.*

(1) $D = 0$ if and only if $f(X)$ has multiple roots.

(2) Assume that $D \neq 0$ and $\mathrm{char}(K) \neq 2$.

(a) $\sqrt{D} \in K$ if and only if $\mathrm{Gal}_K(f(X))$ is isomorphic to a subgroup of $\mathfrak{A}_n$.

(b) $\sqrt{D} \notin K$ if and only if $\mathrm{Gal}_K(f(X))$ is isomorphic to a subgroup of $\mathfrak{S}_n$ that contains half odd and half even permutations. In this case,

$$E^{\mathrm{Gal}_K(f(X))\cap\mathfrak{A}_n} = K(\sqrt{D}).$$

(3) If $D \neq 0$ and $\mathrm{char}(K) = 2$, then $\sqrt{D} \in K$ but $\mathrm{Gal}_K(f(X))$ need not be isomorphic to a subgroup of $\mathfrak{A}_n$.

Proof. Let $\Delta = \sqrt{D}$. Each transposition of the roots sends Δ to $-\Delta$, so for any $\sigma \in \mathrm{Gal}_K(f(X))$,

$$\sigma(\Delta) = (-1)^\sigma \Delta.$$

If $\mathrm{char}(K) = 2$, then $\sigma(\Delta) = \Delta$ for all $\sigma \in \mathrm{Gal}_K(f(X))$ and so Δ is always in the base field K. If $\mathrm{char}(K) \neq 2$, then $\sigma \in \mathrm{Gal}_K(f(X))$ fixes Δ if and only if σ is an even permutation. Put another way, $\Delta \in E^{\mathrm{Gal}_K(f(X))}$ if and only if $\mathrm{Gal}_K(f(X))$ contains only even permutations, that is, $\mathrm{Gal}_K(f(X)) \subseteq \mathfrak{A}_n$.

If $\Delta \notin K$ then $\mathrm{Gal}_K(f(X))$ must contain an odd permutation, and thus exactly half of its elements are even. Hence, if $\Delta \notin K$ then $G = \mathrm{Gal}_K(f(X))$ has even order and $|G \cap \mathfrak{A}_n| = |G|/2$, that is,

$$[G : G \cap \mathfrak{A}_n] = 2.$$

Since all groups are closed, it follows that

$$[E^{G\cap\mathfrak{A}_n} : E^G] = [G : G \cap \mathfrak{A}_n] = 2.$$

Since $[K(\Delta) : K] = 2$ and $K(\Delta) \subseteq E^{G\cap\mathfrak{A}_n}$, we get

$$K(\Delta) = E^{G\cap\mathfrak{A}_n}.$$

Thus, $K(\Delta)$ is the fixed field of the subgroup of even permutations in $\mathrm{Gal}_K(f(X))$. □

The usefulness of Proposition 9.3.8 comes from the fact that D can actually be computed without knowing the roots of $f(X)$ explicitly. This follows from the fact that Δ is the Vandermonde determinant

$$\Delta = \begin{vmatrix} 1 & 1 & 1 & 1 \\ r_1 & r_2 & \cdots & r_n \\ \vdots & \vdots & \cdots & \vdots \\ r_1^{n-1} & r_2^{n-2} & \cdots & r_n^{n-1} \end{vmatrix}$$

Multiplying this by its transpose gives

$$D = \begin{vmatrix} p_0 & p_1 & \cdots & p_{n-1} \\ p_1 & p_2 & \cdots & p_n \\ \vdots & \vdots & \cdots & \vdots \\ p_{n-1} & pn & \cdots & p_{2n-2} \end{vmatrix}$$

where $p_i = r_1^i + \cdots + r_n^i$. Newton's identities can then be used to determine the u_i's in terms of the coefficients of the polynomial $f(X)$.

9.3.2 The Galois groups of some polynomials

9.3.2.1 The quadratic

Quadratic extensions (extensions of degree 2) hold no surprises. Let

$$f(X) = X^2 + bX + c = (X - \alpha)(X - \beta)$$

be a quadratic over K, with splitting field E. To compute the discriminant, observe that

$$p_1 = \alpha + \beta = -b, \quad p_2 = \alpha^2 + \beta^2 = (\alpha + \beta)^2 - 2\alpha\beta = b^2 - 2c.$$

Hence

$$D = \begin{vmatrix} 2 & -b \\ -b & b^2 - 2c \end{vmatrix} = 2(b^2 - 2c) - b^2 = b^2 - 4c$$

a familiar quantity.

If $D = 0$, then $f(X)$ has a double root α and

$$f(X) = (X - \alpha)^2 = X^2 - 2\alpha X + \alpha^2.$$

The root α will lie in K for most well-behaved base fields K. In particular, if $\mathrm{char}(K) \neq 2$, then $2\alpha \in K$ implies $\alpha \in K$. If $\mathrm{char}2 = 2$ and K is perfect (a finite field, for example) then $(X - \alpha)^2$ must be reducible over K and so $\alpha \in K$.

However, the following familiar example shows that $f(X)$ may have a multiple root not lying in K. Let $K = \mathbb{F}_2(t^2)$ where t is transcendental over $\mathbb{F}_2$ and let

$$f(X) = X^2 - t^2 = (X - t)^2.$$

Since $t \notin \mathbb{F}_2(t^2)$, this polynomial is irreducible over $\mathbb{F}_2(t^2)$, but has a multiple root t.

If $D \neq 0$, then $f(X)$ has distinct roots and there are two possibilities:

(1) The roots lie in K, $f(X)$ is reducible and $\mathrm{Gal}_K(f(X))$ is trivial.

(2) The roots do not lie in K, $f(X)$ is irreducible and $\mathrm{Gal}_K(f(X)) \cong \mathfrak{S}_2$ is generated by the transposition (12) of the roots.

We can summarize these arguments into the following proposition.

Proposition 9.3.9. *Let $f(X) \in K[X]$ have degree 2.*

(1) If $D = 0$ then $f(X)$ has a double root α. If $\mathrm{char}(K) \neq 2$ or K is perfect, then $\alpha \in K$. In any case, $\mathrm{Gal}_K(f(X))$ is trivial.

(2) If $D \neq 0$ then $f(X)$ has distinct roots and there are two possibilities:

(a) The roots lie in K, $f(X)$ is reducible and $\mathrm{Gal}_K(f(X))$ is trivial.

(b) The roots do not lie in K, $f(X)$ is irreducible and $\mathrm{Gal}_K(f(X))$ is generated by the transposition of the roots.

When $\mathrm{char}(K) \neq 2$, we can distinguish the two cases as follows: Case (a) holds if $\sqrt{D} \in K$ and case (b) holds if $\sqrt{D} \notin K$.

9.3.2.2 The cubic

Let $f(X) \in K[X]$ be a polynomial of degree 3. Then it has the following form:

$$f(X) = X^3 + bX^2 + cX + d = (X - r)(X - s)(X - t) \in K[X]$$

If $f(X)$ is reducible, then it can be factored over K:

$$f(X) = (X - r)(X^2 + pX + q)$$

where $g(X) = X^2 + pX + q$ is irreducible over K. Hence the Galois group is isomorphic to $\mathfrak{S}_2$ if $g(X)$ is irreducible, and is $\{1\}$ is $g(X)$ is also reducible.

Now let us assume that $f(X)$ is irreducible, and let E be its splitting field. A lengthy computation gives

$$\Delta = -4b^3d + b^2c^2 + 18bcd - 4c^3 - 27d^2,$$

but one may remember the trick of shifting x by $a/3$ (in characteristic $\neq 3$), with the effect of killing the coefficient of X^2:

$$f(X - \frac{a}{3}) = X^3 + pX + q$$

for suitable p and q. This does not change D (shifting all roots α_i by the same amount has no effect on the differences $\alpha_i - \alpha_j$), yet

$$D = -4p^3 - 27q^2$$

is a little more memorable.

If $D = 0$, then $f(X)$ has multiple roots and since each root must have the same multiplicity, we are left with $\mathrm{char}(K) = 3$ and

$$f(X) = (X - r)^3 = X^3 - r^3$$

Hence, the extension $K \subseteq K(r) = E$ is purely inseparable of degree 3 and the Galois group is trivial.

If $D \neq 0$, then $f(X)$ has no multiple roots and is therefore separable. Hence, $K \subseteq E$ is Galois and

$$3 \leq |\mathrm{Gal}_K(f(X))| = [E : K] = 3!$$

which leaves the possibilities $[E : K] = 3$ or $[E : K] = 6$.

We can now give a complete analysis for the cubic. Note that when $\mathrm{char}(K) \neq 2$, knowledge of irreducibility and the value of $\sqrt{D}$ determine the Galois group and the splitting field.

Proposition 9.3.10 (The cubic). *Let $f(X) \in K[X]$ be a separable polynomial of degree 3, with splitting field E and Galois group $G = \mathrm{Gal}_K(f(X))$. Then there are four mututally exclusive possibilities, each of which can be characterized in three equivalent ways:*

(1) *(a)* $[E : K] = 1$,
(b) $E = K$,
(c) $G = \{1\} = \mathfrak{A}_2$,
(d) *(For* $\mathrm{char}(K) \neq 2$*)* *$f(X)$ is reducible and $\sqrt{D} \in K$.*

(2) *(a)* $[E : K] = 2$,
(b) *$f(X)$ is reducible and $E = K(r)$ is a splitting field for $f(X)$, where r is a root not in K.*
(c) $G = \mathfrak{S}_2 \cong \mathbb{Z}/2\mathbb{Z}$,
(d) *(For* $\mathrm{char}(K) \neq 2$*)* *$f(X)$ is reducible and $\sqrt{D} \notin K$.*

(3) *(a)* $[E : K] = 3$,
(b) *$f(X)$ is irreducible and $E = K(r)$ is the splitting field for K, for any root r.*
(c) $G = \mathfrak{A}_3 \cong \mathbb{Z}/3\mathbb{Z}$.
(d) *(For* $\mathrm{char}(K) \neq 2$*)* *$f(X)$ is irreducible and $\sqrt{D} \in K$.*

(4) *(a)* $[E : K] = 6$,
(b) *$f(X)$ is irreducible and $E = K(\sqrt{D}, r)$ is the splitting field for $f(X)$, for any root r.*
(c) $G = \mathfrak{S}_3$.
(d) *(For* $\mathrm{char}(K) \neq 2$*)* *$f(X)$ is irreducible and $\sqrt{D} \notin K$.*

Proof. Since f is separable, E/K is a Galois extension, so we have $[E : K] = |G|$. This is aldeary enough to classifies the Galois group G. We turn to other equivalences.

Let f be reducible:

$$f(X) = (X - r)(X^2 + px + q).$$

If $\mathrm{char}(K) \neq 2$, then $G = \{1\}$ if and only if $g(X) := X^2 + pX + q$ is reducible, and $G = \mathfrak{S}_2$ if and only if $g(X)$ is irreducible. Since

$$D_f = (r - t)^2(r - s)^2(t - s)^2 = (r^2 - (t + s)r + ts)^2(t - s)^2 = (r^2 - (t + s)r + ts)^2 D_g,$$

we see $\sqrt{D}_f \in K$ if and only if $\sqrt{D}_g \in K$, Hence the claim of (1) and (2) follows.

Now assume that f is irreducible, so that no roots of $f(X)$ lies in K. Then since any root of $f(X)$ has degree 3 over K, we conclude that $[E : K] = |G| \geq 3$. By Proposition 9.3.8 $\sqrt{D} \in K$ if and only if $G \subseteq \mathfrak{A}_3 \cong \mathbb{Z}/3\mathbb{Z}$, which then implies $G = \mathfrak{A}_3$. Therefore (3) holds. The other case is $\sqrt{D} \notin K$, which implies $G = \mathfrak{S}_3$ by order consideration. This completes the proof. □

We know that $D \in K$. For $K = \mathbb{Q}$, we can learn more about the roots of a cubic by looking at the sign of D. A cubic $f(X)$ over $\mathbb{Q}$ has either one real root r and two nonreal roots $\{a+bi, a-bi\}$ or three real roots r, s and t. In the former case,

$$\Delta = (r - a - bi)(r - a + bi)2bi = |(r - a) + bi|^2 2bi$$

and so $D < 0$. In the latter case $D = (r - s)^2(r - t)^2(s - t)^2 > 0$.

Proposition 9.3.11 (The cubic over $\mathbb{Q}$). *Let $f(X) \in \mathbb{Q}[X]$ have degree 3. Then*

(a) $D < 0$ if and only if $f(X)$ has exactly one real root,

(b) $D > 0$ if and only if $f(X)$ has three real roots.

Example 9.3.12. Let $f(X) = X^3 - 2X^2 - X + 1$ over $\mathbb{Q}$. Any rational root of $f(X)$ must be $\mathfrak{m}1$ and so $f(X)$ is irreducible. The discriminant is $D = 49 > 0$, so $f(X)$ has three real roots. Since $\sqrt{D} = 7 \in \mathbb{Q}$, we have $\mathrm{Gal}_{\mathbb{Q}}(f(X)) \cong \mathfrak{A}_3 \cong \mathbb{Z}/3\mathbb{Z}$ and $f(X)$ has splitting field $\mathbb{Q}(r)$, for any root r.

Example 9.3.13. For any prime p, the polynomial $f(X) = X^3 - p$ is irreducible over $\mathbb{Q}$ and has discriminant $D = -27p^2 < 0$, whose square root is not in $\mathbb{Q}$. Hence, $f(X)$ has one real root and two nonreal roots, the Galois group of $\mathrm{Gal}_{\mathbb{Q}}(f(X))$ is isomorphic to $\mathfrak{S}_3$ and $f(X)$ has splitting field $\mathbb{Q}(\sqrt{-3}, \sqrt[3]{p})$.

Example 9.3.14. Let $f(X) \in \mathbb{Q}[X]$ be an irreducible polynomial of degree p, where p is prime. Assume that $f(X)$ has $p - 2$ real roots and 2 nonreal, complex roots. Then the Galois group of $f(X)$ is $\mathfrak{S}_p$.

Indeed, complex conjugation induces an automorphism of the splitting field and acts by interchanging the two nonreal roots, so the Galois group G, as a subgroup of $\mathfrak{S}_p$, contains a transposition. On the other hand, the degree of the splitting field (and hence $|G|$) is divisible by p, because it contains a simple extension of order p, obtained by adjoining any one root to $\mathbb{Q}$. Since p is prime, G contains an element of order p by Cauchy's theorem; the only elements of order p in $\mathfrak{S}_p$ are p-cycles, so G contains a p-cycle. It follows that $G = \mathfrak{S}_p$.

For example, the Galois group of $f(X) = X^5 - 5X - 1$ over $\mathbb{Q}$ is $\mathfrak{S}_5$, giving a concrete example of a quintic that cannot be solved by radicals

9.3.3 Geometric impossibilities

9.3.3.1 Constructions by straightedge and compass

We begin with two points O, P in the ordinary, real plane. You are allowed to mark more points and other geometric figures in the plane, but only according to the following rules:

- If you have constructed two points A, B, then you can draw the line joining them (using your straightedge).
- If you have constructed two points A, B, then you can draw the circle with center at A and containing B (using your compass).
- You can mark any number of points of intersection of any two distinct lines, line and circle, or circles that you have drawn already.

The general question is to decide whether a figure can or cannot be constructed this way. Three problems of this kind became famous in antiquity:

- trisecting angles.
- squaring circles.
- doubling cubes.

Preppendicular lines and parallel lines are constructible.

Definition 9.3.15. *A real number r is **constructible** if the point $(r, 0)$ is constructible with straightedge and compass (assuming $O = (0, 0)$ and $P = (1, 0)$, as above). We will denote by $\mathscr{C}_{\mathbb{R}} \subseteq \mathbb{R}$ the set of constructible real numbers.*

Also, we can identify the real plane with $\mathbb{C}$, placing O at 0 and P at 1, and we say that $z = x + iy$ is **constructible** if the point (x, y) is constructible by straightedge and compass. We will denote by $\mathscr{C}_{\mathbb{C}} \subseteq \mathbb{C}$ the set of constructible complex numbers. Summarizing the foregoing discussion, we have proved:

Proposition 9.3.16. *A point (x, y) is constructible by straightedge and compass if and only if $x + iy \in \mathscr{C}_{\mathbb{C}}$, if and only if $x, y \in \mathscr{C}_{\mathbb{R}}$.*

Proposition 9.3.17. *The subset $\mathscr{C}_{\mathbb{R}}$ of constructible numbers is a subfield of $\mathbb{R}$. Likewise, $\mathscr{C}_{\mathbb{C}}$ is a subfield of $\mathbb{C}$, and in fact $\mathscr{C}_{\mathbb{C}} = \mathscr{C}_{\mathbb{R}}(i)$.*

We may view $\mathscr{C}_{\mathbb{R}}$ and $\mathscr{C}_{\mathbb{C}}$ as extensions of $\mathbb{Q}$, drawing a bridge between constructibility by straightedge and compass and field theory: we will be able to understand constructibility of geometric figures if we can understand the field extensions

$$\mathbb{Q} \subseteq \mathscr{C}_{\mathbb{R}} \subseteq \mathscr{C}_{\mathbb{C}}.$$

9.3.3.2 Constructible numbers and quadratic extensions

Our goal is to prove the following amazingly explicit description of $\mathscr{C}_{\mathbb{R}}$ (immediately implying one for $\mathscr{C}_{\mathbb{C}}$).

Theorem 9.3.18. *Let $\gamma \in \mathbb{R}$. Then $\gamma \in \mathscr{C}_{\mathbb{R}}$ if and only if there exist real numbers $\delta_1, \ldots, \delta_k$ such that $\forall j = 1, \ldots, k$*

$$[\mathbb{Q}(\delta_1, \ldots, \delta_j) : \mathbb{Q}(\delta_1, \ldots, \delta_{j-1})] = 2$$

and $\gamma \in \mathbb{Q}(\delta_1, \ldots, \delta_k)$.

Proof. Let's first argue in the geometry to algebra direction. A configuration of points, lines, and circles obtained by a straightedge-and-compass construction may be described by the coordinates of the points and the equations of the lines and circles. Suppose that at one stage in a given construction all coordinates of all points and all coefficients in the equations of lines and circles belong to a field F; we will say that the configuration is **defined over** K.

Then we claim that for every object constructed at the next stage, there exists a number $\delta \in \mathbb{R}$, of degree at most 2 over K, such that the new configuration is defined over $F(\delta)$. The only if part of the theorem follows by induction on the number of steps in the construction, since at the beginning the configuration (that is, the pair of points $O = (0,0)$, $P = (1,0)$) is defined over $\mathbb{Q}$.

Verifying our claim amounts to verifying it for the basic operations defining straightedge-and-compass constructions. Clearly the point of intersection of two lines defined over K has coordinates in K and that lines and circles determined by points with coordinates in K are defined over K. So $\delta = 1$ works in all these cases.

For the intersection of a line ℓ and a circle C, assume that ℓ is not parallel to the y-axis (the argument is entirely analogous otherwise) and that it does meet C; let

$$y = mx + r$$

be the equation of ℓ and let

$$x^2 + y^2 + ax + by + c = 0$$

be the equation of C. We are assuming that $a, b, c, m, r \in K$. Then the x coordinates of the points of intersection of ℓ and C are the solutions of the equation

$$x^2 + (mx + r)^2 + ax + b(mx + r) + c = 0$$

The quadratic formula shows that these coordinates belong to the field $F(\sqrt{D})$ where D is the discriminant of this polynomial: explicitly,

$$D = (2mr + bm + a)^2 - 4(m^2 + 1)(r^2 + br + c)$$

but this is unimportant. What is important is that $D \in K$; hence $\delta = \sqrt{D}$ satisfies our requirement.

For the intersection of two (distinct) circles defined over K, nothing new is needed: if

$$\begin{cases} x^2 + y^2 + a_1x + b_1y + c_1 = 0 \\ x^2 + y^2 + a_2x + b_2y + c_2 = 0 \end{cases}$$

are two circles, subtracting the two equations shows that their points of intersection coincide with the points of intersection of a circle and a line:

$$\begin{cases} x^2 + y^2 + a_1x + b_1y + c_1 = 0 \\ (a_1 - a_2)x + (b_1 - b_2y) + (c_1 - c_2) = 0 \end{cases}$$

with the same conclusion as in the previous case.

This completes the verification of the only if part of the theorem. To prove that every ele-

ment of an extension as stated is constructible, again argue by induction: it suffices to show that if (i) $\delta \in \mathbb{R}$, (ii) all elements of K are constructible, and (iii) $r = \delta^2 \in K$, then δ is constructible (note that in order to construct an element of degree 2 over K, it suffices to construct the square root of the discriminant of its minimal polynomial). Therefore, all we have to show is that we can **take square roots** by a straightedge-and-compass construction. Here is the picture (if $r > 1$) If $A = (r, 0)$ is constructible, so is $B = (-r, 0)$; C is the midpoint of the segment

Figure 3.3.1: squre root

BP (midpoints are constructible); the circle with center C and containing P intersects the positive y-axis at a point $Q = (0, \delta)$, and elementary geometry shows that $\delta^2 = r$. Therefore δ is constructible, concluding the proof of the theorem. □

Corollary 9.3.19. *Let $\gamma \in \mathscr{C}_{\mathbb{C}}$ be a constructible number. Then $[\mathbb{Q}(\gamma) : \mathbb{Q}]$ is a power of 2.*

Proof. By Proposition 9.3.17 and Theorem 9.3.18, there exist $\delta_1, \ldots, \delta_k \in \mathbb{R}$ such that

$$\gamma \in \mathbb{Q}(\delta_1, \ldots, \delta_k, i)$$

and each δ_j has degree ≤ 2 over $\mathbb{Q}(\delta_1, \ldots, \delta_{j-1})$. Repeated application of Proposition 9.1.13 shows that

$$[\mathbb{Q}(\delta_1, \ldots, \delta_k, i) : \mathbb{Q}]$$

is a power of 2, and since

$$\mathbb{Q} \subseteq \mathbb{Q}(\gamma) \subseteq \mathbb{Q}(\delta_1, \ldots, \delta_k, i)$$

the claim follows from Corollary 9.1.14. □

As an example, constructing a regular 7-gon would amount to constructing a 7-th (complex) root of 1, ζ. By definition, ζ satisfies

$$t^7 - 1 = (t - 1)(t^6 + t^5 + \cdots + t + 1)$$

as $\zeta \neq 1$, ζ must satisfy the cyclotomic polynomial $t^6 + \cdots + 1$. This is irreducible, hence again we find that ζ has degree 6 over $\mathbb{Q}$, and Corollary 9.3.19 implies that the regular 7-gon cannot be constructed with straightedge and compass.

Of course 7 is not too special: if p is a positive prime integer, the **cyclotomic polynomial** of degree $p-1$ is irreducible; hence

$$[\mathbb{Q}(\zeta_p):\mathbb{Q}] = p-1$$

where ζ_p is the complex p-th root of 1 with argument $2\pi/p$. Therefore, Corollary 9.3.19 reveals that if p is prime, then the regular p-gon can be constructed only if $p-1$ is a power of 2. This is even more restrictive than it looks at first, due to the following simple lemma.

Lemma 9.3.20. *If 2^k+1 is prime, then K is a power of 2.*

Proof. First note the fractorization:

$$t^{2m+1}+1 = (t+1)(t^{2m}-t^{2m-1}+\cdots+1).$$

Thus K is not odd. Assume that $k=2m$, then $2^k+1 = 2^{2m}+1 = 4^m+1$. Repeat this argument we see m is also odd, and finally we conclude that K is a power of 2. □

Primes of the form $2^{2^\ell}+1$ are called **Fermat primes**. Therefore for a prime p, the regular p-gon if constructible only if p is a Fermat prime.

We now use Galois theory to deal with the constructibility of regular n-gons. The key ingredient is the following result.

Proposition 9.3.21. *Let E/K be a Galois extension, and assume $[F:K] = p^r$ for some prime p and $r \geq 0$. Then there exist intermediate fields*

$$K = E_0 \subseteq E_1 \subseteq E_2 \subseteq \cdots \subseteq E_r = F$$

such that $[E_i : E_{i-1}] = p$ for $i = 1, \ldots, r$.

Proof. As the Galois correspondence is bijective for Galois extensions, this statement follows immediately from the fact that a group of order p^r, with p prime, has a complete series of p-subgroups. □

Theorem 9.3.22. *The regular n-gon is constructible by straightedge and compass if and only if $\phi(n)$ is a power of 2, if and only if $n = 2^m p_1 \cdots p_r$, where $m \geq 0$ and the factors p_i are distinct Fermat primes.*

Proof. We first prove the first equivalence. One direction is proved in Theorem 9.3.18. For the converse, assume $\phi(n) = 2^r$ for some r. The extension $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_n)$ is Galois (it is the splitting field of $\Phi_n(X)$), of order $[\mathbb{Q}(\zeta_n):\mathbb{Q}] = \phi(n) = 2^r$. Proposition 9.3.21 shows that the condition given in Theorem 9.3.18 is satisfied and therefore that ζ_n is constructible, as needed.

Now let $\phi(n)$ be a power of 2. From the equation

$$\phi(n) = p_1^{k_1-1}(p_1-1)p_2^{k_2-1}(p_2-1)\cdots p_i^{k_i-1}(p_i-1)$$

we see that if $k_i - 1 > 0$, then $p_i = 2$. If $k_i - 1 = 0$, then $p_i = 2^m+1$ should be a prime, so p_i is a Fermat prime. Hence $n = 2^m p_1 \cdots p_r$. The converse can also be deduced from the equality above. □

9.3.4 The fundamental theorem of algebra

Theorem 9.3.23. *$\mathbb{C}$ is algebraically closed.*

Proof. Let $f(X) \in \mathbb{C}[X]$ be a nonconstant polynomial; we have to prove that $f(X)$ has roots in $\mathbb{C}$. Note that if $f(X)$ has no roots in $\mathbb{C}$, then neither does $f(X)\overline{f(X)} \in \mathbb{R}[X]$; that is, we may assume that $f(X)$ has real coefficients.

Now consider a tower $\mathbb{R} \subseteq \mathbb{C} \subseteq E$, where E is a splitting field for $p(X) = (X^2+1)f(X)$ over $\mathbb{R}$. Since $[\mathbb{C} : \mathbb{R}] = 2$ divides $[E : \mathbb{R}]$, we conclude that $[E : \mathbb{R}] = 2^k m$, for some $k > 1$ with m odd. Our goal is to show that $E = \mathbb{C}$, showing that $f(X)$ splits over $\mathbb{C}$.

Let P be a 2-Sylow subgroup of $\mathrm{Gal}_{\mathbb{R}}(f(X))$. Then $|P| = 2^k$ and so

$$[E^P : \mathbb{R}] = [\mathrm{Gal}_{\mathbb{R}}(f(X)) : P] = m.$$

By intermediate value theorem, every real polynomial with odd degree must have a root in $\mathbb{R}$, it follows that any nontrivial finite extension of $\mathbb{R}$ must have even degree (its primitive element must has even degree). From this we deduce that $m = 1$ and $G = \mathrm{Gal}_{\mathbb{R}}(f(X))$ is a 2-group of order 2^k. Thus we have the tower

$$\{1\} \subseteq \mathrm{Gal}_{\mathbb{C}}(f(X)) \subseteq G$$

in which $|\mathrm{Gal}_{\mathbb{C}}(f(X))| = 2^{k-1}$. Therefore, according to Cauchy's theorem, $\mathrm{Gal}_{\mathbb{C}}(f(X))$ has a subgroup of any order dividing 2^{k-1}. But $\mathrm{Gal}_{\mathbb{C}}(f(X))$ cannot have a subgroup of order 2^{k-2} that is, index 2: if H is such a group, then

$$\{1\} \subseteq H \subseteq \mathrm{Gal}_{\mathbb{C}}(f(X)) \subseteq G$$

and then

$$2 = [E^H : E^{\mathrm{Gal}_{\mathbb{C}}(f(X))}] = [E^H : \mathbb{C}],$$

which is impossible, since $\mathbb{C}$ does not have any irreducible polynomial of degree 2. It follows that $|\mathrm{Gal}_{\mathbb{C}}(f(X))| = 1$ and so $|G| = 2$, which implies that $[E : \mathbb{R}] = 2$, whence $E = \mathbb{C}$. □

9.3.5 Finite fields

Let F be a finite field, and let p be its characteristic. We know that F may be viewed as an extension

$$\mathbb{F}_p \subseteq F$$

of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$; let $n = [F : F_p]$. Since F has dimension n as a vector space over $\mathbb{F}_p$, it is isomorphic to $\mathbb{F}_p^n$ as a vector space, and in particular $|F| = p^n$ is a power of p.

9.3.5.1 Finite fields as splitting fields

Let F be a finite field of size q. Then $F^\times$ has order $q-1$ and so every element $\alpha \in F$ has exponent $q-1$, that is, $\alpha^{q-1} = 1$. It follows that every element of F is a root of the polynomial

$$f_q(X) = X^q - X$$

Since $f_q'(X) = -1$, this polynomial has no multiple roots and so F is precisely the set of roots of $f_q(X)$ in some splitting field. In fact, since F is a field, it is a splitting field for $f_q(X)$ over the prime subfield $\mathbb{F}_p$. We have the following theorem:

Theorem 9.3.24. *Let $q = p^n$ be a power of a prime integer p.*

(a) The splitting field of the polynomial $f_q(X) = X^q - X$ over $\mathbb{F}_p$ is a field with precisely q elements.

(b) Let F be a field with exactly q elements; then F is a splitting field for $X^q - X$ over $\mathbb{F}_p$. The polynomial $X^q - X$ is separable over $\mathbb{F}_p$.

In particular, for every prime power q there exists one and only one finite field of order q, up to isomorphism.

Proof. Let F be the splitting field of $X^q - X$ over $\mathbb{F}_p$. Let E be the set of roots of $f(X) = X^q - X$ in F. Since $f'(X) = qX^{q-1} - 1 = -1$ (as $q = 0$ in characteristic p), we have $(f(X), f'(X)) = 1$; hence by Proposition 9.1.54 $f(X)$ is separable, and E consists of precisely q elements. We claim that E is a field, and it follows that $E = F$.

To see that E is a field, let $a, b \in E$. Then $a^q = a$ and $b^q = b$; it follows that

$$(a - b)^q = a^p + (-1)^q b^q = a^q - b^q = a - b.$$

(note that $(-1)^q = -1$ if p is odd and $(-1)^q = +1 = -1$ if $p = 2$). If $b \neq 0$,

$$(ab^{-1})^q = a^q (b^q)^{-1} = ab^{-1}.$$

Thus E is closed under subtraction and division by a nonzero element, proving that E is a field and concluding the proof of the first statement.

To prove the second statement, let F be a field with exactly q elements. The nonzero elements of F form a group under multiplication consisting of $q - 1$ elements. Therefore for any elments in $a \in F^\times$ we have $a^{q-1} = 1$. Of course $0^q - 0 = 0$, so the polynomial $X^q - X$ has q roots in F; it follows that F is a splitting field for $X^q - X$, as stated. The final statement comes from the uniqueness of splitting fields. This completes the proof. □

Let us refer to the polynomial $f_q(X) = X^q - X$ as the **defining polynomial** of the finite field $\mathbb{F}_{p^n}$. In view of this theorem, we will often refer to the finite field $\mathbb{F}_{p^n}$.

An immediate consequence of the splitting field characterization of finite fields is that any extension of finite fields is normal.

Corollary 9.3.25. *The extension $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$ is a finite Galois extension. Hence, in the Galois correspondence for $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$, all intermediate fields and all subgroups are closed.*

Example 9.3.26. Let p be a prime integer. Then we claim that the polynomial X^4+1 is **reducible** over $\mathbb{F}_p$ (and therefore over every finite field).

Since $X^4 + 1 = (X + 1)^4$ in $\mathbb{F}_2[X]$, the statement holds for $p = 2$. Thus, we may assume that p is an odd prime. Then we claim that $X^4 + 1$ divides $X^{p^2} - X$. Indeed, the square of every odd number is congruent to 1 mod 8; hence $X^8 - 1$ divides $X^{p^2-1} - 1$, which implies

$$(X^4 + 1) \mid (X^8 - 1) \mid (X^{p^2-1} - 1) \mid (X^{p^2} - X)$$

It follows that X^4+1 factors completely in the splitting field of $X^{p^2}-X$, that is, in $\mathbb{F}_{p^2}$. If α is a root of X^4+1 in $\mathbb{F}_{p^2}$, we have the extensions

$$\mathbb{F}_p \subseteq \mathbb{F}_p(\alpha) \subseteq \mathbb{F}_{p^2}$$

therefore $[\mathbb{F}_p(\alpha):\mathbb{F}_p]$ divides $[\mathbb{F}_{p^2}:\mathbb{F}_p]=2$. That is, α has degree 1 or 2 over $\mathbb{F}_p$. But then its minimal polynomial is a factor of degree 1 or 2 of (X^4+1), showing that the latter is reducible.

Now we wish to examine the subfields of a finite field $\mathbb{F}_{p^n}$. Note that if d and n are positive integers and $n=kd+r$ for $0\le r<d$, then it is easy to see $X^d-1 \mid X^n-1$ if and only if $d\mid n$. This yields the following result on subfields of $\mathbb{F}_{p^n}$.

Proposition 9.3.27 (Classfication of Subfields of $\mathbb{F}_{p^n}$). *The following are equivalent:*

(i) The interger d divides n.

(ii) The defining polynomial $f_{p^d}(X)$ divides the defining polynomial $f_{p^n}(X)$.

(iii) The field $\mathbb{F}_{p^d}$ is contained in $\mathbb{F}_{p^n}$.

Put another way, the following lattices are isomorphic:

(a) $\{d : d$ divides $n\}$, under division.

(b) $\{f_{p^d}(X) : f_{p^d}(X)$ divides $f_{p^n}(X)\}$, under division.

(c) Subfields of $\mathbb{F}_{p^n}$, under set inclusion.

Moreover, $\mathbb{F}_{p^n}$ has exactly one subfield of size p^d, for each d divides n, and each extension $\mathbb{F}_{p^d}\subseteq\mathbb{F}_{p^n}$ is simple.

Proof. To start with, we first prove the following facts:

$$p^d-1 \mid p^n-1 \Leftrightarrow d\mid n \Leftrightarrow X^d-1\mid X^n-1 \tag{3.5.1}$$

In fact, write $n=kd+r$ with $0\le r<d$, then

$$X^n-1 = X^{kd+r}-X^r+X^r-1 = X^r(X^{kd}-1)+X^r-1.$$

Since $X^d-1\mid X^{kd}-1$, this implies

$$X^n-1\equiv X^r-1 \mod X^d-1$$

which proves (3.5.1) immediately. Now apply these results with Theorem 9.3.24, we obtain that

$$d\mid n \Leftrightarrow p^d-1\mid p^n-1 \Leftrightarrow X^{p^d-1}-1\mid X^{p^n-1}-1 \Leftrightarrow f_{p^d}(X)\mid f_{p^n}(X).$$

which says (i) and (ii) are equivalent. Moreover, by Theorem 9.3.24,

$$\mathbb{F}_{p^d}\subseteq\mathbb{F}_{p^n} \Leftrightarrow \mathrm{Root}(f_{p^d}(X))\subseteq\mathrm{Root}(f_{p^n}(X)) \Leftrightarrow f_{p^d}(X)\mid f_{p^n}(X).$$

so (ii) and (iii) are also equivalent. Moreover, if $\mathbb{F}_{p^n}$ has two distinct subfields of size p^d, then the polynomial $f_{p^d}(X)$ would have more than p^d roots in $\mathbb{F}_{p^n}$, which is impossible.

For the last statement, recall that the multiplicative group of nonzero elements of a finite field is cyclic. If $\alpha \in \mathbb{F}_{p^n}$ is a generator of this gorup, then α will generate $\mathbb{F}_{p^n}$ over any subfield. If $d \mid n$, then $\mathbb{F}_{p^n} = \mathbb{F}_{p^d}(\alpha)$, so this extension is simple. □

These results can be translated into rather precise information on the structure of the polynomial ring over a finite field. For example,

Corollary 9.3.28. *Let F be a finite field. Then for all integers $n \geq 1$ there exist irreducible polynomials of degree n in $F[X]$.*

Proof. We know $F = \mathbb{F}_q$ for some prime power q. By Proposition 9.3.27 there is an extension $\mathbb{F}_q \subseteq \mathbb{F}_{q^n}$, generated by an element α. Then $[F_{q^n} : \mathbb{F}_q] = n$, and it follows that the minimal polynomial of α over $F = \mathbb{F}_q$ is an irreducible polynomial of degree n in $F[X]$. □

In fact, our analysis of extensions of finite fields tells us about explicit factorizations, leading to an inductive algorithm for the computation of irreducible polynomials in $\mathbb{F}_q[X]$:

Corollary 9.3.29. *Let $F = \mathbb{F}_q$ be a finite field, and let n be a positive integer. Then the factorization of $X^{q^n} - X$ in $F[X]$ consists of all irreducible monic polynomials of degree d, as d ranges over the positive divisors of n. In particular, all these polynomials factor completely in $\mathbb{F}_{q^n}$, and each irreducible polynomial appears only once in the factorization.*

Proof. By Theorem 9.3.24, $\mathbb{F}_{q^n}$ is the splitting field of $X^{q^n} - X$ over $\mathbb{F}_p$, and hence over $\mathbb{F}_q = F$.

If $f(X)$ is a monic irreducible polynomial of degree d, then $F[X]/(f(X)) = F(\alpha)$ is an extension of degree d of F, that is, an isomorphic copy of $\mathbb{F}_{q^d}$. By Proposition 9.3.27, if $d \mid n$, then there is an embedding of $\mathbb{F}_{q^d}$ in $\mathbb{F}_{q^n}$. But then α must be a root of $X^{q^n} - X$, and hence $X^{q^n} - X$ is a multiple of $f(X)$, as this is the minimal polynomial of α. This proves that every irreducible polynomial of degree $d \mid n$ is a factor of $X^{q^n} - X$.

Conversely, if $f(X)$ is an irreducible factor of $X^{q^n} - X$, then $\mathbb{F}_{q^n}$ contains a root α of $f(X)$; we have the extensions $F = \mathbb{F}_q \subseteq \mathbb{F}_q(\alpha) \subseteq \mathbb{F}_{q^n}$, and $\mathbb{F}_q(\alpha) \cong \mathbb{F}_{q^d}$ for $d = \deg \alpha$. It follows that $d \mid n$, again by Proposition 9.3.27.

For the last statement, note that $(X^{p^n} - X)' = p^n X^{p^n - 1} - 1 = -1$, so $X^{p^n} - X$ is separable by Proposition 9.1.54. This implies each irreducible polynomial appears only once in $X^{p^n} - X$. □

The picture we are trying to convey is the following: the q^n roots of $X^{q^n} - X$ clump into disjoint subsets, with each subset collecting the roots of each and every irreducible polynomial of degree $d \mid n$ in $F[X]$.

Example 9.3.30. Let's contemplate the case $q = 2$: $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$.

- $n = 1$: the polynomial $X^2 - X$ factors as the product of X and $(X - 1)$ (which we could write as $(X + 1)$ just as well, since we are working over $\mathbb{F}_2$). These are all the irreducible polynomials of degree 1 over $\mathbb{F}_2$.
- $n = 2$: the polynomial $X^4 - X$ must factor as the product of all irreducible polynomials of degree 1 and 2; in fact

$$X^4 - X = X(X - 1)(X^2 + X + 1)$$

  and the conclusion is that there is exactly one irreducible polynomial of degree 2 over $\mathbb{F}_2$, namely $X^2 + X + 1$.

- $n = 3$: the quotient of $X^8 - X$ by $X(X-1)$ is a polynomial of degree 6, which must therefore be the product of the two irreducible polynomials of degree 3 over $\mathbb{F}_2$. It takes a moment to find them:
$$X^3 + X^2 + 1, \quad X^3 + X + 1$$
It also follows that $\mathbb{F}_8$ may be realized in two ways as a quotient of $\mathbb{F}_2[X]$ modulo an irreducible polynomial:
$$\frac{\mathbb{F}_2[X]}{(X^3 + X^2 + 1)} \cong \frac{\mathbb{F}_2[X]}{(X^3 + X + 1)}$$

Since extensions of finite fields are simple extensions, our previous work allows us to be much more precise. Restricting our attention to the extensions $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$, for a prime p, we know these can be realized as simple extensions by an element with minimal polynomial of degree n. This polynomial is necessarily separable ($\mathbb{F}_p$ is perfect), so Corollary 9.1.8 immediately gives us the size of the automorphism group: $|\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)| = n$.

Proposition 9.3.31. *The Galois group G of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$ is cyclic of order n, generated by the Frobenius automorphism.*

Proof. We have seen that the Frobenius isomorphism σ is an automorphism of $\mathbb{F}_{p^n}$. If $\alpha \in \mathbb{F}_p$, then $\sigma(\alpha) = \alpha^p = \alpha$ and so σ fixes $\mathbb{F}_p$ and is therefore in the Galois group G. Moreover, the n automorphisms
$$1, \sigma, \sigma^2, \ldots, \sigma^{n-1}$$
are distinct elements of G, for if $\sigma^k = 1$ then $\alpha^{p^k} = \alpha$ for all $\alpha \in \mathbb{F}_{p^n}$ and so $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^d}$, which implies that $k \geq n$. Finally, since $|G| = n$, we see that $G = \langle \sigma \rangle$. □

Corollary 9.3.32. *Let $d \mid n$ be positive integers, then the Galois group G of $\mathbb{F}_{p^n}$ over $\mathbb{F}_{p^d}$ is cyclic of order n/d, generated by the automorphism $\sigma^d : \alpha \mapsto \alpha^{p^d}$.*

Proof. Let σ^d be the automorphism prescribed above. Then σ^d fixes $\mathbb{F}_{p^d}$.and hence is in G, and it has order d/n. By Theorem 9.2.35 we have
$$\mathrm{Gal}(\mathbb{F}_{p^d}/\mathbb{F}_p) \cong \frac{\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)}{\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^d})},$$
and in particular $|\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^d})| = n/d$. Since σ^d also has order n/d, the claim follows. □

Corollary 9.3.33. *The absolute Galois group $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ is isomorphic to $\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$.*

Proof. Let $F = \mathbb{F}_q$ be a finite field. We show that the absolute Galois group is isomorphic to $\widehat{\mathbb{Z}}$. For this, let $\mathcal{N}$ be the category associated to the poset $\mathbb{N}$ of division partial order, and we still denote by n the objects of $\mathcal{N}$. By Proposition 9.3.27 we have an inverse system of groups
$$\left(\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)\right)_{n \in \mathcal{N}}$$
where for $m \mid n$ the map $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \to \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ is the restriction map; that is, the image of an automorphism $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ in $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ is obtained by simply restricting the domain of σ from $\mathbb{F}_{q^n}$ to $\mathbb{F}_{q^m}$. Since $\mathbb{F}_{q^m}$ are all the finite subextensions of $\overline{\mathbb{F}}_q$, by Corollary 9.2.32, we see the inverse limit of this inverse system is exactly $\mathrm{Gal}(\overline{F}_q/\mathbb{F}_q)$. But Corollary 9.3.32 suggests that

$\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}$ and the restriction map corresponds to the quotient map $\mathbb{Z}/n\mathbb{Z} \to Z/m\mathbb{Z}$. Thus the inverse system $\big(\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)\big)_{n\in\mathcal{N}}$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})_{n\in\mathcal{N}}$ and the claim follows from this. □

9.3.5.2 The algebraic closure of a finite field

To conclude, we determine the algebraic closure of a finite field $\mathbb{F}_p$. Since $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$ is algebraic for all positive integers n, an algebraic closure of $\mathbb{F}_p$ must contain all of the fields $\mathbb{F}_{p^n}$. Since $n! \mid (n+1)!$, it follows that $\mathbb{F}_{p^{n!}} \subseteq \mathbb{F}_{p^{(n+1)!}}$ and so the union

$$\Gamma(p) = \bigcup_{n=0}^{\infty} \mathbb{F}_{p^{n!}}$$

is an extension field of $\mathbb{F}_p$ that contains $\mathbb{F}_{p^n}$ for all $n \geq 1$. Moreover, if E is a field for which $\mathbb{F}_{p^n} \subseteq E$ for all n, then $\Gamma(p) \subseteq E$, that is, $\Gamma(p)$ is the smallest field containing each $\mathbb{F}_{p^n}$.

Theorem 9.3.34. *The field $\Gamma(p)$ is the algebraic closure of $\mathbb{F}_p$.*

Proof. Every element of $\Gamma(p)$ lies in some $\mathbb{F}_{p^{n!}}$, whence it is algebraic over $\mathbb{F}_p$. Thus $\Gamma(p)$ is algebraic over $\mathbb{F}_p$. Now let $f(X)$ be an irreducible polynomial over $\Gamma(p)$ of degree d. Then the coefficients of $f(X)$ lie in some $\mathbb{F}_{p^{n!}}$ and so $f(X)$ is irreducible as a polynomial over $\mathbb{F}_{p^{n!}}$. Hence, the splitting field for $f(X)$ is $\mathbb{F}_{p^{n!d}} \subseteq \Gamma(p)$ and so $\Gamma(p)$ splits over $\Gamma(p)$. □

9.3.6 Cyclotomic polynomials and fields

Let K be a field. By a **root of unity** (in K) we shall mean an element $\zeta \in K$ such that $\zeta^n = 1$ for some integer $n > 1$. If the characteristic of K is p, then the equation

$$X^{p^d} = 1$$

has only one root, namely 1, and hence there is no p^d-th root of unity except 1.

Let n be an integer > 1 and not divisible by the characteristic p. The polynomial

$$X^n - 1$$

is separable because its derivative is $nX^{n-1} \neq 0$, and the only root of the derivative is 0, so there is no common root. Hence in $\overline{K}$ the polynomial $X^n - 1$ has n distinct roots, which are roots of unity. They obviously form a group, and we know that every finite multiplicative group in a field is cyclic. Thus the group of n-th roots of unity is cyclic. A generator for this group is called a **primitive n-th root** of unity.

If μ_n denotes the group of all n-th roots of unity in $\overline{n}$ and m, n are relatively prime integers, then

$$\mu_{mn} \cong \mu_m \times \mu_n$$

This follows because μ_m, μ_n cann ot have any element in common except 1, and because $\mu_m\mu_n$ consequently has mn elements, each of which is an mn-th root of unity. Hence $\mu_m\mu_n = \mu_{mn}$ and the decomposition is that of a direct product.

As a matter of notation, to avoid double indices, especially in the prime power case, we write $\mu[n]$ for μ_n. So if p is a prime, $\mu[p^r]$ is the group of p^r-th roots of unity. Then $\mu[p^\infty]$ denotes the union of all $\mu[p^r]$ for all positive integers r.

Let K be any field. Let n be not divisible by the characteristic p. Let ζ_n be a primitive n-th root of unity in $\overline{K}$. Let σ be an embedding of $K(\zeta)$ in $\overline{K}$ over K. Then

$$(\sigma(\zeta))^n = \sigma(\zeta^n) = 1$$

so that $\sigma(\zeta)$ is an n-th root of unity also. Hence $\sigma(\zeta) = \zeta^i$ for some integer $i = i(\sigma)$, uniquely determined mod n. It follows that σ maps $K(\zeta)$ into itself, and hence that $K(\zeta)$ is normal over K. If τ is another automorphism of $K(\zeta)$ over K then

$$\sigma(\tau(\zeta)) = \zeta^{i(\sigma)i(\tau)}$$

Since σ and τ are automorphisms, it follows that $i(\sigma)$ and $i(\tau)$ are coprime to n. In this way we get a homomorphism of the Galois group G of $K(\zeta)$ over K into the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ of integers prime to n, mod n. Our homomorphism is clearly injective since $i(\sigma)$ is uniquely determined by σ mod n, and the effect of σ on $K(\zeta)$ is determined by its effect on ζ. We conclude that $K(\zeta)$ is abelian over K. We know that the order of $(\mathbb{Z}/n\mathbb{Z})^\times$ is $\phi(n)$. Hence the degree $[K(\zeta) : K]$ divides $\phi(n)$.

For a specific field K, the question arises whether the image of $\mathrm{Gal}(K(\zeta)/K)$ in $(\mathbb{Z}/n\mathbb{Z})^\times$ is all of $(\mathbb{Z}/n\mathbb{Z})^\times$. Looking at $K = \mathbb{R}$ or $\mathbb{C}$, one sees that this is not always the case. We now give an important example when it is the case.

Define the n-th **cyclotomic polynomial** $\Phi_n(X)$ to be

$$\Phi_n(X) = \prod_{\zeta \text{ primitive } n\text{-th root of } 1} (X - \zeta) = \prod_{\substack{1 \le m \le n \\ (m,n)=1}} (X - \zeta_n^m)$$

which has degree $\phi(n)$.

Example 9.3.35. If $n = p$ is prime, then every nonidentity element of $\mu_p \cong C_p$ is a generator: every p-th root of 1 is primitive except 1 itself. Therefore

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + \cdots + X + 1$$

Lemma 9.3.36. *For all positive integers n,*

$$X^n - 1 = \prod_{\substack{1 \le d \le n \\ d \mid n}} \Phi_d(X)$$

Proof. If $n = de$, then every d-th root ζ of 1 is an n-th root of 1, because $\zeta^n = \zeta^{de} = (\zeta^d)^e = 1$. In particular, every primitive d-th root ζ of 1 is an n-th root of 1.

On the other hand, every $\zeta \in \mu_n$ generates a subgroup H of μ_n, and $H = \mu_d$ for d equal to the order of ζ, a divisor of n. Thus, every $\zeta \in \mu_n$ is a primitive d-th root of 1 for some $d \mid n$.

Thus the set of n-th roots of 1 equals the union of the sets of primitive d-th roots of 1, as d

ranges over all positive divisors of n. The statement follows immediately:

$$X^n - 1 = \prod_{\zeta \in \mu_n} (X - \zeta) = \prod_{\substack{1 \le d \le n \\ d \mid n}} \left(\prod_{\zeta \text{ primitive } d\text{-th root of } 1} (X - \zeta) \right) = \prod_{\substack{1 \le d \le n \\ d \mid n}} \Phi_d(X)$$

as claimed. □

Lemma 9.3.36 yields an inductive computation of cyclotomic polynomials; the fact that $\Phi_n(X) \in \mathbb{Z}[X]$ follows from this fact. Explicitly,

Corollary 9.3.37. *The cyclotomic polynomials $\Phi_n(X)$ have integer coefficients.*

Proof. Use induction on n. Note that $\Phi_1(X) = x - 1$, and assume we have shown that all $\Phi_m(X)$ have integer coefficients for $m < n$. In particular, $f(X) := \prod_{1 \le d \mid n, d < n} \Phi_d(X)$ is a monic polynomial with integer coefficients. Since $f(X)$ is monic, we can divide it into $X^n - 1$ with remainder, within $\mathbb{Z}[X]$: there exist $q(X), r(X) \in \mathbb{Z}[X]$ such that

$$X^n - 1 = q(X)f(X) + r(X)$$

with $r(X) = 0$ or $\deg r(X) < \deg f(X)$. On the other hand, by Lemma 9.3.36,

$$X^n - 1 = f(X)\Phi_n(X)$$

in $\mathbb{C}[X]$. Therefore

$$f(X)(\Phi_n(X) - q(X)) = r(X)$$

in $\mathbb{C}[X]$. But this forces $r(X) = 0$ (otherwise we would have $\deg r(X) > \deg f(X)$). Therefore $\Phi_n(X) = q(X) \in \mathbb{Z}[X]$. □

Proposition 9.3.38. *For all positive n, $\Phi_n(X) \in \mathbb{Z}[X]$ is irreducible over $\mathbb{Q}$.*

Proof. Arguing by contradiction, assume $\Phi_n(X)$ is reducible. Then its roots ζ_n^m, with $(m, n) = 1$, are divided among the factors; we can choose a root ζ_n^m of one irreducible monic factor $f(X)$, such that another root ζ_n^{mp} (for some prime p not dividing n) is not a root of $f(X)$. Write

$$\Phi_n(X) = f(X)g(X)$$

since $\Phi_n(X) \in \mathbb{Z}[X]$ and $\Phi_n(X)$, $f(X)$ are monic, $f(X)$ and $g(X)$ have integer coefficients. By our choice, $f(X)$ is the minimal polynomial of ζ_n^m over $\mathbb{Q}$, and $g(\zeta_n^{mp}) = 0$.

It follows that ζ_n^m is a root of $g(X^p)$, and hence $f(X) \mid g(X^p)$. Therefore we can write

$$g(X^p) = f(X)h(X)$$

with $h(X) \in \mathbb{Z}[X]$. Reading the last equation modulo p, we get (again using $(a + b)^p = a^p + b^p$, and denoting cosets by bar)

$$\overline{g}(X)^p = \overline{f}(X)\overline{h}(X) \text{in } \mathbb{F}_p[X].$$

In particular, $\overline{f}(X)$ and $\overline{g}(X)$ must have a nontrivial common factor $\overline{\ell}(X)$ in $\mathbb{F}_p[X]$. But then

$$\ell^2(X) \mid \overline{f}(X)\overline{g}(X)$$

the reduction of $\Phi_n(X)$ modulo p must have a multiple factor.

This implies that $X^n - 1 \in \mathbb{F}_p[X]$ has a multiple factor; that is, it is inseparable. However, its derivative $nX^{n-1} \in \mathbb{F}_p[X]$ is nonzero (because p does not divide n by assumption), and Proposition 9.1.54 implies that $X^n - 1$ is separable in $\mathbb{F}_p[X]$.

This contradiction shows that our assumption that $\Phi_n(X)$ is reducible must be nonsense, proving the statement. □

Definition 9.3.39. *The splitting field $\mathbb{Q}(\zeta_n)$ for the polynomial $X^n - 1$ over $\mathbb{Q}$ is the n-th* ***cyclotomic field****.*

Proposition 9.3.40. *The Galois group* $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ *is isomorphic to* $(\mathbb{Z}/n\mathbb{Z})^\times$.

Proof. We know that $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ has cardinality $\phi(n)$ (Corollary 9.1.8; the roots are distinct since $\Phi_n(X)$ is separable), so the homomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$ is an isomorphism. □

Corollary 9.3.41. *If n, m are relative prime integers, then*

$$\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}.$$

Proof. We note that ζ_n and ζ_m are both contained in $\mathbb{Q}(\zeta_{mn})$ since ζ_{mn}^n is a primitive m-th root of unity. Furthermore, $\zeta_m\zeta_n$ is a primitive mn-th root of unity. Hence

$$\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{mn})$$

Our assertion then follows from the multiplicativity $\phi(mn) = \phi(m)\phi(n)$ and Proposition 9.2.38. □

Example 9.3.42. The reader should consider Example 9.1.39 again: by what we have just proved, the automorphism group of the splitting field of $X^8 - 1$ is isomorphic to the group of units in $\mathbb{Z}/8\mathbb{Z}$; this group is immediately seen to be isomorphic to $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, confirming the claim made in Example 9.1.39.

9.3.7 Cyclic extensions

9.3.7.1 Hilbert's theorem 90

Let G be a group. A ***G*-module** is an abelian group M together with an action of G, i.e., a map $G \times M \to M$ such that

- $\sigma(m + n) = \sigma m + \sigma n$ for $m, n \in M$.
- $(\sigma\tau)m = \sigma(\tau m)$ for $\sigma, \tau \in G$ and $m \in M$.
- $1m = m$ for $m \in M$.

Thus, to give an action of G on M is the same as giving a homomorphism $G \to \mathrm{Aut}(M)$ (automorphisms of M as an abelian group).

Example 9.3.43. Let E be a Galois extension of K with Galois group G. Then $(E, +)$ and $(E^\times, \times)$ are G-modules.

Let M be a G-module. A **crossed homomorphism** is a map $f : G \to M$ such that

$$f(\sigma\tau) = f(\sigma) + \sigma f(\tau)$$

for all $\sigma, \tau \in G$. Note that the condition implies that $f(1) = f(1) + f(1)$, and so $f(1) = 0$.

Example 9.3.44.

(a) Let $f : G \to M$ be a crossed homomorphism. For any $g \in G$,

$$\begin{aligned} f(\sigma^2) &= f(\sigma) + \sigma f(\sigma), \\ f(\sigma^3) &= f(\sigma) + \sigma f(\sigma^2) = f(\sigma) + \sigma f(\sigma) + \sigma^2 f(\sigma) \\ &\vdots \\ f(\sigma^n) &= f(\sigma) + \sigma f(\sigma) + \cdots + \sigma^{n-1} f(\sigma) \end{aligned}$$

Thus, if G is a cyclic group of order n generated by σ, then a crossed homomorphism $f : G \to M$ is determined by its value, x say, on σ, and x satisfies the equation

$$x + \sigma x + \cdots + \sigma^{n-1} x = 0 \tag{3.7.1}$$

Moreover, if $x \in M$ satisfies (3.7.1), then the formulas $f(\sigma^i) = x + \sigma x + \cdots + \sigma^{i-1} x$ define a crossed homomorphism $f : G \to M$. Thus, for a finite cyclic group $G = \langle \sigma \rangle$, there is a one-to-one correspondence

$$\{\text{crossed homomorphisms } f : G \to M\} \leftrightarrows \{x \in M \text{ satisfying (3.7.1)}\}.$$

(b) For every $x \in M$, we obtain a crossed homomorphism by putting

$$f(\sigma) = \sigma x - x$$

for all $\sigma \in G$. A crossed homomorphism of this form is called a **principal crossed homomorphism**.

(c) If G acts trivially on M, i.e., $\sigma m = m$ for all $\sigma \in G$ and $m \in M$, then a crossed homomorphism is simply a homomorphism, and there are no nonzero principal crossed homomorphisms.

The sum and difference of two crossed homomorphisms is again a crossed homomorphism, and the sum and difference of two principal crossed homomorphisms is again principal. Thus we can define

$$H^1(G, M) = \frac{\text{crossed homomorphisms}}{\text{principal crossed homomorphisms}}$$

(quotient abelian group). An exact sequence of G-modules

$$0 \longrightarrow M \longrightarrow N \longrightarrow L \longrightarrow 0$$

gives rise to an exact sequence

$$0 \longrightarrow M^G \longrightarrow N^G \longrightarrow L^G \xrightarrow{\delta} H^1(G, M) \longrightarrow H^1(G, N) \longrightarrow H^1(G, L)$$

Let $\ell \in L^G$, and let $n \in N$ map to ℓ. For all $\sigma \in G$, $\sigma n - n$ lies in the submodule M of N, and the crossed homomorphism $\sigma \mapsto \sigma n - n : G \to M$ represents $\delta(\ell)$.

Example 9.3.45. Let $\pi : \widetilde{X} \to X$ be the universal covering space of a topological space X, and let Γ be the group of covering transformations. Under some fairly general hypotheses, a Γ-module M will define a sheaf $\mathcal{M}$ on X, and $H^1(X, \mathcal{M}) \cong H^1(\Gamma, M)$. For example, when $M = \mathbb{Z}$ with the trivial action of Γ, this becomes the isomorphism $H^1(X, \mathbb{Z}) \cong H^1(\Gamma, \mathbb{Z}) = \mathrm{Hom}(\Gamma, \mathbb{Z})$.

Theorem 9.3.46. *Let E be a finite Galois extension of K with group G; then $H^1(G, E^\times) = 0$ and $H^1(G, E) = 0$.*

Proof. Let f be a crossed homomorphism $G \to E^\times$. In multiplicative notation, this means that

$$f(\sigma\tau) = f(\sigma) \cdot (\sigma f(\tau))$$

for $\sigma, \tau \in G$, and we have to find a $\gamma \in E^\times$ such that $f(\sigma) = \sigma(\gamma)/\gamma$ for all $\sigma \in G$. Because the $f(\tau)$ are nonzero, Corollary 9.1.36 implies that

$$\sum_{\tau \in G} f(\tau)\tau : E \to E$$

is not the zero map, i.e., there exists an $\alpha \in E$ such that

$$\beta := \sum_{\tau \in G} f(\tau)\tau(\alpha) \neq 0.$$

But then, for $\sigma \in G$,

$$\begin{aligned}\sigma(\beta) &= \sigma\Big(\sum_{\tau \in G} f(\tau)\tau(\alpha)\Big) = \sum_{\tau \in G} \sigma(f(\tau))\sigma(\tau(\alpha)) \\ &= f(\sigma)^{-1} \sum_{\tau \in G} f(\sigma\tau)(\sigma\tau)(\alpha) = f(\sigma)^{-1}\beta.\end{aligned}$$

Therefore $f(\sigma) = \beta/\sigma(\beta)$ and we can take $\gamma = \beta^{-1}$.

For the additive version, let $f : G \to E$ be a crossed homomorphism. Then we have

$$f(\sigma\tau) = f(\sigma) + \sigma f(\tau)$$

for $\sigma, \tau \in G$. Let $\gamma \in E$ an element in E such that $\mathrm{tr}(\gamma) \neq 0$ (this element exists by linearly independence), and consider

$$\beta := \sum_{\tau \in G} f(\tau)\tau(\gamma).$$

Then we have

$$\begin{aligned}\sigma(\beta) &= \sigma\Big(\sum_{\tau \in G} f(\tau)\tau(\gamma)\Big) = \sum_{\tau \in G} \sigma(f(\tau))\sigma(\tau(\gamma)) \\ &= \sum_{\tau \in G} f(\sigma\tau)(\sigma\tau)(\gamma) - f(\sigma) \sum_{\tau \in G} (\sigma\tau)(\gamma) = \beta - f(\sigma)\mathrm{tr}(\gamma).\end{aligned}$$

Since $\mathrm{tr}(\gamma) \neq 0$, we obtain $f(\sigma) = \beta/\mathrm{tr}(\gamma) - \sigma(\beta/\mathrm{tr}(\gamma))$, so f is principal. □

Corollary 9.3.47 (Hilbert's theorem 90, multiplicative version). *Let E be a finite cyclic extension of K and let σ generate* $\mathrm{Gal}(E/K)$. *Let $\alpha \in E$, if $N(\alpha) = 1$, then $\alpha = \beta/\sigma(\beta)$ for some $\beta \in E$.*

Proof. Let $n = [E : K]$. The condition on α is that $\alpha\sigma(\alpha)\cdots\sigma^{n-1}(\alpha) = 1$, and so by (3.7.1) there is a crossed homomorphism $f : G \to E^\times$ with $f(\sigma) = \alpha$. **??** now shows that f is principal, which means that there is a $\beta \in E$ such that $\alpha = \beta/\sigma(\beta)$. □

Corollary 9.3.48 (Hilbert's theorem 90, additive version). *Let E be a finite cyclic extension of K and let σ generate* $\mathrm{Gal}(E/K)$. *Let $\alpha \in E$, if* $\mathrm{tr}(\alpha) = 0$, *then $\alpha = \beta - \sigma(\beta)$ for some $\beta \in E$.*

Proof. Let $n = [E : K]$. The condition on α is that $\alpha + \sigma(\alpha) + \cdots + \sigma^{n-1}(\alpha) = 1$, and so by (3.7.1) there is a crossed homomorphism $f : G \to E$ with $f(\sigma) = \alpha$. **??** now shows that f is principal, which means that there is a $\beta \in E$ such that $\alpha = \beta/\sigma(\beta)$. □

9.3.7.2 Abelian and Cyclic Extensions

Extensions are often named after their Galois groups. Here is a very important example.

Definition 9.3.49. *A Galois extension E/K is **abelian** if its Galois group* $\mathrm{Gal}(E/K)$ *is abelian and **cyclic** if the Galois group is cyclic.*

The basic properties of abelian and cyclic extensions are given in the next proposition. Note that abelian and cyclic extensions are not (quite) distinguished.

Proposition 9.3.50 (Property of abelian and cyclic extensions).

- ***(Composite of abelian is abelian)*** *If $K \subseteq E_i$ are abelian, then $K \subseteq \bigvee E_i$ is abelian.*
- ***(Lifting of abelian (cyclic) is abelian (cyclic))*** *If $K \subseteq E$ is abelian (cyclic) and $K \subseteq F$, then $F \subseteq EF$ is abelian (cyclic).*
- ***(Steps in an abelian (cyclic) tower are abelian (cyclic))*** *If $K \subseteq E \subseteq F$ with $K \subseteq E \subseteq F$ abelian (cyclic), then $K \subseteq E$ and $E \subseteq F$ are abelian (cyclic).*

Proof. Let $K \subseteq E_i$ be abelian extensions, then since E_i/K are Galois, the extension $K \subseteq \bigvee E_i$ is also Galois. Moreover, by Proposition 9.2.43, the Galois group $\mathrm{Gal}(\bigvee E_i/K)$ is a subgroup of $\prod \mathrm{Gal}(E_i/K)$, which is abelian, and hence is also abelian.

Now consider a lifting of abelian (cyclic) extension. By Proposition 9.2.38 the extension $F \subseteq EF$ is Galois, and $\mathrm{Gal}(EF/F) \cong \mathrm{Gal}(E/E \cap F)$. Note that $\mathrm{Gal}(E/E \cap F)$ is a subgroup of $\mathrm{Gal}(E/K)$, and hence is abelian (cyclic) if $\mathrm{Gal}(E/K)$ is abelian (cyclic).

Finally, consider a tower $K \subseteq E \subseteq F$, where F/K is abelian (cyclic). Since all subgroups of $\mathrm{Gal}(F/K)$ is then normal, we see E/K and F/E are both Galois extensions, and $\mathrm{Gal}(E/K)$, $\mathrm{Gal}(F/E)$ are isomorphic to subgroups of $\mathrm{Gal}(F/K)$, which are abelian (cyclic). □

Abelian and cyclic extensions fail to be distinguished because, and only because if the steps in a tower are abelian (cyclic), this does not imply that the full extension is abelian (cyclic). What does it imply?

Suppose that

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n = E$$

is a tower in which each step K_{i+1}/K_i is abelian (cyclic). Taking Galois groups gives the series

$$\{1\} = \mathrm{Gal}(E/E) \subseteq \mathrm{Gal}(E/K_{n-1}) \subseteq \cdots \subseteq \mathrm{Gal}(E/K_1) \subseteq \mathrm{Gal}(E/K_0) = \mathrm{Gal}(E/K).$$

Consider the subtower $K_i \subseteq K_{i+1} \subseteq E$. Since the lower step is normal, it follows from Theorem 9.2.35(a) that $\mathrm{Gal}(E/K_{i+1})$ is a normal subgroup of its parent $\mathrm{Gal}(E/K_i)$ and that

$$\frac{\mathrm{Gal}(E/K_i)}{\mathrm{Gal}(E/K_{i+1})} \hookrightarrow \mathrm{Gal}(K_{i+1}/K_i).$$

Since the latter is abelian (cyclic), so is the former. Thus,

$$\{1\} = \mathrm{Gal}(E/E) \lhd \mathrm{Gal}(E/K_{n-1}) \lhd \cdots \lhd \mathrm{Gal}(E/K_1) \lhd \mathrm{Gal}(E/K).$$

where each quotient group is abelian (cyclic). In the language of group theory, this series of subgroups is an **abelian series**. (When the groups are finite, the cyclic case and the abelian case are equivalent.) A group that has an abelian series is said to be **solvable**.

Proposition 9.3.51. *If $K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = E$ is a tower of fields in which each step $K_i \subseteq K_{i+1}$ is abelian, then the Galois group* $\mathrm{Gal}(E/K)$ *is solvable.*

In the follows, we classify cyclic extensions under certain conditions, which will be used when we study the solvability of polynomials. The follwoing two theorems are good applications of Hilbert's theorem 90.

Theorem 9.3.52. *Let K be a field, n an positive integer coprime to the characteristic of K, and assume that there is a primitive n-th root of unity in K.*

(i) Let E be a cyclic extension of degree n of K. Then there exists $\alpha \in E$ such that $E = K(\alpha)$, and α satisfies an equation $X^n - a = 0$ for some $a \in K$.

(ii) Conversely, let $a \in K$. Let α be a root of $X^n - a$. Then $K(\alpha)$ is cyclic over K, of degree d for some $d \mid n$, and α^d is an element of K.

Proof. Let ζ be a primitive n-th root of unity in K, and let E/K be cyclic with group G. Let σ be a generator of G. We have $N(\zeta^{-1}) = (\zeta^{-1})^n = 1$. By Hilbert's theorem 90, there exists $\alpha \in E$ such that $\zeta^{-1} = \alpha/\sigma(\alpha)$. Since ζ is in K, we have $\sigma^i(\alpha) = \zeta^i\alpha$ for $i = 1, \ldots, n$. Hence the elements $\zeta^i(\alpha)$ are n distinct conjugates of α over K, whence $[K(\alpha) : K]$ is at least equal to n. Since $[E : K] = n$, it follows that $E = K(\alpha)$. Furthermore,

$$\sigma(\alpha^n) = \sigma(\alpha)^n = \zeta^n\alpha^n = \alpha^n.$$

Hence α^n is fixed under σ, and so under G. Therefore α^n is an element of K, and we let $a = \alpha^n$. This proves the first part of the theorem.

Conversely, let $a \in K$. Let α be a root of $X^n - a$. Then $\alpha\zeta^i$ is also a root for each $i = 1, \ldots, n$, and hence all roots lie in $K(\alpha)$ which is therefore normal over K. All the roots are distinct so $K(\alpha)$ is Galois over K. Let G be the Galois group. If σ is an automorphism of $\mathrm{Gal}(K(\alpha)/K)$ then $\sigma(\alpha)$ is also a root of $X^n - a$. Hence $\sigma(\alpha) = \omega_\sigma\alpha$ where ω_σ is an n-th root of unity, not necessarily primitive. The map $\sigma \mapsto \omega_\sigma$ is obviously a homomorphism of G into the group of n-th roots of unity, and is injective. Since a subgroup of a cyclic group is cyclic, we conclude that G is cyclic,

of order d, and $d \mid n$. The image of G is a cyclic group of order d. If σ is a generator of G, then ω_σ is a primitive d-th root of unity. Now we get

$$\sigma(\alpha^d) = \sigma(\alpha)^d = \omega_\sigma^d \alpha^d = \alpha^d.$$

Hence α^d is fixed under G, whence is in K, and our theorem is proved. □

We now pass to cyclic extensions of degree p in characteristic p.

Theorem 9.3.53 (Artin-Schreier). *Let K be a field of characteristic p.*

(i) Let E be a cyclic extension of K of degree p. Then there exists $\alpha \in E$ such that $E = K(\alpha)$ and α satisfies an equation $X^p - X - a = 0$ with some $a \in K$.

(ii) Conversely, given $a \in K$, the polynomial $f(X) = X^p - X - a$ either has one root in K, in which case all its roots are in K, or it is irreducible. In this latter case, if α is a root then $K(\alpha)$ is cyclic of degree p over K.

Proof. Let E be a cyclic extension of K of degree p, and σ be a generator of $\mathrm{Gal}(E/K)$. Since $-1 \in K$, every automorphism in $\mathrm{Gal}(E/K)$ fixes -1, it follows that $\mathrm{tr}(-1) = 0$. By the additive version of Hilbert's theorem 90, there is a element $\beta \in E$ such that $-1 = \beta - \sigma(\beta)$. Then

$$\sigma(\beta) = \beta + 1, \quad \sigma^i(\beta) = \sigma^{i-1}(\beta) + 1 = \cdots = \beta + i$$

It follows that the minimal polynomial of α has degree $\geq p$, so $[K(\alpha) : K] \geq p$. But $[E : K] = p$. So $E = K(\alpha)$. Note that

$$\sigma(\alpha^p - \alpha) = \sigma^p(\alpha) - \sigma(\alpha) = (\alpha + 1)^p - \alpha - 1 = \alpha^p - \alpha.$$

Hence $\alpha^p - \alpha$ is fixed under σ, and therefore under $\mathrm{Gal}(E/K)$. It lies in the fixed field K. If we let $a := \alpha^p - \alpha$, we see α satisfies the equation $X^p - X - a = 0$. This proves the first part of the theorem.

Conversely, let $a \in K$. If α is a root of $f(X) = X^p - X - a$, then

$$f(\alpha + 1) = (\alpha + 1)^p - \alpha - 1 - a = \alpha^p - \alpha - a = 0$$

so $\alpha + 1$ is also a root. Therefore the roots of $f(X)$ are

$$\alpha_1 := \alpha, \quad \alpha_2 := \alpha + 1, \quad \cdots, \quad \alpha_p := \alpha + p - 1$$

If $\alpha \in K$, then all α_i is in K. If $\alpha \notin K$, then all α_i is not in K. In this case, any sum $\sum_I$ with $I \neq \{1, \ldots, p\}$ and $I \neq \varnothing$ is not an element of K. Therefore $f(X)$ is irreducible by Exercise 9.1.3. Since all roots of $f(X)$ is in $K(\alpha)$, it follows that $K(\alpha)$ is normal over K. Since $f(X)$ has no multiple roots, it follows that $K(\alpha)$ is Galois over K. Since $\alpha + 1$ is a root of $f(X)$, there exists an automorphism σ of $K(\alpha)$ over K such that $\sigma(\alpha) = \alpha + 1$. Then the powers σ^i give $\sigma^i(\alpha) = \alpha + i$ for $i = 1, \ldots, p$ and are distinct. Since $[K(\alpha) : K] = p$, it follows that $\mathrm{Gal}(K(\alpha)/K) = \langle \sigma \rangle$ and is cyclic of order p, there by proving the theorem. □

9.3.8 Solvable and radical extensions

9.3.8.1 Solvable extensions

A finite separable extension E/K is said to be **solvable** if the Galois group of the normal closure of E/K is a solvable group. This is equivalent to saying that there exists a solvable Galois extension F of K such that $K \subseteq E \subseteq F$: Indeed, we have $K \subseteq E \subseteq \langle E/K \rangle \subseteq F$ and the Galois group of $\langle E/K \rangle / K$ is a homomorphic image of $\mathrm{Gal}(F/K)$, which is thus solvable.

Proposition 9.3.54. *Solvable extensions form a distinguished class of extensions.*

Proof. We first deal with liftings. Let E/K be solvable and F be a field containing K and assume E, F are subfields of some algebraically closed field. Let L be Galois solvable over K and $E \subseteq L$. Then LF is Galois over F and $\mathrm{Gal}(LF/F)$ is a subgroup of $\mathrm{Gal}(L/K)$ by Proposition 9.2.38. Hence LF/F is solvable, and it follows that EF/F is slovable.

Now let $K \subseteq E \subseteq F$ be a tower of extensions. If F/K is slovable, then there exists a field L containing F such that L/K is Galois and solvable. The by definition E/K is solvable. For F/E, it is clear that L/E is Galois, and since $\mathrm{Gal}(L/E)$ is a subgroup of $\mathrm{Gal}(L/K)$, it is also solvable. It follows that F/E is solvable.

Figure 3.8.1: A tower of solvable extensions is solvable.

For the converse, assume that F/E and E/K are solvable. Let L be a finite solvable Galois extension of K containing E. Then as a lifting, we see FL/L is solvable. Let M be a finite solvable Galois extension of K containing FL. If σ is any embedding of M over K in a given algebraic closure, then since L/K is Galois, we have $\sigma(L) = L$ and hence $\sigma(M)$ is also solvable extension of L. We let N be the compositum of all extensions $\sigma(M)$ for all embeddings σ of M over K. Then N is Galois over K and is therefore Galois over L. The Galois group $\mathrm{Gal}(N/L)$ is a subgroup of the product $\prod \mathrm{Gal}(\sigma(M)/L)$ by Proposition 9.2.43, hence is solvable. Since L is Galois over K, we have a isomorphism

$$\mathrm{Gal}(L/K) \cong \frac{\mathrm{Gal}(N/K)}{\mathrm{Gal}(N/L)}$$

by Theorem 9.2.35, which shows $\mathrm{Gal}(N/K)$ is slovable. Since $F \subseteq N$, this proves N is solvable, which completes the proof. □

9.3.8.2 Radical extensions

Loosely speaking, when $\mathrm{char}(K) \neq 0$, an extension $K \subseteq E$ is solvable by radicals if it is possible to reach E from K by adjoining a finite sequence of n-th roots of existing elements.

More specifically, we have the following definitions, which also deal with the case $\mathrm{char}(K) \neq 0$.

Let $K \subseteq R$ be a finite extension. A **radical series** for $K \subseteq R$ is a tower of fields

$$K = R_0 \subseteq R_1 \subseteq R_2 \subseteq \cdots \subseteq R_n = R$$

such that each step R_{i+1}/R_i is one of the following types:

(1) It is obtained by adjoining a root of unity.

(2) It is obtained by adjoining a root of a polynomial $X^n - a$ with $a \in E_i$ and n coprime to the characteristic.

(3) It is obtained by adjoining a root of an equation $X^p - X - a$ with $a \in E_i$, if p is the characteristic of K.

A finite separable extension $K \subseteq R$ that has a radical series is called a **radical extension**. For convenience, we write $K \subseteq R/\{R_i\}$ or $K \subseteq R/\{R_1, \ldots, R_n\}$ to denote the fact that $\{R_i\} = (R_0 \subseteq \cdots \subseteq R_n)$ is a radical series for the extension.

Proposition 9.3.55 (Properties of radical extensions).

*(a) (**Lifting**) If $K \subseteq R$ is a radical extension and $K \subseteq S$, then the lifting $S \subseteq RS$ is a radical extension.*

*(b) (**Each step implies full extension**) If $K \subseteq R \subseteq S$, where $K \subseteq R$ and $R \subseteq S$ are radical extensions, then so is the full extension $K \subseteq S$.*

*(c) (**Composite**) If $K \subseteq R$ and $K \subseteq S$ are radical extensions, then so is the composite extension $K \subseteq RS$.*

*(d) (**Normal closure**) If $K \subseteq R$ is a radical extension, then so is $K \subseteq \langle R/K \rangle$.*

Proof. Note that lifting a radical series gives another radical series with the same class of steps, for if $R_{i+1} = R_i(\alpha)$, where α is a root of $f(X) \in R_i[X]$, then

$$SR_{i+1} = (SR_i)(\alpha)$$

where α is a root of $f(X) \in (SR_i)[X]$.

For (a), let $K \subseteq R/\{R_i\}$. Lifting the series $\{R_i\}$ by $K \subseteq S$ gives the radical series

$$S = R_0S \subseteq R_1S \subseteq \cdots R_nS = RS$$

and so $S \subseteq RS$ is a radical extension.

For (b), if $K \subseteq R/\{R_i\}$ and $R \subseteq S/\{S_j\}$, then lift the series $\{S_j\}$ by R:

$$R \subseteq RS/(R = RS_0 \subseteq \cdots \subseteq RS_n)$$

and append it to the end of $K \subseteq R/\{R_i\}$ to get

$$K \subseteq RS/(R_0 \subseteq \cdots \subseteq R_n = R = RS_0 \subseteq \cdots \subseteq RS_n)$$

and so $K \subseteq RS = S$ is a radical extension.

For (c), if $K \subseteq R$ and $K \subseteq S$ are radical extensions, then so is the lifting $R \subseteq RS$ and so is the full extension $K \subseteq RS$.

For (d), the normal closure is

$$\langle R/K \rangle = \bigvee_{\sigma \in \mathrm{Hom}_K(R,\overline{R})} \sigma(R).$$

Since $K \subseteq R$ is a finite separable extension, $\mathrm{Hom}_K(R, \overline{R})$ is a finite set. Hence, the composite above is a finite one. If $K \subseteq R/\{R_i\}$ is a radical series, then so is $K \subseteq \sigma(R)/\{\sigma(R_i)\}$. Hence, $K \subseteq \sigma(R)$ is a radical extension, and therefore so is the finite composite $K \subseteq \langle R/K \rangle$. □

9.3.8.3 Solvability by radicals

We are interested in extensions $K \subseteq E$ where E is contained in a radical extension $K \subseteq R$.

Definition 9.3.56. *A finite separable extension $K \subseteq E$ is **solvable by radicals** if $K \subseteq E \subseteq R$, where $K \subseteq R$ is a radical extension.*

Proposition 9.3.57.

(a) The class of extensions that are solvable by radicals is distinguished.

(b) If $K \subseteq E$ is solvable by radicals then so is $K \subseteq \langle E/K \rangle$. In fact, if $K \subseteq E \subseteq R$ where $K \subseteq R$ is a radical extension, then

$$K \subseteq E \subseteq \langle E/K \rangle \subseteq \langle R/K \rangle$$

where $K \subseteq \langle R/K \rangle$ is a normal radical extension.

Proof. Let $K \subseteq E \subseteq F$ be a tower. If $K \subseteq F$ is solvable by radicals then there is a field R containing F such that R/K is a radical extension. It follows that E/K solvable by radicals. For the upper step, R/K radical implies R/E is radical by Proposition 9.3.55 and so F/E is solvable by radicals. Now suppose the steps in the tower are radical. Then we have the following extensions:

$$\begin{tikzcd}
 & R_{E/K}R_{F/E} \arrow[dl, dash] \arrow[dd, dash] \\
R_{F/E} \arrow[d, dash] & \\
F \arrow[d, dash] & R_{E/K} \\
E \arrow[ur, dash] \arrow[d, dash] & \\
K &
\end{tikzcd}$$

where $K \subseteq R_{E/K}$ and $E \subseteq R_{F/E}$ are radical extensions. Lifting the extension $E \subseteq R_{F/E}$ by $K \subseteq R_{E/K}$ gives the radical extension $R_{E/K} \subseteq R_{E/K}R_{F/E}$, so the tower

$$K \subseteq R_{E/K} \subseteq R_{E/K}R_{F/E}$$

is radical. It follows that the full extension is radical and so $K \subseteq E$ is solvable by radicals.

As to lifting, if $K \subseteq E \subseteq R$ with R/K radical, the lifting by $K \subseteq F$ gives

$$F \subseteq EF \subseteq RF$$

and since $F \subseteq RF$ is radical, EF/F is solvable by radicals.

The second part of the theorem follows from the fact that if $K \subseteq E \subseteq R$ with R/K is radical, then

$$K \subseteq \langle E/K \rangle \subseteq \langle R/K \rangle$$

with $K \subseteq \langle R/K \rangle$ radical by Proposition 9.3.55. □

Now we come to the key result that links the concepts of solvable extension and solvability by radicals.

Theorem 9.3.58. *Let E be a finite separable extension of K. Then E is solvable by radicals if and only if E/K is solvable.*

Proof. Assume that E/K is solvable, and let F be a finite solvable Galois extension of K containing E. Let m be the product of all prime divisors the degree $[F : K]$ that are unequal to the characteristic, and let $L = K(\zeta)$ where ζ is a primitive m-th root of unity. Then L/K is abelian. We lift F over L, so that FL is solvable over L. Since every solvable group admits a cyclic composition series whose factor groups are of prime order, we can use the Galois correspondence to find a tower of subfields between L and FL such that each step is cyclic of prime order. By Theorem 9.3.52 and 9.3.53, we conclude that FL is solvable by radicals over L, and hence is solvable by radicals over K. This proves that E/L is solvable by radicals.

$$\begin{tikzcd}
 & FL \\
F \arrow[ur, dash] \arrow[d, dash] & \\
E \arrow[d, dash] & L \arrow[uu, dash] \\
K \arrow[ur, dash] &
\end{tikzcd}$$

Conversely, assume that E/K is solvable by radicals. For any embedding σ of E in $\overline{E}$ over K, the extension $\sigma(E)/K$ is also solvable by radicals. Hence the normal closure F of E/K is solvable by radicals. Let m be the product of all prime divisors the degree $[F : K]$ that are unequal to the characteristic and again let $L = K(\zeta)$ where ζ is a primitive m-th root of unity. It will suffice to prove that FL is solvable over L, because it follows then that FL is solvable over K and hence F/K is slovable by Proposition 9.3.54. But FL/L can be decomposed into a tower of extensions, such that each step is prime degree and of the type described in Theorem 9.3.52 or Theorem 9.3.53, and the corresponding root of unity is in the field L. Hence FL/L is solvable, and our theorem is proved. □

9.3.9 Solvability of polynomial equations by radicals

We begin this part with a brief history of the study of roots of polynomials. Mathematicians of the Middle Ages, and probably those in Babylonia, knew the **quadratic formula** giving the roots of a quadratic polynomial $f(X) = X^2 + bX + c$. Setting $X = x - b/2$ transforms $f(X)$ into a polynomial $g(X)$ with no x term:

$$g(X) = X^2 + c - b^2/4.$$

Note that a number α is a root of $g(X)$ if and only if $\alpha - b/2$ is a root of $f(X)$. The roots of $g(X)$ are $\pm(\sqrt{b^2-4c})/2$, and so the roots of $f(X)$ are $(-b \pm \sqrt{b^2-4c})/2$.

Here is a derivation of the cubic formula. A cubic $f(X) = X^3 + aX^2 + bX + e$ can be transformed, by setting $X = X - a/3$, into a polynomial $g(X)$ with no X^2 term:

$$g(X) = X^3 + qX + r.$$

and a number α is a root of $g(X)$ if and only if $\alpha - a/3$ is a root of $f(X)$. If α is a root of $g(X)$, write $\alpha = \beta + \gamma$, where β and γ are to be found. Now

$$\begin{aligned}\alpha^3 &= (\beta+\gamma)^3 = \beta^3 + \gamma^3 + 3(\beta^2\gamma + \beta\gamma^2)\\ &= \beta^3 + \gamma^3 + 3\alpha\beta\gamma,\end{aligned}$$

and so evaluating $g(\alpha)$ gives

$$\beta^3 + \gamma^3 + (3\beta\gamma + q)\alpha + r = 0. \tag{3.9.1}$$

Impose the condition that $\beta\gamma = -q/3$ (forcing the middle term of (3.9.1) to vanish), we get

$$\beta^3 + \gamma^3 = -r.$$

This, together with our assumption on $\beta\gamma$, allow us to solve β and γ explicitly. In fact, a substitution gives

$$\beta^3 - \frac{q^3}{27\beta^3} = -r,$$

and so the quadratic formula yields

$$\beta^3 = \frac{-r \pm \sqrt{r^2 + 4q^3/27}}{2}, \quad \gamma^3 = \frac{-r \mp \sqrt{r^2 + 4q^3/27}}{2}.$$

If $\omega = e^{2\pi i/3}$ is a primitive cube root of unity, there are now six cube roots available: β, $\omega\beta$, $\omega^2\beta$, γ, $\omega\gamma$, $\omega^2\gamma$; these may be paired to give product $-q/3$:

$$-q/3 = \beta\gamma = (\omega\beta)(\omega^2\gamma) = (\omega^2\beta)(\omega\gamma).$$

It follows that the roots of $g(X)$ are $\beta + \gamma$, $\omega\beta + \omega^2\gamma$, and $\omega^2\beta + \omega\gamma$; this is the cubic formula.

Next we derive the quartic formula. A quartic $f(X) = X^4 + aX^3 + bX^2 + eX + d$ can be transformed, by setting $X = x - a/4$, into a polynomial $g(X)$ with no X^3 term:

$$g(X) = X^4 + qX^2 + rX + s,$$

moreover, a number α is a root of $g(X)$ if and only if $\alpha - a/4$ is a root of $f(X)$. Factor $g(X)$ into quadratics:

$$X^4 + qX^2 + rX + s = (X^2 + kX + l)(X^2 - kX + m)$$

(the coefficient of X in the second factor must be $-k$ because there is no cubic term in $g(X)$). If K, l, and m can be found, then the roots of $g(X)$ can be found by the quadratic formula.

Expanding the right side and equating coefficients of like terms gives

$$\begin{aligned} l + m - k^2 &= q, \\ km - kl &= r, \\ lm &= s. \end{aligned}$$

Rewrite the first two equations as

$$\begin{aligned} m + l &= q + k^2, \\ m - l &= r/k. \end{aligned}$$

Adding and subtracting these equations gives

$$m = \frac{q + k^2 + r/k}{2}, \quad l = \frac{q + k^2 - r/k}{2}.$$

These two equations show that we are done if K can be found. But $lm = s$ gives

$$(k^2 + q + r/k)(k^2 + q - r/k) = 4s$$

a cubic in k^2. The cubic formula allows one to solve for k^2, and it is now easy to determine l, m, and the roots of $g(X)$.

The most ambitious goal, in line with what occurs for degrees 2, 3, and 4, would be to produce a formula for the solutions to the general polynomial equation

$$X^n + a_{n-1}X^{n-2} + \cdots + a_0 = 0$$

in terms of the coefficients ai and basic operations such as taking roots. This would be a solution *by radicals* of the equation. Well, such a formula simply does not exist:

Theorem 9.3.59. *The general polynomial equation of degree* 5 *or higher admits no solution by radicals.*

Proof. Recall that the extension $K(s_1, \ldots, s_n) \subseteq K(t_1, \ldots, t_n)$ has Galois group $\mathfrak{S}_n$, which is not solvable for $n \geq 5$. Therefore by Theorem 9.3.58 this extension is not solvable by radicals. This means there is no formula for the solution of the general polynomial $g(X)$. □

Corollary 9.3.60. *Let K be a field of characteristic* 0*, and let $f(X) \in K[X]$ be an irreducible polynomial. Then $f(X)$ is solvable by radicals if and only if its Galois group is solvable.*

Corollary 9.3.60 is called **Galois' criterion**. Ruffini (1799) and Abel (1824) had previously established that general formulas in radicals for the solutions of equations of degree ≥ 5 do not exist (that is, Theorem 9.3.59); but it was Galois who identified the precise condition given in Corollary 9.3.60.

In fact, we could now do more: we know that $\mathfrak{S}_3$ and $\mathfrak{S}_4$ are solvable; from a composition series with cyclic quotients we could in principle decompose explicitly the splitting field of general polynomials of degree 3 and 4 as radical extensions and as a consequence recover the Tartaglia/Cardano/Ferrari formulas for their solutions.

9.3.10 Exercise

Exercise 9.3.1. A subgroup G of $\mathfrak{S}_n$ is **transitive** if the induced action of G on $\{1, \ldots, n\}$ is transitive.

- Prove that if $G \subseteq \mathfrak{S}_n$ is transitive, then $|G|$ is a multiple of n.
- List the transitive subgroups of $\mathfrak{S}_3$.
- Prove that the following subgroups of $\mathfrak{S}_4$ are all transitive:
  (1) $\langle (1234) \rangle \cong \mathbb{Z}/4\mathbb{Z}$ and its conjugates.
  (2) $\langle (12)(34), (13)(24) \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
  (3) $\langle (12)(34), (1234) \rangle \cong D_4$ and its conjugates.
  (4) $\mathfrak{A}_4$ and $\mathfrak{S}_4$.
- With a bit of stamina, prove that these are the only transitive subgroups of $\mathfrak{S}_4$.

Proof. Since G acts transitively on $\{1, \ldots, n\}$, we have (by the class formula, where G_1 is the isotopy of 1)

$$|G| = n|G_1|.$$

This shows $|G|$ is a multiple of n.

We have

$$\mathfrak{S}_3 = \{e, (12), (13), (23), (123), (132)\}$$

Assume G is a transitive subgroup of $\mathfrak{S}_3$, it must have order 3 or 6. Assume $|G| = 3$, then G must have a element of order 3, hence it contains a 3-cycle. Then

$$\mathfrak{A}_3 = \{e, (123), (132)\} \cong \mathbb{Z}/3\mathbb{Z}.$$

If $|G| = 6$, then $G = \mathfrak{S}_3$. So the transitive subgroups of $\mathfrak{S}_3$ are $\mathfrak{A}_3, \mathfrak{S}_3$.

It is easy to verify that the subgroups of $\mathfrak{S}_4$ listed above are transitive. If G is a transitive subgroup of $\mathfrak{S}_n$, then $\sigma G \sigma^{-1}$ acts transitively on $\{\sigma(1), \ldots, \sigma(n)\} = \{1, \ldots, n\}$ for some $\sigma \in \mathfrak{S}_n$. It follows that $\sigma G \sigma^{-1}$ is also a transitive subgroup of $\mathfrak{S}_n$. So the subgroups listed are all transitive subgroup of $\mathfrak{S}_4$, so are their conjugates.

Now Assume G is a transitive subgroup of $\mathfrak{S}_4$. Since G is transitive, by the first point we know 4 divides $|G|$. Therefore, the only possible candidates for $|G|$ are $4, 8, 12, 24$. It's clear that $|G| = 24$ iff $G = \mathfrak{S}_4$, and $|G| = 12$ iff $G = \mathfrak{A}_4$.

If $|G| = 4$, then $G \cong \mathbb{Z}/4\mathbb{Z}$ or $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. If $|G| = 8$, then G is a 2-sylow subgroup in $\mathfrak{S}_4$, and so is conjugate to any other 8 subgroups. Since D_4 is transitive, all 8 subgroups are transitive. □

Exercise 9.3.2. Compute the Galois group of the polynomial $X^4 - 2$.

Proof. The splitting field of $X^4 - 2$ is $\mathbb{Q}(i, \sqrt[2]{2})$. So it Galois group G has order 8. Since G is a subgroup of $\mathfrak{S}_4$, we see it is a 2-Sylow subgroup. All such groups are isomorphic to D_4. □

Exercise 9.3.3. Prove that the polynomial $X^5 - 5X - 1$ has exactly 3 real roots (this is a calculus exercise) and is irreducible over $\mathbb{Q}$. Prove that its Galois group is $\mathfrak{S}_5$.

Proof. $f(X) = X^5 - 5X - 1$, then $f(-2) = -23, f(-1) = 3, f(0) = -1, f(2) = 21$. So $f(X)$ has 3 real roots. And by Example 9.3.14, $f(X)$ has Galois group $\mathfrak{S}_5$. □

Exercise 9.3.4. Let $f(X) \in K[X]$ be a separable irreducible polynomial of prime degree p over a field K, and let $\alpha_1, \ldots, \alpha_p$ be the roots of $f(X)$ in its splitting field K. Prove that the Galois group of $f(X)$ contains an element σ of order p, cycling through the roots.

Proof. The splitting field of $f(X)$ contains a simple extension $K \subseteq K(\alpha_1)$ which has degree p. So the order of its Galois group divides p. Since p is a prime, Cauchy's theorem gives an element of order p. □

Exercise 9.3.5. Let $f(X) \in K[X]$ be a separable irreducible polynomial of prime degree p over a field K. Let α be a root of $f(X)$ in $\overline{K}$, and suppose you can express another root of $f(X)$ as a polynomial in α, with coefficients in K. Prove that you can express all roots as polynomials in α and that the Galois group of $f(X)$ is $\mathbb{Z}/p\mathbb{Z}$.

Proof. Assume σ is an element of order p. Without loss of generality, we may assume that $\sigma(\alpha)$ is a plolynomial of α:

$$\alpha = f(\alpha)$$

then

$$\sigma(\sigma(\alpha)) = \sigma(f(\alpha)) = f(\sigma(\alpha))$$

which means $\sigma^2(\alpha)$ is a polynomial of $\sigma(\alpha)$, hence is contained in $K(\alpha)$. Keep this process, we can show that all roots of $f(X)$ is in $K(\alpha)$. This means $K(\alpha)$ is the splitting field of $f(X)$, and $|\mathrm{Gal}_K(f(X))| = p$. In particular, σ is a generator, so $\mathrm{Gal}_K(f(X)) \cong \mathbb{Z}/p\mathbb{Z}$. □

Exercise 9.3.6. Let $f(X) \in K[X]$ be a separable irreducible polynomial of degree n over a field K, and let F be its splitting field. Assume $\mathrm{Aut}_K(F) \cong \mathfrak{S}_n$, and let α be a root of $f(X)$ in K.

- Prove that $\mathrm{Aut}_{K(\alpha)}(F) \cong \mathfrak{S}_{n-1}$.
- Prove that there are no proper subfields of $K(\alpha)$ properly containing K.

Proof. We see $\sigma \in \mathrm{Aut}_{K(\alpha)}(F)$ if and only if $\sigma(\alpha) = \alpha$. Since α is a root of $f(X)$, this means σ only change the other $n-1$ roots. This corresponds the group $\mathfrak{S}_{n-1}$, so $\mathrm{Aut}_{K(\alpha)}(F) \cong \mathfrak{S}_{n-1}$. Since there is no subgroup between $\mathfrak{S}_{n-1}$ and $\mathfrak{S}_n$, the second claim follows. □

Exercise 9.3.7. Prove that every element of a finite field F is a sum of two squares in F.

Proof. If F has characteristic 2, then $x \mapsto x^2$ is an isomorphism of F, so we may consider the case $\mathrm{char} F \neq 2$.

We consider the map $\phi : F^\times \to F^\times$ defined by $\phi(X) = x^2$. The image of ϕ is the subset of F that can be written as a^2 for some $a \in F$. If $\phi(a) = \phi(b)$ then $a = b$ or $a = -b$. Since $\mathrm{char} F \neq 2$, we know that $b \neq -b$, so ϕ is a two-to-one map. This implies that

$$|\operatorname{im}\phi| = \frac{|F^\times|}{2} = \frac{|F|-1}{2}.$$

Since 0 is also a squre element, there are totally

$$\frac{|F|-1}{2} + 1 = \frac{|F|+1}{2}$$

squre elements in F. Let S be the set of all squre elements in F. We just observe that $|S| = (|F|+1)/2$.

For any element $x \in F$, consider the set

$$T = \{x - b^2 \mid b \in F\}$$

We onserve that $|S| = |T|$, and

$$|S| + |T| = |F| + 1 > |F|.$$

Thus $|S| \cap |T| \neq \varnothing$. This immediately implies that x is a sum of squres. □

Exercise 9.3.8. Find the cyclotomic polynomials $\Phi_{2^m}(X)$ for all $m \geq 0$.

Proof. We have by Lemma 9.3.36

$$X^{2^m} - 1 = \prod_{i=1}^{m} \Phi_{2^i}(X)$$

so

$$\Phi_{2^m}(X) = \frac{X^{2^m} - 1}{X^{2^{m-1}} - 1} = X^{2^{m-1}} + 1$$

which gives the result. □

Exercise 9.3.9. For a prime p, find the factorization of $\Phi_p(X)$ over $\mathbb{F}_p$.

Proof. We have

$$(a-b)^p = a^p + (-1)^p b^p = a^p - b^p$$

on $\mathbb{F}_p$. So

$$\Phi_p(X) = \frac{X^p - 1}{x - 1} = \frac{(X-1)^p}{X-1} = (X-1)^{p-1}$$

which gives the result. □

Exercise 9.3.10. For a, b, c positive integers with $c > 1$, prove that $c^a - 1$ divides $c^b - 1$ if and only if $a \mid b$. Prove that $X^a - 1$ divides $X^b - 1$ in $\mathbb{Z}[X]$ if and only if $a \mid b$.

Proof. For the interesting implications, assume $c^a - 1 \mid c^b - 1$, write $b = ad + r$, then we have

$$c^b - 1 = c^{ad} \cdot c^r - 1 = c^{ad} \cdot c^r - c^r + c^r - 1 = c^r(c^{ad} - 1) + c^r - 1$$

since $c^a - 1 \mid c^{ad} - 1$, we know that $c^a - 1 \mid c^r - 1$. This implies $a \leq r$, which is a contradiction. So $a \mid d$. □

Exercise 9.3.11. Let a, n be positive integers, with $a > 1$. Prove that if $\Phi_n(a)$ divides $a - 1$, then $n = 1$.

Proof. If $n > 1$, then every primitive n-th root satisfies

$$|a - \zeta| > a - 1$$

Now we have $\Phi_n(a) \mid a - 1$, this is a contradiction, since $|\Phi_n(a)| = \prod |a - \zeta| > a - 1$. □

Exercise 9.3.12. Let a, d, n be positive integers, with $d < n$ and $a > 1$. Assume that $a^d - 1$ divides $a^n - 1$. Prove that $\Phi_n(a)$ divides the quotient $(a^n - 1)/(a^d - 1)$.

Proof. We know that $d \mid n$, so

$$\Phi_n(X) = \frac{X^n - 1}{\prod_{1 \le d \mid n, d < n} \Phi_d(X)} = \frac{X^n - 1}{\prod_{\substack{1 \le i \mid n \\ i < n, i \ne d}} \Phi_i(X) \cdot \Phi_d(X)} = \frac{(X^n - 1) \prod_{1 \le j \mid d, j < d} \Phi_j(X)}{\prod_{\substack{1 \le i \mid n \\ i < n, i \ne d}} \Phi_i(X)(X^d - 1)}$$

but if $j \mid d$, then $j \mid n$, so for the quotient we have

$$\frac{(X^n - 1) \prod_{1 \le j \mid d, j < d} \Phi_j(X)}{\prod_{\substack{1 \le i \mid n \\ i < n, i \ne d}} \Phi_i(X)(X^d - 1)} = \frac{X^n - 1}{X^d - 1} \frac{1}{\prod_{1 \le i \mid n, i \nmid d} \Phi_i(X)}$$

this show $\Phi_n(X) \mid (X^n - 1)/(X^d - 1)$. □

Exercise 9.3.13. Let R be a finite division ring.

- Prove that the center of R is isomorphic to $\mathbb{F}_q$, for q a prime power. Prove that $|R| = q^n$ for some n.
- For every $x \in R$, prove that the centralizer of x in the multiplicative group $(R^\times, \cdot)$ has order $q^d - 1$ for some $d \le n$.
- Prove that there are integers $d_1, \ldots, d_r < n$ such that

$$q^n - 1 = q - 1 + \sum_{i=1}^{r} \frac{q^n - 1}{q^{d_i} - 1}$$

- Deduce that $\Phi_n(q)$ divides $q - 1$ and hence $n = 1$.
- Conclude that R equals its center, showing that R is commutative.

Thus, every finite division ring is a field: this is Wedderburn's little theorem. The argument given here is due to Ernst Witt.

Proof. Note that for any $r \in R^\times, x \in R$,

$$rx = xr \Leftrightarrow r^{-1}x = xr^{-1}$$

So the center of R is closed under inversion, hence is a subfield. Set $F := Z_R$, we know that $F \cong \mathbb{F}_q$ for some q a prime power. Then R becomes a K-vector space with finite dimension, denoted it by n. Then $|R| = q^n$.

For every $x \in R$, the centralizer of x is the stablizer of x under congruence action in $R^\times$. So it is a subgroup of $R^\times$, with order $q^d - 1$. Since $q^d - 1 \mid |R^\times| = q^n - 1$, we have $d \mid n$. Recall the class formula:

$$|R^\times| = |G| + \sum |R^\times : G_x|$$

where G is the set of fixed points, that is, $F \setminus \{0\}$. Since each G_x has order $q^d - 1$ for some $d \mid n$, we get the equation

$$q^n - 1 = q - 1 + \sum_{i=1}^{r} \frac{q^n - 1}{q^{d_i} - 1}$$

Since $d_i \mid n$, $d_i < n$, we have

$$\frac{X^n - 1}{X^{d_i} - 1} = \prod_{d \mid n, d \nmid d_i} \Phi_d(X)$$

note that $n \mid n$, so $\Phi_n(X)$ is in the product above. Concluding we get

$$\Phi_n(X) \mid \frac{X^n - 1}{X^{d_i} - 1}$$

At the same time, $\Phi_n(X) \mid X^n - 1$. Plug into $x = q$ yields $\Phi_n(q) \mid q - 1$. But this is only possible when $n = 1$. So $F = R$. □

Exercise 9.3.14. Let a, p, n be integers, with p, n positive and p prime, $p \nmid n$.

- Show that $X^n - 1$ has no multiple roots modulo p.
- Show that if p divides $\Phi_n(a)$, then $a^n \equiv 1$ modulo p. (In particular, $p \nmid a$, so $[a]_p \in (\mathbb{Z}/p\mathbb{Z})^\times$.)
- Show that if p divides $\Phi_n(a)$, then $a^d \not\equiv 1$ modulo p for every $d < n$.
- Deduce that $p \mid \Phi_n(a)$ if and only if the order of $[a]_p$ in $(\mathbb{Z}/p\mathbb{Z})^\times$ is n.
- Compute $\Phi_{15}(9)$, and show it is divisible by 31.

Proof. The polynomial $f(X) := X^n - 1$ is separable over $\mathbb{F}_p$, since $f(X)' = nX^{n-1}$. Since $p \nmid n$, we conclude that $(f(X), f(X)') = 1$, so $f(X)$ is separable.

Since

$$a^n - 1 = \prod_{1 \le d \mid n} \Phi_d(a)$$

modding p we get the claim in the second point.

If there is some $d < n$ such that $a^d \equiv 1$ modulo p, then d must be a divisor of n (order consideration). And from the formula

$$a^d - 1 = \prod_{1 \le i \mid d} \Phi_i(a)$$

we know that there is some $i < d$, $i \mid d$ such that $\Phi_i(a) \equiv 0$ modulo p. Agian from

$$a^n - 1 = \prod_{1 \le d \mid n} \Phi_d(a)$$

and $i \mid d \mid n$, we know that $a^n - 1$ at least has two roots in $\mathbb{F}_p$, which cotradicts our previous result.

One direction is immediate. Assume a has order p, then $a^n = 1$, $a^d \not\equiv 1$ for $d < n$. Then we claim that $\Phi_d(a) \not\equiv 0$ for $d < n$: In fact, for any $d < n$, we have

$$a^d - 1 = \prod_{1 \le i \mid d} \Phi_i(a)$$

since $a^d \not\equiv 1$, we get the claim. □

Exercise 9.3.15. Let a, p, n be integers, with p, n positive and p prime, $p \nmid n$. Assume that p divides $\Phi_n(a)$. Prove that $p \equiv 1 \bmod n$.

Proof. From Exercise 9.3.14, we know that $[a]_p$ has order n in $(\mathbb{Z}/p\mathbb{Z})^\times$. In particular, $n \mid p - 1$. □

9.4 Transcendental extensions

9.4.1 Transcendental basis

Definition 9.4.1. *Let E/K be a field extension. A subset S of E is* ***algebraically dependent over K*** *if there exists a finite subset $\{s_1, \ldots, s_n\} \subseteq S$ and a nonzero polynomial $f(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$ with $f(s_1, \ldots, s_n) = 0$. A subset S of E is* ***algebraically independent*** *if it is not algebraically dependent. An extension field E/K is* ***purely transcendental*** *if either $E = K$ or E contains an algebraically independent subset S and $E = K(S)$.*

In fancier language, consider the map defined by

$$K[S] \to K, \quad f(X_1, \ldots, X_n) \mapsto f(s_1, \ldots, s_n).$$

Then S is algebraically independent if and only if this map is injective. Since algebraically dependent subsets are necessarily nonempty, it follows that the empty subset $\varnothing$ is algebraically independent. A singleton $\{\alpha\} \subseteq E$ is algebraically dependent if α is algebraic over K. If $\{\alpha\}$ is algebraically independent, then α is transcendental over K, in which case $K(\alpha) \cong K(X)$. The following lemma extends the second case in Proposition 9.1.5.

Lemma 9.4.2. *Let E/K be a purely transcendental extension with $S = \{s_1, \ldots, s_n\}$ is a finite algebraically independent subset. If $K(X_1, \ldots, X_n)$ is the function field with indeterminates $X_1, \ldots, X_n$, then there is an isomorphism $K(X_1, \ldots, X_n) \cong E$ with $X_i \mapsto s_i$ for all i.*

Proof. The bijection $X = \{X_1, \ldots, X_n\} \to S$ given by $X_i \mapsto s_i$ extends to an isomorphism $K[X_1, \ldots, X_n] \cong K[s_1, \ldots, s_n]$, which in turn extends to an isomorphism of fraction fields. □

We can now improve Lemma 9.4.2 by removing the finiteness hypothesis.

Theorem 9.4.3. *Let E/K be a purely transcendental extension; that is, $E = K(S)$, where S is an algebraically independent subset. Then $E \cong K(X)$, the function field with indeterminates X, where $|X| = |S|$, via an isomorphism $\varphi : K(X) \to E$ with $\varphi(X) \in S$ for all $x \in X$.*

Proof. By the well ordering principle, we may assume that S is well-ordered. Now let X be a set equipped with a bijection $h : X \to S$; we may assume that X is well-ordered by defining $x \le y$ to mean $h(x) \le h(y)$. If $y \in X$, define

$$X_y = \{x \in X : x \le y\} \quad S_y = \{h(x) \in S : x \le y\}.$$

We prove by transfinite induction that there are isomorphisms $\varphi_y : K(X_y) \to K(S_y)$ with $\varphi_y(x) = h(x)$ for all $x \le y$ and with φ_{y_2} extending φ_{y_1} whenever $y_1 \le y_2$. This will suffice, for $K(X) = \bigcup_{y \in X} K(X_y)$ and $E = K(S) = \bigcup_{y \in X} K(S_y)$.

The base step was proved in Lemma 9.4.2 with $E = K(S_y) = K(y)$, where y is the smallest element in S. The inductive step wants an isomorphism $\varphi_z : K(X_z) \to K(S_z)$ with $y \mapsto h(y)$ for all $y \leq z$. If z is a successor, say z is the next index after y, then $K(X_y)(z) = K(X_z)$, and Lemma 9.4.2 gives an isomorphism $K(X_y)(z) \to K(S_y)(h(z))$. If z is a limit, observe that the family of subfields $K(X_y)$ for all $y < z$ is an increasing chain, and so $K_* = \bigcup_{y<z} K(X_y)$ is a field; similarly, $E_* = \bigcup_{y<z} K(S_y)$ is a field. If $y_1 \leq y_2 < z$, then the isomorphism φ_{y_2} extends φ_{y_1}, so that $\bigcup_{y<z} \varphi_y$ is a (well-defined) isomorphism from K_* to E_*. As the isomorphisms φ_y agree whenever possible, they can be assembled to an isomorphism $\varphi_z : K(X_z) \to K(S_z)$. This finishes the induction process and hence the proof. □

Recall that if V is a vector space and $S = \{v_1, \dots, v_n\}$ is a subset in V, then S is linearly dependent if and only if some v_i is in the subspace spanned by the others. Here is an analog of this for algebraic dependence.

Proposition 9.4.4. *Let E/K be an extension field. Then $S \subseteq E$ is algebraically dependent over K if and only if there is $s \in S$ with s is algebraic over $K(S \setminus \{s\})$.*

Proof. If S is algebraically dependent over K, then there is a finite algebraically dependent subset $\{s_1, \dots, s_n\} \subseteq S$; thus, we may assume that S is finite. We prove, by induction on n, that some s_i is algebraic over $K(S \setminus \{s_i\})$.

If $n = 1$, then there is some nonzero $f(X) \in K[X]$ with $f(s_1) = 0$; that is, s_1 is algebraic over K. But $S \setminus \{s_1\} = \varnothing$, and so s_1 is algebraic over $K(S \setminus \{s_1\}) = K(\varnothing) = K$.

For the inductive step, let $S = \{s_1, \dots, s_{n+1}\}$ be algebraically dependent. We may assume that $\{s_1, \dots, s_n\}$ is algebraically independent (otherwise, the inductive hypothesis gives some s_j, for $1 \leq j \leq n$, which is algebraic over $K(s_1, \dots, \widehat{s_j}, \dots, s_n)$ and, hence, algebraic over $K(S \setminus \{s_j\})$). Since S is algebraically dependent, there is a nonzero $f(X_1, \dots, X_n, Y)$ in $K[X_1, \dots, X_n, Y]$ with $f(s_1, \dots, s_n, s_{n+1}) = 0$. We may write

$$f(X_1, \dots, X_n, Y) = \sum_i g_i(X_1, \dots, X_n) Y^i$$

where $g_i \in K[X_1, \dots, X_n]$. Since $f(X_1, \dots, X_n, Y) \neq 0$, some $g_i(X_1, \dots, X_n) \neq 0$, and it follows from the algebraic independence of $\{s_1, \dots, s_n\}$ that $g_i(s_1, \dots, s_n) \neq 0$. Therefore, $h(Y) = \sum_i g_i(s_1, \dots, s_n) Y^i \in K(S)[Y]$ is not the zero polynomial. But $h(s_{n+1}) = f(s_1, \dots, s_n, s_{n+1}) = 0$, so that un+1 is algebraic over $K(s_1, \dots, s_n)$.

For the converse, assume that s is algebraic over $K(S \setminus \{s\})$. We may assume that $S \setminus \{s\}$ is finite. We prove, by induction on $n = |S|$, that S is algebraically dependent.

If $n = 1$, then $S = \{s\}$, and s is algebraic over K. Therefore S is algebraically dependent. For the inductive step, let $S = \{s_1, \dots, s_{n+1}\}$, and we may assume that s_{n+1} is algebraic over $K(\{s_1, \dots, s_n\})$. We may assume that $\{s_1, \dots, s_n\}$ is algebraically independent, since otherwise S, as a superset of it, is also algebraically dependent. By hypotheses, there is a nonzero polynomial $f(Y) = \sum_i c_i Y^i \in K(s_1, \dots, s_n)[Y]$ with $f(s_{n+1}) = 0$. As $f(Y) \neq 0$, we may assume that at least one of its coefficients is nonzero. For all i, the coefficient $c_i \in K(s_1, \dots, s_n)$, so there are rational functions $c_i(X_1, \dots, X_n)$ with $c_i(s_1, \dots, s_n) = c_i$ (because $K(s_1, \dots, s_n) \cong K(X_1, \dots, X_n)$, the function field in n variables). Since $f(s_{n+1}) = 0$, we may clear denominators and assume that each $c_i(X_1, \dots, X_n)$ is a polynomial in $K[x_1, \dots, x_n]$. Moreover, that some $c_i(s_1, \dots, s_n) \neq 0$

implies $c_i(s_1, \ldots, s_n) \neq 0$. Hence

$$c(X_1, \ldots, X_n, Y) = \sum_i c_i(X_1, \ldots, X_n)Y^i \in K[X_1, \ldots, X_n, Y]$$

is nonzero and vanishes on $(s_1, \ldots, s_{n+1})$; therefore, $S = \{s_1, \ldots, s_{n+1}\}$ is algebraically dependent. □

There is a strong parallel between linear dependence in a vector space and algebraic dependence in a field. The analog of a basis in a vector space is a transcendental basis in a field; the analog of dimension is transcendence degree. In fact, both discussions are special cases of theorems about **dependence relations**.

Let E/K be an extension field. If $\alpha \in E$ and $S \subseteq E$, then α is **dependent on S**, denoted by

$$\alpha \preceq S,$$

if α is algebraic over $K(S)$, the subfield of E generated by K and S.

Proposition 9.4.5. *Let E/K be an extension field, let $\alpha \in E$, and let $S \subseteq E$.*

(i) *(**Reflexivity**) If $\alpha \in S$, then $\alpha \preceq S$.*

(ii) *(**Compactness**) If $\alpha \in S$, then there exists a finite subset $S_0 \subseteq S$ with $\alpha \preceq S_0$.*

(iii) *(**Transitivity**) Let $T \subseteq E$; if $\alpha \in S$ and each element of S is dependent on T, then α is dependent on T.*

(iv) *(**Exchange Property**) If α is dependent on $S \cup \{\beta\}$ but not on S, then β is dependent on $S \cup \{\alpha\}$ but not on S.*

Proof. It is easy to check (i) and (ii). We now verify (iii). If $\alpha \preceq S$, then α is algebraic over $K(S)$. Suppose there is some $T \subseteq E$ with $s \preceq T$ for every $s \in S$; then it follows from Theorem 9.1.22 that $K(T) \subseteq K(S)(T)$ is an algebraic extension. Since α is algebraic over $K(S)$ and hence $K(S)(T)$, it is then algebraic over $K(T)$. That is, α is dependent on T.

Let us verify (iv). The exchange property assumes that $\alpha \preceq S \cup \{\beta\}$ (that is, α is algebraic over $K(S \cup \{\beta\})$) and α is transcendental over $K(S\backslash)$. We first note that $\beta \not\preceq S$: otherwise β is algebraic over $K(S)$, and hence $K(S) \subseteq K(S \cup \{\beta\})$ is algebraic. But this implies α is algebraic over $K(S)$, which contradicts the hypothesis. Now since $K(S \cup \{\beta\}) = K(S)(\beta)$, we conclude from Proposition 9.4.4 that $\{\alpha, \beta\}$ is algebraic dependent over $K(S)$. Thus there is a nonzero polynomial $f(X, Y) \in K(S)[X, Y]$ with $f(\alpha, \beta) = 0$. In more detail, $f(X, Y) = g_0(X) + g_1(X)Y + \cdots + g_n(X)Y^n$, where $g_i(X) \in K(S)[X]$. Define $h(Y) = f(\alpha, Y) = \sum_i g^i(\alpha)Y^i \in K(S, \alpha)[Y]$. Since α is not dependent on S, $h(Y)$ is not the zero polynomial. But $h(\beta) = f(\alpha, \beta) = 0$, so β is dependent on $S \cup \{\alpha\}$. □

Returning to extension fields E/K, by Proposition 9.4.4 a nonempty subset $S \subseteq E$ is algebraically independent if and only if $s \not\preceq S \setminus \{s\}$ for all $s \in S$. It follows that every subset of an algebraically independent set is itself algebraically independent.

Definition 9.4.6. *If E/K is an extension field, then a subset $S \subseteq E$ **generates** E if $x \preceq S$ for all $x \in E$. Or equivalently, if E is algebraic over $K(S)$. A **transcendental basis** is a maximal algebraically independent subset of E over K.*

Lemma 9.4.7. *Let E/K be an extension field. If $S \subseteq E$ is algebraically independent over K and $\alpha \in E$ is transcendental over $K(S)$, then $S \cup \{\alpha\}$ is algebraically independent.*

Proof. Since $\alpha \not\preceq S$, Proposition 9.4.5(i) gives $\alpha \notin S$, and so $S \subsetneq S \cup \{\alpha\}$. If $S \cup \{\alpha\}$ is algebraically dependent, then there exists $s \in S \cup \{\alpha\}$ with $s \preceq (S \cup \{\alpha\}) \setminus \{s\}$. If $s = \alpha$, then $(S \cup \{\alpha\}) \setminus \{s\} = S$, contradicting $\alpha \not\preceq S$. Therefore, $s \in S$. Since S is algebraically independent, $s \not\preceq S \setminus \{s\}$. Combining with the observation $(S \cup \{\alpha\}) \setminus \{s\} = (S \setminus \{s\}) \cup \{\alpha\}$, we obtain

$$s \preceq (S \setminus \{s\}) \cup \{\alpha\}, \quad s \not\preceq S \setminus \{s\}.$$

Therefore it follows from the exchange property that $\alpha \preceq (S \setminus \{s\}) \cup \{s\} = S$, contradicting the hypothesis. Therefore $S \cup \{\alpha\}$ is algebraically independent. □

Note that Lemma 9.4.7 implies that a if S is a transcendental basis of E, then S automatically generates E: there is no element in E that is transcendental over $K(S)$. We now prove that every algebraically independent set in E can be extended to a maximal algebraically independent set, and hence a transcendantal basis for E.

Theorem 9.4.8. *If E/K is an extension field, then E has a transcendental basis. In fact, every algebraically independent subset is part of a transcendental basis.*

Proof. Let S be an algebraically independent subset of E. We use Zorn's Lemma to prove the existence of maximal algebraically independent subsets of E containing S. Let $\mathcal{X}$ be the family of all algebraically independent subsets of E containing S, partially ordered by inclusion. Note that X is nonempty, for $S \in \mathcal{X}$. Suppose that $\mathcal{S} = (S_\alpha)_{\alpha \in A}$ is a chain in $\mathcal{X}$. It is clear that $S^* = \bigcup_{\alpha \in A} S_\alpha$ is an upper bound of $\mathcal{S}$ if it lies in $\mathcal{X}$, that is, if S^* is algebraically independent. If, on the contrary, S^* is algebraically dependent, then there is $s \in S^*$ with $s \preceq S^* \setminus \{s\}$. By the compactness property, there is a finite subset $\{s_1, \ldots, s_n\} \subseteq S^* \setminus \{s\}$ with $s \preceq \{s_1, \ldots, s_n\}$. Now there is $S_0 \in \mathcal{S}$ with $s \in S_0$, and, for each i with $1 \leq i \leq n$, there is S_{α_i} with $s_i \in S_{\alpha_i}$. Since $\mathcal{S}$ is a chain, one of these, call it S', contains all the others, and the algebraically dependent set $\{s, s_1, \ldots, s_n\}$ is contained in S'. But since S' is algebraically independent, so are its subsets, and this is a contradiction. Zorn's Lemma now provides a maximal element M of $\mathcal{X}$; that is, M is a maximal algebraically independent subset of E containing S. If M is not a basis, then there exists $\alpha \in E$ with $\alpha \not\preceq M$. By Lemma 9.4.7, $M \cup \{\alpha\}$ is an algebraically independent set strictly larger than M, contradicting the maximality of M. □

Theorem 9.4.9. *If E/K be a field extension. Then a subset $S \subseteq E$ is a transcendental basis for E/K if and only if S is algebraically independent and $E/K(S)$ is algebraic.*

Proof. One direction is clear from our observation, so assume that $S \subseteq E$ is auch that $K(S)/K$ is purely transcendental and $E/K(S)$ is algebraic. By definition, this means S is an algebraically independent set, and that S is maximal. Therefore S is a transcendental basis for E. □

We now prove an important theorem about the cardinality of a transcendental basis for E. It allows us to define the "dimension" of a transcendental extension.

Theorem 9.4.10. *Let E/K be a field extension. Then any transcendental basis of E over K has the same cardinality.*

Proof. Let S and T be two transcendantal basis for E over K. If $S = \varnothing$, we claim that $T = \varnothing$. Otherwise, there exists $t \in T$. We have $t \preceq S$ since S generates E and $\varnothing \subseteq T \setminus \{t\}$, so that transitivity gives $t \preceq T \setminus \{t\}$, a contradiction since T is algebraically independent. Therefore, we may assume that both S and T are nonempty.

Now assume that S is finite; say, $S = \{s_1, \dots, s_n\}$. We claim that some $t_1 \in T$ is transcendental over $K(s_2, \dots, s_n)$. Assume the contrary, then every element in T is algebraic over $K(s_2, \dots, s_n)$, whence $K(s_2, \dots, s_n)(T)$ is algebraic over $K(s_2, \dots, s_n)$ by Theorem 9.1.22. Since E is algebraic over $K(T)$, it is necessarily algebraic over $K(T)(s_2, \dots, s_n) = K(s_2, \dots, s_n)(T)$. Therefore E is algebraic over $K(s_2, \dots, s_n)$ by Corollary 9.1.21. In partial, s_1 is algebraic over $K(s_2, \dots, s_n)$. But S is algebraically independent over K, this is a contradiction. Thus some $t_1 \in T$ must be transcendental over $K(s_2, \dots, s_n)$, and consequently $\{t_1, s_2, \dots, s_n\}$ is algebraic independent by Lemma 9.4.7.

Now if s_1 were transcendental over $K(t_1, s_2, \dots, s_n)$, then $\{t_1, s_1, s_2, \dots, s_n\}$ is algebraic independent over K, which is impossible since S is a maximal algebraically independent set. consequently, $K(S)(t_1) = K(t_1, s_2, \dots, s_n)(s_1)$ is algebraic over $K(t_1, s_2, \dots, s_n)$, whence E is algebraic over $K(t_1, s_2, \dots, s_n)$ (Theorem 9.4.9). Therefore $\{t_1, s_2, \dots, s_n\}$ is a transcendental basis for E by Theorem 9.4.9.

A similar argument shows that some $t_2 \in T$ is transcendental over $K(t_1, s_3, \dots, s_n)$, and hence $\{t_1, t_2, s_3, \dots, s_n\}$ is a transcendental basis for E. Repeating this process we eventually obtain $t_1, \dots, t_n \in T$ such that $\{t_1, \dots, t_n\}$ is a transcendantal basis for E over K. This implies $T = \{t_1, \dots, t_n\}$ and therefore $|T| = |S|$.

Finally, we assume that S is infinite. Then by the argument above, T must also be infinite. If $s \in S$, then s is algebraic over $K(T)$. The coefficients of the minimal polynomial f of s over $K(T)$ all lie in $K(T_s)$ for some finite subset $T_s \subseteq T$. Consequently, $f \in K(T_s)[X]$ and s is algebraic over $K(T_s)$. Choose such a finite set T_s for each s. We claim that $T = \bigcup_{s \in S} T_s$. In fact, if $t \in T \setminus \{T_s\}$, then for any $s \in S$ we have $T_s \subseteq T \setminus \{t\}$ and thus

$$s \preceq T_s \preceq T \setminus \{t\}.$$

This then implies $t \preceq S \preceq T \setminus \{t\}$, which contradicts the algebraically independence of T. With this, we conclude

$$|T| = \left| \bigcup_{s \in S} T_s \right| \leq \aleph_0 \cdot |S| = |S|.$$

Reversing the roles of S and T shows that $|S| = |T|$. □

Definition 9.4.11. *Let E/K be a field extension, the* ***transcendental degree of EK*** *is defined by*

$$\operatorname{tr.deg}(E/K) = |S|$$

where $|S|$ is any transcendental degree for E over K.

Proposition 9.4.12 (Additivity of transcendental degree). *Let $K \subseteq E \subseteq F$ be field extensions. Then*

$$\operatorname{tr.deg}(F/K) = \operatorname{tr.deg}(F/E) + \operatorname{tr.deg}(E/K).$$

Proof. Let S be a transcendental besis of E over K, and T be that of F over E. Since $S \subseteq E$, $S \cap T = \varnothing$. It suffices if we show $S \cup T$ is a transcendental basis of F over K.

First of all, E is algebraic over $K(S)$ by Theorem 9.4.9, and hence over $K(S \cup T)$. Thus $K(S \cup T)(E)$ is algebraic over $K(S \cup T)$ by Theorem 9.1.22. Since

$$K(S \cup T) = K(S)(T) \subseteq E(T) \subseteq K(S \cup T)(E),$$

it follows from Corollary 9.1.21that $E(T)$ is algebraic over $K(S \cup T)$. Since F is algebraic over $E(T)$ by Theorem 9.4.9, we conclude that F is algebraic over $K(S \cup T)$. Now we only need to prove $S \cup T$ is algebraically independent.

Suppose there is a polynomial $f(X_1, \ldots, X_n, Y_1, \ldots, Y_m)$ such that

$$f(s_1, \ldots, s_n, t_1, \ldots, t_m) = 0$$

for some $s_1, \ldots, s_n \in S$, $t_1, \ldots, t_m \in T$. Since S and T are both algebraically independent, the coefficients of s_i, t_j are not trivial. Then we can write

$$h(Y_1, \ldots, Y_m) := f(s_1, \ldots, s_n, Y_1, \ldots, Y_m) \in K(S)[Y_1, \ldots, Y_m]$$

satisfies $h(t_1, \ldots, t_m) = 0$. Since $s_1, \ldots, s_n \in E$, this means T is not algebraically independent over E, which is an contradiction. □

Now we use Proposition 9.4.12 to prove the following useful result.

Proposition 9.4.13. *Let $K \subseteq E \subseteq L$ be field extensions and suppose that E/K is algebraic. If $S \subseteq L$ is algebraically independent over K, then S is also algebraically independent over E. In other words, L remains algebraically independent over any algebraic extension of the base field.*

Proof. Since $K \subseteq E$ is algebraic, so is the extension $K(S) \subseteq E(S)$. Now, by Proposition 9.4.12,

$$\operatorname{tr.deg}(E(S)/E) + \operatorname{tr.deg}(E/K) = \operatorname{tr.deg}(E(S)/K) = \operatorname{tr.deg}(E(S)/K(S)) + \operatorname{tr.deg}(K(S)/K)$$

and so

$$\operatorname{tr.deg}(E(S)/E) = \operatorname{tr.deg}(K(S)/K) = |S|$$

which shows that S must be a transcendence basis for L over E. □

9.4.2 Simple transcendantal extension and Lüroth's theorem

The class of purely transcendental extensions is much less well behaved than the class of algebraic extensions. For example, let α be transcendental over K. Then in the tower $K \subseteq K(\alpha^2) \subseteq K(\alpha)$, the extension $K \subseteq K(\alpha)$ is purely transcendental (and simple) but the second step $K(\alpha^2) \subseteq K(\alpha)$ is not transcendental at all. In addition, if $K \subseteq L$ is purely transcendental and $K \subseteq E \subseteq L$, it does not necessarily follow that the extension L/E is purely transcendental.

However, there is a famous theorem about the simple extension $K \subseteq K(X)$ which identify every intermediate field of this extension. We now prove this theorem to illustrate some of the apparent complexities in dealing with transcendental extensions.

We first consider the automorphism group $\operatorname{Aut}_K(K(X))$. A rational function $\varphi \in K(X)$ is called a **linear fractional transformation** if

$$\varphi = \frac{aX + b}{cX + d}$$

where $a, b, c, d \in K$ and $ad - bc \neq 0$. The function φ can be viewed as a automorphism on $K(X)$ just by sending x to φ. The linear fractional transformations turns out to be the whole groups $\mathrm{Aut}_K(K(X))$. To prove this, we need the following definition.

Definition 9.4.14. *If $\varphi \in K(X)$ is in lowest terms, then $\varphi = g(X)/h(X)$, where $g(X), h(X) \in K[X]$ and $\gcd(g, h) = 1$. Define the **degree** of φ by*

$$\deg(\varphi) = \max\{\deg(g), \deg(h)\}.$$

Now $\varphi \in K(X)$ has height 0 if and only if φ is a constant (that is, $\varphi \in K$), while φ has height 1 if and only if φ is a linear fractional transformation.

Proposition 9.4.15. *Let K be a field, let $\varphi = g(X)/h(X) \in K(X)$ be nonconstant, where $g(X) = \sum_i a_i X^i$, $h(X) = \sum_i b_i X^i$, and $\gcd(g, h) = 1$. Then*

(i) φ is transcendental over K.

(ii) $K(X)$ is a finite extension of $K(\varphi)$;

(iii) the minimal polynomial of x over $K(\varphi)$ is $\theta(Y)$, where

$$\theta(Y) = g(Y) - \varphi h(Y) \in K(\varphi)[Y]$$

and therefore $[K(X) : K(\varphi)] = \deg(\varphi)$.

Proof. Let us describe $\theta(Y)$ in more detail (we allow some coefficients of g and h to be zero, so that even though we use the same index i of summation, we are not assuming that g and h have the same degree). We have

$$\theta(Y) = g(Y) - \varphi h(Y) = \sum_i (a_i - \varphi b_i) Y^i.$$

If $\theta(Y)$ is the zero polynomial, then all its coefficients are 0. But h is not the zero polynomial (being the denominator of φ), so h has some nonzero coefficient, say b_i. If the i-th coefficient $a_i - \varphi b_i$ of θ is 0, then $\varphi = a_i/b_i$, contradicting φ not being a constant. Thus, $\theta \neq 0$. We compute $\deg(\theta)$:

$$\deg(\theta) = \deg(g(Y) - \varphi h(Y)) = \max\{\deg(g), \deg(h)\} = \deg(\varphi).$$

Now x is a root of θ, because $\varphi = g/h$; therefore x is algebraic over $K(\varphi)$ and $K(X)/K(\varphi)$ is a finite extension field.

Were φ algebraic over K, then $K(\varphi)/K$ would be finite, and so

$$[K(X) : K] = [K(X) : K(\varphi)][K(\varphi) : K]$$

is also finite, a contradiction. Therefore, φ is transcendental over K. Thus we have verifed statements (i) and (ii).

We claim that $\theta(Y)$ is an irreducible polynomial in $K(\varphi)[Y]$. If not, then $\theta(Y)$ factors in $K[\varphi][Y] = K[Y][\varphi]$, by Gauss's Lemma. But $\theta(Y) = g(Y) - \varphi h(Y)$ is of degree one in φ, and $\gcd(g, h) = 1$, so it is irreducible in $K[Y][\varphi]$, contradiction. Finally, since $\deg(\theta) = \deg(\varphi)$, we have $[K(X) : K(\varphi)] = \deg(\varphi)$. □

Corollary 9.4.16. *Let $\varphi \in K(X)$, where $K(X)$ is the field of rational functions over a field K. Then $K(\varphi) = K(X)$ if and only if φ is a linear fractional transformation.*

Define a map $\rho : \mathrm{GL}(n, K) \to \mathrm{Aut}_K(K(X))$ by

$$\rho : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \frac{aX + b}{cX + d}$$

It is easily checked that ρ is a homomorphism of groups: If $\varphi : x \mapsto (aX + b)/(cX + d)$ and $\psi : X \mapsto (rX + s)/(tX + u)$, then

$$\begin{aligned}\sigma(\begin{pmatrix} r & s \\ t & u \end{pmatrix} \sigma \begin{pmatrix} a & b \\ c & d \end{pmatrix}(X) = (\psi \circ \varphi)(X) = \frac{r\varphi + s}{t\varphi + u} &= \frac{\frac{r(aX+b)}{cX+d} + s}{\frac{t(aX+b)}{cX+d} + u} = \frac{r(aX + b) + s(cX + d)}{t(aX + b) + u(cX + d)} \\ &= \frac{(ra + sc)X + (rb + sd)}{(ta + uc)X + (tb + bd)} = \sigma\Big(\begin{pmatrix} r & s \\ t & u \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\Big)(X).\end{aligned}$$

It is clear that the $\ker \rho = Z(2, K)$, the center of $\mathrm{GL}(n, K)$ consisting of all nonzero 2×2 scalar matrices. Hence, if

$$\mathrm{PGL}(2, K) = \mathrm{GL}(2, K)/Z(2, K)$$

then $\mathrm{Aut}_K(K(X)) \cong \mathrm{PGL}(2, K)$.

Corollary 9.4.17. *If $K(X)$ is the field of rational functions over a field K, then* $\mathrm{Aut}_K(K(X)) = \mathrm{PGL}(2, K)$.

We now prove Lüroth's Theorem which classifies all the intermediate fields $K \subsetneq E \subseteq K(X)$, where X is transcendental over K; the proof is essentially a converse of that of Proposition 9.4.15.

Lemma 9.4.18. *Let K be a field, and let*

$$I(X, Y) = Y^n + \frac{g_{n-1}(X)}{h_{n-1}(X)}Y^{n-1} + \cdots + \frac{g_0(X)}{h_0(X)} \in K(X)[Y]$$

where each g_i/h_i is in lowest terms. If $I^*(X, Y) \in K[X][Y]$ is the associated primitive polynomial of I, then

$$\max\{\deg(g_i/h_i)\} \leq \deg_X(I^*),$$

where $\deg_X(I^*)$ is the highest power of X occurring in I^*.

Proof. The associated primitive polynomial is then,

$$I^* = cI(X, Y) = cY^n + c\frac{g_{n-1}(X)}{h_{n-1}(X)}Y^{n-1} + \cdots + c\frac{g_0(X)}{h_0(X)} \in K[X, Y],$$

where $c = \mathrm{lcm}(h_0, h_1, \ldots, h_{n-1})$. Since c is the lcm, there are $u_i \in K[X]$ with $c = u_i h_i$ for all i. Hence, each coefficient $c(g_i/u_i) = u_i g_i \in K[X]$. Thus

$$\deg_X(I^*) = \max\{\deg(c), \deg(c(g_i/h_i))\} = \max\{\deg(c), \deg(u_i g_i)\}.$$

Now $h_i \mid c$ for all i, so that $\deg(h_i) \leq \deg(c)$. Also, $\deg(g_i) \leq \deg(u_i g_i)$. We conclude that $\max_i\{\deg(g_i), \deg(h_i)\} \leq \deg_X(I^*)$. □

Theorem 9.4.19 (Lüroth's Theorem). *If $K(X)$ is a simple transcendental extension, then every intermediate field E with $E \neq K$ is also a simple transcendental extension of K: there is $\varphi \in K$ with $E = K(\varphi)$.*

Proof. If $\beta \in E$ is not constant, then Proposition 9.4.15 says that β is transcendental over K, the extension $K(X)/K(\beta)$ is algebraic, and $[K(X) : K(\beta)]$ is finite. As $K(\beta) \subseteq E \subseteq K(X)$, we have

$$[K(X) : K(\beta)] = [K(X) : E][E : K(\beta)],$$

so that $K(X)/E$ is a finite extension field. Let $I(X, Y) \in E[Y]$ be the minimal polynomial of X over E:

$$I(X, Y) = Y^n + b_{n-1}Y^{n-1} + \cdots + b_0 \in K[Y]$$

(where $n = [K(X) : E]$). Each coefficient b_i of $I(X, Y)$ is a rational function lying in E, say, $b_i = g_i(X)/h_i(X)$, where $g_i, h_i \in K[X]$ and $\gcd(g_i, h_i) = 1$. Thus,

$$I(X, Y) = Y^n + \frac{g_{n-1}(X)}{h_{n-1}(X)}Y^{n-1} + \cdots + \frac{g_0(X)}{h_0(X)} \in E[Y]. \tag{4.2.1}$$

We may assume that $X \notin E$ (otherwise $E = K(X)$ and the theorem is obviously true). It follows that not all the coefficients $b_i = g_i/h_i$ of $I(X, Y)$ lie in K, otherwise X is algebraic over K. Choose an index j such that $b_j = g_j/h_j \notin K$, we simplify notation by omitting the subscript j and defining $\varphi = b_j$, $g(X) = g_j(X)$, and $h(X) = h_j(X)$; thus, $\varphi = g/h \in E$ with $\varphi \notin K$. Define

$$\theta(X, Y) = g(Y) - \varphi h(Y) \in K[Y]. \tag{4.2.2}$$

Since $\varphi \neq 0$, we have $\theta(X, Y) \neq 0$. But $\theta(X, X) = 0$, so $I(X, Y) \mid \theta(X, Y)$ over K. In other words, there exists $q(X, Y) \in K[Y]$ such that

$$\theta(X, Y) = q(X, Y)I(X, Y). \tag{4.2.3}$$

We are in the setting of Gauss's treatment of UFDs, and we now factor each polynomial as the product of its content and its associated primitive polynomial. We have $c(\theta) = 1/h(X)$ and $\theta = c(\theta)\theta^*$, where

$$\theta^*(X, Y) = h(X)g(Y) - g(X)h(Y) \in E[X][Y].$$

Reversing the roles of X and Y, there is an anti-symmetry: $\theta^*(Y, X) = -\theta^*(X, Y)$, thus

$$\deg_X(\theta^*) = \deg_Y(\theta^*).$$

Taking associated primitive polynomials and using (4.2.3), we get

$$\theta^*(X, Y) = q^*(X, Y)I^*(X, Y).$$

and therefore

$$\deg_X(\theta^*) = \deg_X(q^*) + \deg_X(I^*).$$

By Lemma 9.4.18, we have $\deg_X(I^*) \geq \deg(\varphi) = \deg_X(\theta^*)$, so that $\deg_X(q^*) = 0$; that is, q^* is a function of Y alone. The anti-symmetry of θ^* says that θ^* is primitive as a polynomial in X. But $\theta^* = q^*I^*$, so we must have $\deg_Y(q^*) = 0$; that is, q^* is a constant. Now take y-degree we

get

$$\deg_Y(\theta) = \deg_Y(\theta^*) = \deg_Y(I^*) = \deg_Y(I).$$

This then conclude that $[K(X) : K(\varphi)] = [K(X) : E]$, so the claim follows. $\square$

Chapter 10

Localizations

10.1 Prime ideals and maximal ideals

10.1.1 Prime ideals

Definition 10.1.1. *An ideal $\mathfrak{p}$ of a ring A is called* ***prime*** *if the ring $A/\mathfrak{p}$ is an integral domain.*

A maximal ideal $\mathfrak{m}$ of A is prime since $A/\mathfrak{m}$ is a field; then it follows from Krull's theorem that every proper ideal of A is contained in at least one prime ideal. In particular, for prime ideals to exist in a ring A, it is necessary and sufficient that A be not reduced to 0.

Let $\rho : A \to B$ be a ring homomorphism and $\mathfrak{q}$ an ideal of B. Set $\mathfrak{p} = \rho^{-1}(\mathfrak{q})$. Then the homomorphism $\bar{\rho} : A/\mathfrak{p} \to B/\mathfrak{q}$ derived from ρ by taking quotients is injective. Suppose that $\mathfrak{q}$ is prime; as the ring $B/\mathfrak{q}$ is an integral domain, so is $A/\mathfrak{p}$, being isomorphic to a subring of $B/\mathfrak{q}$. Consequently the ideal $\mathfrak{p} = \rho^{-1}(\mathfrak{q})$ is prime. In particular, let A be a subring of B. For every ideal $\mathfrak{q}$ of B, $\mathfrak{q} \cap A$ is a prime ideal A.

If ρ is surjective, then $\bar{\rho}$ is an isomorphism, so the conditions "$\mathfrak{p}$ is prime" and "$\mathfrak{q}$ is prime" are then equivalent. Hence, if $\mathfrak{p}$ and $\mathfrak{a}$ are ideals of A such that $\mathfrak{a} \subseteq \mathfrak{p}$, a necessary and sufficient condition for $\mathfrak{p}$ to be prime is that $\mathfrak{p}/\mathfrak{a}$ be prime in $A/\mathfrak{a}$.

Proposition 10.1.2. *Let A be a ring, $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ ideals of A and $\mathfrak{p}$ a prime ideal of A. If $\mathfrak{p}$ contains the product $\prod_{i=1}^n \mathfrak{a}_i$, it contains at least one of the $\mathfrak{a}_i$.*

Proof. Suppose in fact that $\mathfrak{p}$ contains none of the $\mathfrak{a}_i$. For $1 \leq i \leq n$l there exists then an element $s_i \in \mathfrak{a}_i - \mathfrak{p}$. Then $s = \prod_{i=1}^n s_i$ is contained in $\mathfrak{a}_1 \cdots \mathfrak{a}_n$ and is not contained in $\mathfrak{p}$, which is absurd. □

Corollary 10.1.3. *Let $\mathfrak{m}$ be a maximal ideal of A. Then for every integer $n > 0$, the only prime ideal containing $\mathfrak{m}^n$ is $\mathfrak{m}$.*

Proposition 10.1.4. *Let A be a ring, $\mathfrak{a}$ a non-empty set of A which is closed under addition and multiplication and $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ ideals of A. Suppose that $\mathfrak{a}$ is contained in the union of the $\mathfrak{p}_i$ and that at most two of the $\mathfrak{p}_i$ are not prime. Then $\mathfrak{a}$ is contained in one of the $\mathfrak{p}_i$.*

Proof. We argue by induction on n. The proposition is trivial if $n = 1$. Suppose that $n \geq 2$; if there exists an index j such that $\mathfrak{a} \cap \mathfrak{p}_j \subseteq \bigcup_{i \neq j} \mathfrak{p}_i$, then the set $\mathfrak{a}$, which is the union of the $\mathfrak{a} \cap \mathfrak{p}_i$ where $1 \leq i \leq n$, is contained in $\bigcup_{i \neq j} \mathfrak{p}_i$, and hence in one of the $\mathfrak{p}_i$, by the induction hypothesis. Suppose then that such an index does not exist.

For every $1 \leq j \leq n$ let y_j be an element of $\mathfrak{a} \cap \mathfrak{p}_j$ not belonging to any $\mathfrak{p}_i$ for $i \neq j$. Let k be chosen such that $\mathfrak{p}_k$ is prime if $n > 2$ and chosen arbitrarily if $n = 2$. Let $z = y_k + \prod_{j \neq k} y_j \in \mathfrak{a}$. If $i \neq k$ then $\prod_{j \neq k} y_j$ belongs to $\mathfrak{p}_i$, but $y_k \notin \mathfrak{p}_i$, whence $z \notin \mathfrak{p}_i$. On the other hand, $\prod_{j \neq k} y_j$ does not belong to $\mathfrak{p}_k$, as none of the factors y_j belongs to it and $\mathfrak{p}_k$ is prime if $n > 2$; as $y_k \in \mathfrak{p}_k$, z does not belong to $\mathfrak{p}_k$, and the proposition is established. □

Proposition 10.1.5. *Let A be a ring. Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be ideals and let $\mathfrak{p}$ be a prime ideal containing $\bigcap_{i=1}^n \mathfrak{a}_i$. Then $\mathfrak{p} \supseteq \mathfrak{a}_i$ for some i. If $\mathfrak{p} = \bigcap_{i=1}^n \mathfrak{a}_i$, then $\mathfrak{p} = \mathfrak{a}_i$ for some i.*

Proof. Suppose that $\mathfrak{p} \not\supseteq \mathfrak{a}_i$ for all i. Then for each $1 \leq i \leq n$ there exist $x_i \in \mathfrak{a}_i$ such that $x_i \notin \mathfrak{p}$, and therefore $\prod x_i \in \prod \mathfrak{a}_i \subseteq \bigcap_i \mathfrak{a}_i$; but $\prod x_i \notin \mathfrak{p}$ (since $\mathfrak{p}$ is prime). Hence $\mathfrak{p} \not\supseteq \bigcap_i \mathfrak{a}_i$, contradiction. Finally, if $\mathfrak{p} = \bigcap_{i=1}^n \mathfrak{a}_i$, then $\mathfrak{p} \subseteq \mathfrak{a}_i$ for all i and hence $\mathfrak{p} = \mathfrak{a}_i$ for some i. □

10.1.2 Nilradical and Jacobson radical

An element $x \in A$ is **nilpotent** if $x^n = 0$ for some $n > 0$.

Proposition 10.1.6. *The set $\mathfrak{n}$ of all nilpotent elements in a ring A is an ideal, and $A/\mathfrak{n}$ has no nilpotent element except 0. This is called the **nilradical** of A.*

Proof. If $x \in \mathfrak{n}$, clearly $ax \in \mathfrak{n}$ for all $a \in A$. Let $x, y \in \mathfrak{n}$: say $x^m = 0$, $y^n = 0$. By the binomial theorem (which is valid in any commutative ring), $(x+y)^{m+n-1}$ is a sum of integer multiples of products $x^r y^s$. Since $r + s = m + n - 1$, we can not have $r < m, s < n$ simutanously. Hence $(x+y)^{m+n-1} = 0$, $x + y \in \mathfrak{n}$. □

The following proposition gives an alternative definition of the nilradical.

Proposition 10.1.7. *The nilradical of A is the intersection of all the prime ideals of A.*

Proof. We divide the proof into two parts. We first prove that $\mathfrak{n}$ is contained in every prime ideal of A. Suppose a is an element of the nilradical of A, so $a^n = 0$. And let $\mathfrak{p}$ be a prime ideal of A. If a is not contained in $\mathfrak{p}$, then $a + \mathfrak{p}$ is nonzero in $A/\mathfrak{p}$. But

$$(a + \mathfrak{p})^n = a^n + \mathfrak{p} = 0 + \mathfrak{p}$$

since $\mathfrak{p}$ is prime, $A/\mathfrak{p}$ is an integral domain, which is a contradiction.

Now consider the family $\mathscr{F}$ of ideals of A that intersect the set $\{r^n\}_{n \in \mathbb{N}}$ only at 0. Clearly $\mathscr{F}$ is nonempty and ordered by inclusion. So by Zorn's lemma there is a maximal element $\mathfrak{p}$ in $\mathscr{F}$.

Now we prove that $\mathfrak{p}$ is prime: Suppose $a, b \notin \mathfrak{p}$ but $ab \in \mathfrak{p}$. Then the ideals $\mathfrak{p} + (a)$ and $\mathfrak{p} + (b)$ properly contain $\mathfrak{p}$. Since $\mathfrak{p}$ is maximal, these two ideals are not in $\mathscr{F}$. So there are $m, n > 0$ such that

$$r^m \in \mathfrak{p} + (a), \quad r^n \in \mathfrak{p} + (b)$$

Now we find $r^{m+n} \in \mathfrak{p} + (ab) = \mathfrak{p}$, which is a contradiction. This shows at least one of a, b belongs to $\mathfrak{p}$, hence $\mathfrak{p}$ is prime.

Since we find a prime ideal $\mathfrak{p}$ such that $r \notin \mathfrak{p}$, we conclude that r is not in the intersection of all prime ideals. The contrapositive gives another inclusion, which finishes the proof. □

Proposition 10.1.8. *Let A be a commutative ring, and let $\mathfrak{n}$ be its nilradical. Then $A/\mathfrak{n}$ contains no nonzero nilpotent elements. (Such a ring is said to be **reduced**.)*

Definition 10.1.9. *Define the* ***Jacobson radical*** $\mathfrak{r}$ *of* A *is defined to be the intersection of all the maximal ideals of* A.

Proposition 10.1.10. *An element* r *of* A *is in the Jacobson radical* $\mathfrak{r}$ *if and only if* $1 + rs$ *is invertible for every* $s \in A$.

Proof. Consider the ideal $\mathfrak{a} := (1 + rs)$, if $1 + rs$ is not invertible, this is a proper ideal, hence is contained in some maximal ideal $\mathfrak{m}$. Since r is in the Jacobson radical, it is contained in $\mathfrak{m}$, and then we find $1 \in \mathfrak{m}$. But $\mathfrak{m}$ is proper, this is not possible.

Assume $1 + rs$ is invertible for every $s \in A$. Consider a maximal ideal $\mathfrak{m}$: If $r \notin \mathfrak{m}$, then $\mathfrak{m} + rA$ is an ideal properly contains $\mathfrak{m}$, then $A = \mathfrak{m} + rA$ since $\mathfrak{m}$ is maximal. In particular, $1 = m + rs$ for some $m \in \mathfrak{m}$ and $s \in A$. Then $m = 1 - rs$ is invertible by assumption, which contradicts that $\mathfrak{m}$ is a maximal ideal. □

10.1.3 Coprime ideals

Two ideals $\mathfrak{a}, \mathfrak{b}$ are said to be **coprime** (or **comaximal**) if $\mathfrak{a} + \mathfrak{b} = (1)$. Clearly two ideals $\mathfrak{a}, \mathfrak{b}$ are coprime if and only if there exist $x \in \mathfrak{a}$ and $y \in \mathfrak{b}$ such that $x + y = 1$.

Proposition 10.1.11. *Let* $\mathfrak{a}$ *and* $\mathfrak{b}$ *be two relatively prime ideals of a ring* A. *Let* $\mathfrak{a}'$ *and* $\mathfrak{b}'$ *be two ideals of* A *such that every element of* $\mathfrak{a}$ *(resp.* $\mathfrak{b}$*) has a power in* $\mathfrak{a}'$ *(resp.* $\mathfrak{b}'$*). Then* $\mathfrak{a}'$ *and* $\mathfrak{b}'$ *are relatively prime.*

Proof. Under the given hypothesis, every prime ideal which contains $\mathfrak{a}'$ contains $\mathfrak{a}$ and every prime ideal which contains $\mathfrak{b}'$ contains $\mathfrak{b}$. If a prime ideal contains $\mathfrak{a}'$ and $\mathfrak{b}'$, then it contains $\mathfrak{a}$ and $\mathfrak{b}$, which is absurd, since $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime; hence $\mathfrak{a}'$ and $\mathfrak{b}'$ are relatively prime. □

Proposition 10.1.12. *Let* $\mathfrak{a}, \mathfrak{b}_1, \ldots, \mathfrak{b}_n$ *be ideals of a ring* A. *If* $\mathfrak{a}$ *is relatively prime to each of the* $\mathfrak{b}_i$, *it is relatively prime to* $\prod_{i=1}^n \mathfrak{b}_i$.

Proof. Let $\mathfrak{p}$ be a prime ideal of A. If $\mathfrak{p}$ contains $\mathfrak{a}$ and $\prod_{i=1}^n \mathfrak{b}_i$ then it contains one of the $\mathfrak{b}_i$, which is absurd since $\mathfrak{a}$ and $\mathfrak{b}_i$ are relatively prime. □

Proposition 10.1.13. *Let* A *be a ring and* $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ *ideals of* A. *Define a homomorphism*

$$\phi : A \to \prod_{i=1}^n (A/\mathfrak{a}_i), \quad \phi(x) = (x + \mathfrak{a}_1, \ldots, x + \mathfrak{a}_n).$$

(a) If $\mathfrak{a}_i, \mathfrak{a}_j$ *are coprime whenever* $i \neq j$, *then* $\prod_i \mathfrak{a}_i = \bigcap_i \mathfrak{b}_i$.

(b) ϕ *is surjective if and only if* $\mathfrak{a}_i, \mathfrak{b}_j$ *are coprime whenever* $i \neq j$.

(c) ϕ *is injective if and only if* $\bigcap_i \mathfrak{a}_i = (0)$.

Proof. First we prove (a). The case $n = 2$ is dealt with above. Suppose $n > 2$ and the result true for $\mathfrak{a}_1, \ldots, \mathfrak{a}_{n-1}$, and let $\mathfrak{b} = \mathfrak{a}_1 \cap \cdots \mathfrak{a}_{n-1}$. Since $\mathfrak{a}_i + \mathfrak{a}_j = (1)$ we have equations $x_i + y_i = 1$ ($x_i \in \mathfrak{a}_i, y_i \in \mathfrak{a}_n$) and therefore

$$\prod_{i=1}^{n-1} x_i = \prod_{i=1}^{n-1} (1 - y_i) \equiv 1 \mod \mathfrak{a}_n.$$

This means $\mathfrak{a}_n + \mathfrak{b} = (1)$. And so

$$\prod_{i=1}^{n} \mathfrak{a}_i = \mathfrak{b}\mathfrak{a}_n = \mathfrak{b} \cap \mathfrak{a}_n = \bigcap_{i=1}^{n} \mathfrak{a}_i.$$

Now we turn to part (b). First assume that ϕ is surjective. Let us show for example that $\mathfrak{a}_1, \mathfrak{a}_2$ are coprime. There exists $x \in A$ such that $\phi(x) = (1, 0, \ldots, 0)$; hence

$$x \equiv 1 \mod \mathfrak{a}_1 \quad \text{and} \quad x \equiv 0 \mod \mathfrak{a}_2,$$

so that $1 = (1 - x) + x \in \mathfrak{a}_1 + \mathfrak{a}_2$. The other case is done similarly.

Now suppose that $\mathfrak{a}_i$ and $\mathfrak{a}_j$ are coprime. It is enough to show, for example, that there is an element $x \in A$ such that $\phi(x) = (1, 0, \ldots, 0)$. Since $\mathfrak{a}_1 + \mathfrak{b}_i = (1)$ for $i > 1$, we have equations

$$u_i + v_i = 1, \quad u_i \in \mathfrak{a}_1, v_i \in \mathfrak{a}_i, i = 2, \ldots, n.$$

Take $x = \prod_{i=2}^{n} v_i$. then

$$x = \prod_{i=2}^{n} v_i = \prod_{i=2}^{n} (1 - u_i) = 1 \mod \mathfrak{a}_1.$$

Hence $\phi(x) = (1, 0, \ldots, 0)$. The other case is done similarly. □

Corollary 10.1.14 (Chinese remainder theorem). *Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be ideals of A such that $\mathfrak{a}_i + \mathfrak{b}_j = (1)$ for all $i \neq j$. Then the natural homomorphism*

$$\phi : A \to \prod_{i=1}^{n} (A/\mathfrak{a}_i)$$

is surjective and induces an isomorphism $\tilde{\phi} : A/\prod_{i=1}^{n} \mathfrak{a}_i \to \prod_{i=1}^{n} (A/\mathfrak{a}_i)$.

10.1.4 Local rings and semilocal rings

A ring A with exactly one maximal ideal $\mathfrak{m}$ is called a **local ring**. The field $k = A/\mathfrak{m}$ is called the residue field of A.

Proposition 10.1.15. *Let $A \neq 0$ be a ring. The following are equivalent:*

(a) A has a proper ideal $\mathfrak{m}$ and every element of $A - \mathfrak{m}$ is a unit.

(b) A is not the zero ring and for every $x \in A$ either x or $1 - x$ is invertible or both.

Proof. Let $\mathfrak{m} \neq (1)$ be an ideal. If every element of $A - \mathfrak{m}$ is a unit then $\mathfrak{m}$ is clearly maximal and every ideal of A is contained in $\mathfrak{m}$. Thus A is local. The converse is clear.

If A is local and x is not a unit. Then $x \in \mathfrak{m}$, and $1 - x$ must be a unit since otherwise $1 = 1 - x + x \in \mathfrak{m}$. Conversely, the condition in (b) holds, and $\mathfrak{m}_1$ and $\mathfrak{m}_2$ are distince maximal ideal of A. Then by the Chinese remained theorem we can choose $x \in A$ such that $x \equiv 0$ mod $\mathfrak{m}_1$ and $x \equiv 1$ mod $\mathfrak{m}_2$. Then x is not invertible and neither is $1 - x$ which is a contradiction. □

Lemma 10.1.16. *Let $\varphi : A \to B$ be a ring map. Assume A and B are local rings. The following are equivalent:*

(a) $\varphi(\mathfrak{m}_A) \subseteq \mathfrak{m}_B$.

(b) $\varphi^{-1}(\mathfrak{m}_B) = \mathfrak{m}_A$.

(c) For any $x \in A$, if $\varphi(x)$ is invertible in B, then x is invertible in A.

If φ satisfies these conditions, we say φ is a ***local homomorphism****.*

Proof. For $(a) \Rightarrow (b)$, the condition $\varphi(\mathfrak{m}_A) \subseteq \mathfrak{m}_B$ clearly implies $\mathfrak{m}_A \subseteq \varphi^{-1}(\varphi(A)) \subseteq \varphi^{-1}(\mathfrak{m}_B)$, hence $\mathfrak{m}_A = \varphi^{-1}(\mathfrak{m}_B)$.

For $(b) \Rightarrow (c)$, assume that $\varphi^{-1}(\mathfrak{m}_B) = \mathfrak{m}_A$. If $\varphi(x)$ is invertible, then $\varphi(x) \notin \mathfrak{m}_B$, so $x \notin \mathfrak{m}_A$. This implies that x is invertible. The implication $(c) \Rightarrow (a)$ is clear. □

Now we consider semilocal rings. They are characterized by the following proposition.

Proposition 10.1.17. *Let A be a ring. The following properties are equivalent:*

(a) The set of maximal ideals of A is finite.

(b) The quotient of A by its Jacobson radical is the direct product of a finite number of fields.

Proof. Suppose that the quotient of A by its Jacobson radical $\mathfrak{r}(A)$ is a direct product of a finite number of fields. Then $A/\mathfrak{r}(A)$ possesses only a finite number of ideals and a fortiori only a finite number of maximal ideals. As every maximal ideal contains $\mathfrak{r}(A)$, the maximal ideals of A are the inverse images of the maximal ideals of $A/\mathfrak{r}(A)$) under the canonical homomorphism $A \to A/\mathfrak{r}(A)$; hence they are finite in number.

Conversely, suppose that A has a finite number of distinct maximal ideals $\mathfrak{m}_1, \dots, \mathfrak{m}_n$. The $A/\mathfrak{m}_i$ are fields and it follows from Proposition 10.1.13 that the canonical mapping $A \to \prod_{i=1}^n A/\mathfrak{m}_i$ is surjective; as its kernel $\bigcap_{i=1}^n \mathfrak{m}_i$ is the Jacobson radical A. Thus $A/\mathfrak{r}(A)$ is isomorphic to $\prod_{i=1}^n A/\mathfrak{m}_i$. □

Every local ring is semilocal. Every quotient of a semilocal ring is semilocal. Every finite product of semi-local rings is semi-local. Another example, generalizing the construction of the local rings $A_\mathfrak{p}$, is provided by the following proposition:

Proposition 10.1.18. *Let A be a ring and $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ prime ideals of A. We write $S = \bigcap_{i=1}^n (A - \mathfrak{p}_i) = A - \bigcup_{i=1}^n \mathfrak{p}_i$.*

(a) The ring $S^{-1}A$ is semilocal; if $\mathfrak{q}_1, \dots, \mathfrak{q}_r$ are the distinct maximal elements (with respect to inclusion) of the set of $\mathfrak{p}_i$, the maximal ideals of $S^{-1}A$ are the $S^{-1}\mathfrak{q}_j$ and these ideals are distinct.

(b) The ring $A_{\mathfrak{p}_i}$ is canonically isomorphic to $(S^{-1}A)_{S^{-1}\mathfrak{p}_i}$.

(c) If A is an integral domain, then $S^{-1}A = \bigcap_{i=1}^n A_{\mathfrak{p}_i}$ in the field of fractions of A.

Proof. The ideals of A not meeting S are the ideals contained in the union of the $\mathfrak{p}_i$ and hence in at least one of the $\mathfrak{p}_i$ (by Proposition 10.1.4); the $\mathfrak{q}_i$ are therefore the maximal elements of the set of ideals not meeting S; consequently, the $S^{-1}\mathfrak{q}_i$ are the maximal ideals of $S^{-1}A$ by Proposition 10.2.36. Also, (b) follows from Corollary 10.2.22.

Suppose that A is an integral domain. If $\mathfrak{p}_i \subseteq \mathfrak{p}_j$ then $A_{\mathfrak{p}_i} \supseteq A_{\mathfrak{p}_j}$; to prove (c), we may therefore suppose that no two $\mathfrak{p}_i$ are comparable. Then it follows from (a) and Proposition 10.3.25 that $S^{-1}A = \bigcap_{i=1}^n (S^{-1}A)_{S^{-1}\mathfrak{p}_i}$; whence (c) in view of (b). □

Corollary 10.1.19. *Let A be an integral domain and $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ prime ideals of A, no two of which are comparable with respect to inclusion. If $A = \bigcap_{i=1}^n A_{\mathfrak{p}_i}$ in the field of fractions of A, then the maximal ideals of A are $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$.*

Proof. Setting $S = \bigcap_{i=1}^n (A - \mathfrak{p}_i)$. Then by Proposition 10.1.18 $S^{-1}A = A$; hence the elements of S are invertible in A and $S^{-1}\mathfrak{p}_i = \mathfrak{p}_i$ for all i. Our assertion then follows by virtue of Proposition 10.1.18(a). □

10.1.5 Operations on ideals

If $\mathfrak{a}, \mathfrak{b}$ are ideals in a ring A, their **ideal quotient** is

$$(\mathfrak{a} : \mathfrak{b}) = \{x \in A : x\mathfrak{b} \subseteq \mathfrak{a}\}$$

which is an ideal. In particular, $(0 : \mathfrak{b})$ is called the **annihilator** of $\mathfrak{b}$ and is also denoted by $\mathrm{Ann}(\mathfrak{b})$: it is the set of all $x \in A$ such that $x\mathfrak{b} = 0$. In this notation the set of all zero-divisors in A is

$$D = \bigcup_{x \neq 0} \mathrm{Ann}(x)$$

If $\mathfrak{b}$ is a principal ideal (x), we shall write $(\mathfrak{a} : x)$ in place of $(\mathfrak{a} : (x))$.

Example 10.1.20. If $A = \mathbb{Z}$, $\mathfrak{a} = (m)$, $\mathfrak{b} = (n)$, where $m = \prod_p p^{\mu_p}, \quad n = \prod_p p^{\nu_p}$, then $(\mathfrak{a} : \mathfrak{b}) = (q)$ where $q = \prod_p p^{\gamma_p}$ and

$$\gamma_p = \max(\mu_p - \nu_p, 0) = \mu_p - \min(\mu_p, \nu_p)$$

Hence $q = m/(m, n)$.

Proposition 10.1.21. *For ideals $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ of A, we have the following properties.*

(a) $\mathfrak{a} \subseteq (\mathfrak{a} : \mathfrak{b})$.

(b) $(\mathfrak{a} : \mathfrak{b})\mathfrak{b} \subseteq \mathfrak{a}$.

(c) $((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}) = (\mathfrak{a} : \mathfrak{b}\mathfrak{c}) = ((\mathfrak{a} : \mathfrak{c}) : \mathfrak{b})$.

(d) $(\bigcap_i \mathfrak{a}_i : \mathfrak{b}) = \bigcap_i (\mathfrak{a}_i : \mathfrak{b})$.

(e) $(\mathfrak{a} : \sum_i \mathfrak{b}_i) = \bigcap_i (\mathfrak{a} : \mathfrak{b}_i)$.

Proof. Part (a), (b) and (e) follow from the defnition. As for (c), we have

$$((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}) = \{x \in A : x\mathfrak{c} \subseteq (\mathfrak{a} : \mathfrak{b})\} = \{x \in A : x\mathfrak{c}\mathfrak{b} \subseteq \mathfrak{a}\} = (\mathfrak{a} : \mathfrak{c}\mathfrak{b}),$$

and the second equality holds since $\mathfrak{b}\mathfrak{c} = \mathfrak{c}\mathfrak{b}$.

Now we prove (d). If $x\mathfrak{b} \subseteq \bigcap_i \mathfrak{a}_i$, then it is contained in $(\mathfrak{a}_i, \mathfrak{b})$ for all i, hence $(\bigcap_i \mathfrak{a}_i : \mathfrak{b}) \subseteq \bigcap_i (\mathfrak{a}_i : \mathfrak{b})$. Conversely, if $x \in (\mathfrak{a}_i, \mathfrak{b})$ for all i, then $X\mathfrak{b} \subseteq \mathfrak{a}_i$, hence in $\bigcap_i \mathfrak{a}_i$. □

Now if $\mathfrak{a}$ is any ideal of A, the **radical** of $\mathfrak{a}$ is defined to be

$$\sqrt{\mathfrak{a}} = \{x \in A : x^n \in \mathfrak{a} \text{ for some } n > 0\}.$$

If $\phi : A \to A/\mathfrak{a}$ is the standard homomorphism, then $\sqrt{\mathfrak{a}} = \phi^{-1}(\mathfrak{n}(A/\mathfrak{a}))$ and hence $\sqrt{\mathfrak{a}}$ is an ideal. Moreover, according to Proposition 10.1.7, we see the radical of an idea $\mathfrak{a}$ is the intersection of the prime ideals which contain $\mathfrak{a}$:

$$\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{p} \supseteq \mathfrak{a}} \mathfrak{p}.$$

Example 10.1.22. If $A = \mathbb{Z}$, $\mathfrak{a} = (m)$, let p_i $(1 \leq i \leq r)$ be the distinct prime divisors of m. Then $\sqrt{\mathfrak{a}} = (p_1 \cdots p_r) = \bigcap_i (p_i)$.

Proposition 10.1.23. *Let $\mathfrak{a}, \mathfrak{b}$ be ideals of A. Prove the following*

(a) $\mathfrak{a} \subseteq \sqrt{\mathfrak{a}}$.

(b) $\sqrt{\sqrt{\mathfrak{a}}} = \sqrt{\mathfrak{a}}$.

(c) $\sqrt{\mathfrak{a}\mathfrak{b}} = \sqrt{\mathfrak{a} \cap \mathfrak{b}} = \sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}}$.

(d) $\sqrt{\mathfrak{a}} = (1)$ *if and only if* $\mathfrak{a} = (1)$.

(e) $\sqrt{\mathfrak{a} + \mathfrak{b}} = \sqrt{\sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}}}$.

(f) If $\mathfrak{p}$ is prime, $\sqrt{\mathfrak{p}^n} = \mathfrak{p}$ for all $n > 0$.

Proof. Part (a), (d) are clear, and (b) holds since

$$x^n \in \sqrt{\mathfrak{a}} \Rightarrow (x^n)^m \in \mathfrak{a} \Rightarrow x^{nm} \in \mathfrak{a}.$$

For (c), since $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$, we have $\sqrt{\mathfrak{a}\mathfrak{b}} \subseteq \sqrt{\mathfrak{a} \cap \mathfrak{b}}$. Conversely, if $x \in \sqrt{\mathfrak{a} \cap \mathfrak{b}}$, then $x^n \in \mathfrak{a} \cap \mathfrak{b}$ for some $n > 0$. This means $x^n \in \mathfrak{a}$ and $x^n \in \mathfrak{b}$, hence $x^{2n} = x^n \cdot x^n \subseteq \mathfrak{a}\mathfrak{b}$, which means $x \in \sqrt{\mathfrak{a}\mathfrak{b}}$.

The argument above also gives $x \in \sqrt{\mathfrak{a}}$ and $x \in \sqrt{\mathfrak{b}}$, hence $\sqrt{\mathfrak{a} \cap \mathfrak{b}} \subseteq \sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}}$. The other direction is also easy to verify.

Now we prove (e). Since $\mathfrak{a} + \mathfrak{b} \subseteq \sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}}$, we have $\sqrt{\mathfrak{a} + \mathfrak{b}} \subseteq \sqrt{\sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}}}$. Now assume that $x^n \in \sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}}$, then $x^n = m + n$ for $m^a \in \mathfrak{a}$ and $n^b \in \mathfrak{b}$. Then

$$(x^n)^{a+b} = (m+n)^{a+b} = \sum_{i=0}^{a+b} \binom{a+b}{i} m^i n^{a+b-i}$$

It is clear that the terms of the sum either belongs to $\mathfrak{a}$ or $\mathfrak{b}$. Hence this sum belongs to $\mathfrak{a} + \mathfrak{b}$. So $x \in \sqrt{\mathfrak{a} + \mathfrak{b}}$.

For (f), since $\mathfrak{p}^n \subseteq \mathfrak{p}$, we have $\sqrt{\mathfrak{p}^n} \subseteq \sqrt{\mathfrak{p}}$. But since $\mathfrak{p}$ is prime, we have $\sqrt{\mathfrak{p}} = \mathfrak{p}$, and therefore $\sqrt{\mathfrak{p}^n} \subseteq \mathfrak{p}$. Conversely, if $x \in \mathfrak{p}$, then $x^n \in \mathfrak{p}^n$, and therefore $x \in \sqrt{\mathfrak{p}^n}$. These together prove (f). □

Proposition 10.1.24. *Let $\mathfrak{a}, \mathfrak{b}$ be ideals in a ring A such that $\sqrt{\mathfrak{a}}, \sqrt{\mathfrak{b}}$ are coprime. Then $\mathfrak{a}, \mathfrak{b}$ are coprime.*

Proof. we have

$$\sqrt{\mathfrak{a} + \mathfrak{b}} = \sqrt{\sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}}} = \sqrt{(1)} = (1)$$

hence $\mathfrak{a} + \mathfrak{b} = (1)$, by Proposition 10.1.23. □

Let $\rho : A \to B$ be a ring homomorphism. If $\mathfrak{a}$ is an ideal in A, the set $\rho(\mathfrak{a})$ is not necessarily an ideal in B (e.g., let ρ be the embedding of $\mathbb{Z}$ in $\mathbb{Q}$, the field of rationals, and take $\mathfrak{a}$ to be any non-zero ideal in $\mathbb{Z}$.). We define the **extension** $\mathfrak{a}^e$ of $\mathfrak{a}$ to be the ideal generated by $\rho(\mathfrak{a})$ in B: explicitly,

$$\mathfrak{a}^e = \Big\{ \sum y_i \rho(x_i) : x_i \in \mathfrak{a}, y_i \in B \Big\}$$

If $\mathfrak{b}$ is an ideal of B, then $\rho^{-1}(\mathfrak{b})$ is always an ideal of A, called the **contraction** $\mathfrak{b}^c$ of $\mathfrak{b}$. If $\mathfrak{b}$ is prime, $\mathfrak{b}^c$ is prime. If $\mathfrak{a}$ is prime, $\mathfrak{a}^e$ need not to be prime: For example, if $\rho : \mathbb{Z} \to \mathbb{Q}$ is the inclusion and $\mathfrak{p}$ is any nonzero prime ideal of $\mathbb{Z}$, then $\mathfrak{p}^e = \mathbb{Q}$ is not prime.

We can factorize ρ as follows:

$$A \xrightarrow{\tilde{\rho}} \rho(B) \xrightarrow{j} B$$

where $\tilde{\rho}$ is surjective and j is injective. For ρ the situation is very simple: there is a one-to-one correspondence between ideals of $\rho(A)$ and ideals of A which contain $\ker f$, and prime ideals correspond to prime ideals. For j, on the other hand, the general situation is very complicated. The classical example is from algebraic number theory.

Example 10.1.25. Consider $\mathbb{Z} \to \mathbb{Z}[i]$, where $i = \sqrt{-1}$. A prime ideal (p) of $\mathbb{Z}$ may or may not stay prime when extended to $\mathbb{Z}[i]$. In fact $\mathbb{Z}[i]$ is a principal ideal domain (because it has a Euclidean algorithm) and the situation is as follows:

(a) $(2)^e = ((1+i)^2)$, the square of a prime ideal in $\mathbb{Z}[i]$.

(b) If $p \equiv 1 \bmod 4$ then $(p)^e$ is the product of two distinct prime ideals.

(c) If $p \equiv 3 \bmod 4$ then $(p)^e$ is prime in $\mathbb{Z}[i]$.

In fact the behavior of prime ideals under extensions of this sort is one of the central problems of algebraic number theory.

Proposition 10.1.26. *Let $\rho : A \to B$, $\mathfrak{a}$ and $\mathfrak{b}$ be as before. Then*

(a) $\mathfrak{a} \subseteq \mathfrak{a}^{ec}$, $\mathfrak{b} \supseteq \mathfrak{b}^{ce}$.

(b) $\mathfrak{b}^c = \mathfrak{b}^{cec}$, $\mathfrak{a}^e = \mathfrak{a}^{ece}$.

(c) If C is the set of contracted ideals in A and if E is the set of extended ideals in B, then

$$C = \{\mathfrak{a} \mid \mathfrak{a}^{ec} = \mathfrak{a}\}, \quad E = \{\mathfrak{b} \mid \mathfrak{b}^{ce} = \mathfrak{b}\},$$

and $\mathfrak{a} \mapsto \mathfrak{a}^e$ is a bijective map of C onto E, whose inverse is $\mathfrak{b} \mapsto \mathfrak{b}^c$.

Proof. The first part is clear, and (b) follows from (a):

$$\mathfrak{b}^c \subseteq (\mathfrak{b}^c)^{ec} = \mathfrak{b}^{cec} \quad \text{and} \quad \mathfrak{b} \supseteq \mathfrak{b}^{ce} \Rightarrow \mathfrak{b}^c \supseteq \mathfrak{b}^{cec}$$

Hence $\mathfrak{b}^c = \mathfrak{b}^{cec}$. Also, part (c) is a concequence of part (b). □

Proposition 10.1.27. *If $\mathfrak{a}_1, \mathfrak{a}_2$ are ideals of A and if $\mathfrak{b}_1, \mathfrak{b}_2$ are ideals of S, then we have*

(a) $(\mathfrak{a}_1 + \mathfrak{a}_2)^e = \mathfrak{a}_1^e + \mathfrak{a}_2^e$ *and* $(\mathfrak{b}_1 + \mathfrak{b}_2)^c \supseteq \mathfrak{b}_1^c + \mathfrak{b}_2^c$.

(b) $(\mathfrak{a}_1 \cap \mathfrak{a}_2)^e \subseteq \mathfrak{a}_1^e \cap \mathfrak{a}_2^e$ *and* $(\mathfrak{b}_1 \cap \mathfrak{b}_2)^c = \mathfrak{b}_1^c \cap \mathfrak{b}_2^c$.

(c) $(\mathfrak{a}_1\mathfrak{a}_2)^e = \mathfrak{a}_1^e\mathfrak{a}_2^e$ *and* $(\mathfrak{b}_1\mathfrak{b}_2)^c \supseteq \mathfrak{b}_1^c\mathfrak{b}_2^c$.

(d) $(\mathfrak{a}_1 : \mathfrak{a}_2)^e \subseteq (\mathfrak{a}_1^e : \mathfrak{a}_2^e)$ *and* $(\mathfrak{b}_1 : \mathfrak{b}_2)^c \subseteq (\mathfrak{b}_1^c : \mathfrak{b}_2^c)$.

(e) $(\sqrt{\mathfrak{a}})^e \subseteq \sqrt{\mathfrak{a}^e}$ *and* $(\sqrt{\mathfrak{b}})^c = \sqrt{\mathfrak{b}^c}$.

Therefore, the set of ideals E is closed under sum and product, and C is closed under intersection and radical.

Proof. Note that the extension and contraction preserve inclusions. Since f is a ring homomorphism, part (a), (b), and (c) are easy to see. We first show part (d). If $x \in (\mathfrak{a}_1 : \mathfrak{a}_2)^e$, then $x = \sum y_i f(x_i)$ for $x_i \in (\mathfrak{a}_1 : \mathfrak{a}_2)$. Pick one term $y_i f(x_i)$, since $x_i\mathfrak{a}_2 \subseteq \mathfrak{a}_1$, we have $f(x_i)f(\mathfrak{a}_2) \subseteq f(\mathfrak{a}_1)$. So we have $y_i f(x_i) \in (\mathfrak{a}_1^e : \mathfrak{a}_2^e)$ and then $x \in (\mathfrak{a}_1^e : \mathfrak{a}_2^e)$. This gives $(\mathfrak{a}_1 : \mathfrak{a}_2)^e \subseteq (\mathfrak{a}_1^e : \mathfrak{a}_2^e)$. Similarly, if $x \in (\mathfrak{b}_1 : \mathfrak{b}_2)^c$, then $f(x)\mathfrak{b}_2 \subseteq \mathfrak{b}_1$. So $f(x\mathfrak{b}_2^c) \subseteq f(x)\mathfrak{b}_2 \subseteq \mathfrak{b}_1$. This shows $x\mathfrak{b}_2^c \subseteq \mathfrak{b}_1^c$, hence $(\mathfrak{b}_1 : \mathfrak{b}_2)^c \subseteq (\mathfrak{b}_1^c : \mathfrak{b}_2^c)$.

We turn to part (e). If $x = \sum y_i f(x_i)$ for $x_i^{n_i} \in \mathfrak{a}$. Then

$$(y_i f(x_i))^{n_i} = y_i^n f(x_i^{n_i}) \in \mathfrak{a}^e.$$

Since x is a finite sum, we get $x^N \in \mathfrak{a}^e$ for some N. Hence $x \in \sqrt{\mathfrak{a}^e}$, which shows $(\sqrt{\mathfrak{a}})^e \subseteq \sqrt{\mathfrak{a}^e}$. Finally, if $f(x) \in \sqrt{\mathfrak{b}}$, then $(f(x))^n = f(x^n) \in \mathfrak{b}$, so $x \in \sqrt{\mathfrak{b}^c}$. So $(\sqrt{\mathfrak{b}})^c \subseteq \sqrt{\mathfrak{b}^c}$. Conversely, if $x^n \in \mathfrak{b}^c$, then $f(x^n) = (f(x))^n \in \mathfrak{b}$. Hence $f(x) \in \sqrt{\mathfrak{b}}$, $x \in (\sqrt{\mathfrak{b}})^c$. □

10.1.6 Exercise

Exercise 10.1.1. Let x be a nilpotent element of a ring A. Show that $1 + x$ is a unit of A. Deduce that the sum of a nilpotent element and a unit is a unit.

Proof. Assume $x^n = 1$ for $n > 0$, then consider the polynomials

$$1 + x^n, \quad 1 - x^n$$

Either of them has a root -1: $1 + x^n$ for n odd, $1 - x^n$ for n even. Then we can insert x to get a decomposition of 1 since $x^n = 0$. Hence $1 + x$ is a unit.

For $u+x$ with u a unit, since there is $t \in A$ such that $ur = 1$, we have $r(u+x) = ur+xr = 1+xr$. Since $(xr)^n = 0$, $1 + xr$ is a unit. Then $u + x$ is also a unit. □

Exercise 10.1.2. Let A be a ring and let $A[X]$ be the ring of polynomials in an indeterminate X, with coefficients in A. Let $f = a_0 + a_1X + \cdots + a_nX^n \in A[X]$. Prove that

(a) f is a unit in $A[X]$ if and only if a_0 is a unit in A and $a_1, \ldots, a_n$ are nilpotent.

(b) f is nilpotent if and only if $a_0, a_1, \ldots, a_n$ are nilpotent.

(c) f is a zero-divisor if and only if there exists $a \neq 0$ in A such that $af = 0$.

(d) f is said to be primitive if $(a_0, a_1, \ldots, a_n) = (1)$. Prove that if $f, g \in A[X]$, then fg is primitive if and only if f and g are primitive.

These results can be generized to a polynomial ring $A[X_1, \ldots, X_r]$ in several indeterminates.

Proof. Let f be a unit in $A[X]$. Then for any prime ideal $\mathfrak{p}$ of A, the image $\bar{f}$ in $(A/\mathfrak{p})[X]$ is also a unit. Since $A/\mathfrak{p}$ is an integral domain, this implies $\deg(\bar{f}) = 0$, hence $a_1, \dots, a_n \in \mathfrak{p}$ and $a_0 \notin \mathfrak{p}$. Since this holds for any prime ideal of A, it follows that a_0 is a unit and $a_1, \dots, a_n \in \bigcap \mathfrak{p} = \mathfrak{n}(A)$. That is, $a_1, \dots, a_n$ are nilpotents. Conversely, if a_0 is a unit, then f has an inverse g in $A[[X]]$. If in addition $a_1, \dots, a_n$ are nilpotent, this inverse g is in $A[X]$, hence f is a unit in $A[X]$.

Similarly, if f is nilpotent then it image in $(A/\mathfrak{p})[X]$ is nilpotent for any prime ideal $\mathfrak{p}$, hence is zero. This implies $a_0, \dots, a_n \in \mathfrak{n}(A)$, so they are nilpotent. The converse can be proved similarly.

Let $g(X) = b_0 + b_1X + \cdots + b_mX^m$ be such that $fg = 0$ and $g \neq 0$. If $f = 0$ then the claim follows, so we may assume that f is nonzero and in particular that $a_n \neq 0$. Then $a_nb_m = 0$ follows immediately. Note that $f \cdot (a_ng)$ is also zero, so by replacing g with a_ng we elimate the degree of g by 1. This argument always holds except $\deg g = 0$, so there is $a \in A, a \neq 0$ such that $af = 0$. The converse is trivial.

Note that a polynomial is primitive just if no maximal ideal contains all its coefficients. Let $\mathfrak{m} \subseteq A$ be maximal. Since $A/\mathfrak{m}$ is a field, $A[X]/\mathfrak{m}[X] = (A/\mathfrak{m})[X]$ is an integral domain. Thus

$$f, g \notin \mathfrak{m}[X] \iff \bar{f}, \bar{g} \neq 0 \text{ in } (A/\mathfrak{m})[X] \iff \overline{fg} \neq 0 \text{ in } (A/\mathfrak{m})[X] \iff fg \notin \mathfrak{m}[X]$$

Therefore no maximal ideal contains all the coefficients of fg just if the same holds for f and g. □

Exercise 10.1.3. In the ring $A[X]$, the Jacobson radical is equal to the nilradical.

Proof. Since maximal ideal is prime, $\mathfrak{n}(A) \subseteq \mathfrak{r}(A)$ holds for all ring A. Now assume $f(x) = a_0 + a_1X + \cdots + a_nX^n$ is in $J(A[X])$, then $1 + f(X)g(X)$ is a unit for any $g(X) \in A[X]$. In particular, $1 + f(X)$ is a unit, then by Exercise 10.1.2, a_i are nilpotent for $i \geq 1$. Let $g(X) = 1 + X$, we obtain $a_0 + a_1$ is nilpotent (because it is the coefficient of X in $1 + fg$), hence a_0 is nilpotent. Agian by Exercise 10.1.2, $f(X)$ is nilpotent. □

Exercise 10.1.4. Let A be a ring and let $A[[X]]$ be the ring of formal power series with coefficients in A. Show that

(a) f is a unit in $A[[X]]$ if and only if a_0 is a unit in A.

(b) If f is nilpotent, then a_n is nilpotent for all $n \geq 0$. Is the converse true?

(c) f belongs to the Jacobson radical of $A[[X]]$ if and only if a_0 belongs to the Jacobson radical of A.

(d) The contraction of a maximal ideal $\mathfrak{m}$ of $A[[X]]$ is a maximal ideal of A, and $\mathfrak{m}$ is generated by $\mathfrak{m}^c$ and X.

(e) Every prime ideal of A is the contraction of a prime ideal of $A[[X]]$.

Proof. If f is a unit, then a_0 is a unit. If a_0 is a unit, consider the expansion

$$\frac{1}{1 + a_0^{-1}X} \sum_{n=0}^{\infty} (-a_0^{-1}X)^n$$

Plug into $X = f - a_0$, we get an inverse of $1 + a_0^{-1}(f - a_0) = a_0^{-1}f$, hence $a_0^{-1}f$ is a unit, so is f.

If f is nilpotent, then a_0 is nilpotent, and $f - a_0$ is nilpotent. By repeting this we can show a_n are all nilpotent.

To see that the converse fails, let Y_n be a collection of indeterminates over $\mathbb{Z}$, indexed by the natural numbers. Let

$$A = \mathbb{Z}[Y_1, Y_2, \cdots]/(Y_1, Y_2^2, Y_3^3, \cdots)$$

Let

$$f(X) = \sum_n Y_n X^n \in A[[X]]$$

Then $a_n = Y_n$ is nilpotent for all n, but there is no N such that $f^N = 0$ (this would establish some non-trivial relation amongst the Y_n for $n > N$ other than $Y_n^n = 0$).

$f \in J(A[[X]])$ if and only if $1 + fg$ is a unit for all $g \in A[[X]]$. Since for $g = \sum b_n X^n$, the contant term of $1 + fg$ is $1 + a_0 b_0$, the condition is equivalent to that $1 + a_0 b_0$ is a unit for all b_0, and hence to $a_0 \in \mathfrak{r}(A)$.

Since x has constant term $0 \in \mathfrak{r}(A)$ in $A[[X]]$, by (c) above we get $X \in J(A[[X]])$, and hence $(X) \subseteq J(A[[X]])$. As $\mathfrak{m} - (X) = \mathfrak{m}^c$, we get $\mathfrak{m} = \mathfrak{m}^c + (X)$. Now $A/\mathfrak{m}^c \cong A[[X]]/\mathfrak{m}$ is a field, so $\mathfrak{m}^c$ is maximal.

To see $I = I^{ec}$, we only need to verify I^e is prime when I is prime. Let $f, g \in A[[X]]$ with contant term a_0, b_0. If $f, g \notin \mathfrak{p}^e$, then $a_0, b_0 \notin \mathfrak{p}$. Since fg has contant term $a_0 b_0$, which is not in $\mathfrak{p}$, $fg \notin \mathfrak{p}^e$. So $\mathfrak{p}^e$ is prime. □

Exercise 10.1.5. Let A be a ring, $\mathfrak{n}(A)$ its nilradical. Show that the following are equivalent:

(a) A has exactly one prime ideal.

(b) Every element of A is either a unit or nilpotent.

(c) $A/\mathfrak{n}(A)$ is a field.

Proof. Assume A has exactly one prime ideal $\mathfrak{p}$. Suppose $x \in A$ is not a unit, then $x \in \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. Since $\mathfrak{m}$ is also prime, we must have $\mathfrak{m} = \mathfrak{p}$. Hence $x \in \mathfrak{p}$. Since we also have $\mathfrak{n}(A) = \mathfrak{p}$, x is nilpotent.

Since $\mathfrak{n}(A)$ contains all nilpotent elements, $A - \mathfrak{n}(A)$ contains only units. Then every elements in $A/\mathfrak{n}(A)$ is a unit, so $A/\mathfrak{n}(A)$ is a field.

If $A/\mathfrak{n}(A)$ is a field, then $A - \mathfrak{n}(A)$ contains only units. Let $\mathfrak{p}$ be a prime ideal in A, then $\mathfrak{p} \in n(A)$ since it contains no units, and then $\mathfrak{n}(A) = \mathfrak{p}$ since $\mathfrak{n}(A) \subseteq \mathfrak{p}$. So A contains only one prime ideal $\mathfrak{n}(A)$. □

Proof. Let $x \in A$ be idempotent, and let $\mathfrak{m}$ be the unique maximal ideal. Then in $A/\mathfrak{m}$ we see

$$\bar{x}(1 - \bar{x}) = 0$$

so $\bar{x} = 0$ or $\bar{x} = 1$, which means $x \in \mathfrak{m}$ or $x \in 1 + \mathfrak{m}$. Since $\mathfrak{m} = \mathfrak{r}(A)$, if $x \in \mathfrak{m}$ then $1 - x$ is a unit, and if $x \in 1 + \mathfrak{m}$ then x is a unit. Since $x(1 - x) = 0$, in the former case $x = 0$, and in the latter case $x = 1$. □

Exercise 10.1.6. In a ring A, let Σ be the set of all ideals in which every element is a zero-divisor. Show that the set Σ has maximal elements and that every maximal element of Σ is a prime ideal. Hence the set of zero-divisors in A is a union of prime ideals.

Proof. Clearly $(0) \in \Sigma$, so Σ is non-empty. Let $(I_i)_{i \in I}$ be a chain in Σ. The union a of the chain is still an ideal, and consists only of zero-divisors. Thus Σ, so by Zorn's Lemma Σ has maximal elements.

Let I be a maximal element of Σ, and suppose that $xy \in I$ with $y \notin I$. Then $I \subsetneq (I, a)$ so y is not a zero-divisor by the maximality of I. But xy is a zero-divisor, so there exists some $z \in A, z \neq 0$ such that $zxy = 0$. As y is not a zero-divisor we must have that $xz = 0$, so that x is a zero-divisor and thus is contained in I. □

10.2 Rings and modules of fractions

10.2.1 Definition of rings of fractions

Definition 10.2.1. *A subset S of a commutative ring A is a* ***multiplicative subset*** *(or* ***multiplicatively closed****) if*

- $1 \in S$.
- *if $s, t \in S$ then $st \in S$.*

In other words, S is a subsemigroup of the multiplicative semigroup of A.

Example 10.2.2 (Example of multiplicative subsets).

(a) For every $a \in A$, the set of a^n, where $n \in \mathbb{N}$, is a multiplicative subset of A.

(b) Let A be a ring and $\mathfrak{a}$ an ideal of A, then $1 + \mathfrak{a}$ is multiplicative closed.

(c) Let $\mathfrak{p}$ be an ideal of A. For $A - \mathfrak{p}$ to be a multiplicative subset of A, it is necessary and sufficient that $\mathfrak{p}$ be prime.

(d) The set of elements of A which are not divisors of zero is a multiplicative subset of A.

(e) If S and T are multiplicative subsets of A, the set ST of products st, where $s \in S$ and $t \in T$, is a multiplicative subset.

(f) Let $\mathcal{S}$ be a directed set (with respect to inclusion) of multiplicative subsets of A. Then $T = \bigcup_{S \in \mathcal{S}} S$ is a multiplicative subset of A, as any two elements of T belong to some subset $S \in \mathcal{S}$, hence their product belongs to T.

Proposition 10.2.3. *Let A be a ring, S a multiplicative subset, and $\mathfrak{a}$ an ideal with $\mathfrak{a} \cap S = \varnothing$. Set $\mathcal{S} := \{$ideals $\mathfrak{b} \mid \mathfrak{b} \supseteq \mathfrak{a}$ and $\mathfrak{b} \cap S = \varnothing\}$. Then $\mathcal{S}$ has a maximal element $\mathfrak{p}$, and every such $\mathfrak{p}$ is prime.*

Proof. By Zorn's lemma, similar to Proposition 10.1.7. □

For every subset S of a ring A, there exist multiplicative subsets of A containing S, for example A itself. The intersection of all these subsets is the smallest multiplicative subset of A containing S; it is said to be **generated** by S. It follows immediately that it is the set consisting of all the finite products of elements of S.

Proposition 10.2.4. *Let A be a ring and S a subset of A. There exists a ring $\tilde{A}$ and a homomorphism $i : A \to \tilde{A}$ with the following properties:*

(a) *the elements of $i(S)$ are invertible in $\tilde{A}$;*

(b) *for every homomorphism f of A to a ring B such that the elements of $f(S)$ are invertible in B, there exists a unique homomorphism $\tilde{f} : \tilde{A} \to B$ such that $f = \tilde{f} \circ i$.*

Proof. Define a relation on the set of pairs $A \times S$ as follows:

$$(a, s) \sim (a', s') \iff (\exists t \in S)\, t(s'a - sa') = 0 \tag{2.1.1}$$

Now we denote by a/s the equivalence class of (a, s), and define the operations $+, \cdot$ on such fractions as

$$\frac{a}{s} + \frac{a'}{s'} = \frac{as' + a's}{ss'}, \quad \frac{a}{s} \cdot \frac{a'}{s'} = \frac{aa'}{ss'}.$$

The set $S^{-1}A$ of fractions, endowed with the operations $+, \cdot$, is a commutative ring and the function $a \mapsto a/1$ defines a ring homomorphism $i_A^S : A \to S^{-1}A$. It is now clear that $i(s)$ is invertible for any $s \in S$. If $\rho : A \to B$ is a homomorphism such that $f(S)$ are invertible, then the map $\tilde{\rho} : S^{-1}A \to B$ defined by $\tilde{f}(a/s) = f(a)f(s)^{-1}$ is well-defined and clearly satisfies the requirement. □

Let A be a ring, S a subset of A and $\bar{S}$ the multiplicative subset generated by S. The ring of fractions of A defined by $\bar{S}$ and denoted by $S^{-1}A$ is the quotient set of $A \times \bar{S}$ under the equivalence relation (2.1.1) with the ring structure dfined by

$$a/s + b/t = (ta + bs)/st, \quad (a/s)(b/t) = ab/st.$$

for $a, b \in A$ and $s, t \in \bar{S}$. The canonical map i_A^S of A to $S^{-1}A$ is the homomorphism $a \mapsto a/1$, which makes $S^{-1}A$ into an A-algebra.

Corollary 10.2.5. *If $\rho : A \to B$ is a ring homomorphism such that*

(a) *$\rho(S)$ is invertible in B.*

(b) *$\rho(a) = 0$ if and only if $as = 0$ for some $s \in S$.*

(c) *Every element of B is of the form $\rho(a)\rho(s)^{-1}$.*

Then there is a unique isomorphism $h : S^{-1}A \to B$ such that $\rho = h \circ i$.

Proof. We only have to show that $h : S^{-1}A \to B$, defined by

$$h(a/s) = \rho(a)\rho(s)^{-1}$$

is an isomorphism. By (c), his surjective. To show h is injective, look at the kernel of h: if $h(a/s) = 0$, then $\rho(a) = 0$, hence by (b) we have $as = 0$ for some $s \in S$, hence $(a, s) = (0, 1)$, i.e., $a/s = 0$ in $S^{-1}A$. □

Example 10.2.6 (Example of localizations).

(a) Let A be a commutative ring, and let $\mathfrak{p}$ be a prime ideal of A. Then the set $S = A - \mathfrak{p}$ is multiplicatively closed. The localizations $S^{-1}A$, $S^{-1}M$ are then denoted $A_\mathfrak{p}$, $M_\mathfrak{p}$. The process of passing from A to $A_\mathfrak{p}$ is called **localization at** $\mathfrak{p}$.

(b) Let $f \in A$ and let $S = \{f^n\}$, we write A_f for $S^{-1}A$ in this case.

(c) Let $A = \mathbb{Z}$, $\mathfrak{p} = (p)$ where p a prime number. Then $\mathbb{Z}_\mathfrak{p}$ is set of all rational numbers m/n where n is prime to p; if $f \in \mathbb{Z}$ and $f \neq 0$, then $\mathbb{Z}_f$ is the set of all rational numbers whose denominator is a power of f.

(d) Let $A = k[X_1, \dots, X_n]$, where k is a field and the X_i are independent indeterminates, $\mathfrak{p}$ a prime ideal in A. Then $A_\mathfrak{p}$ is the ring of all rational functions f/g, where $g \notin \mathfrak{p}$. If V is the variety defined by the ideal $\mathfrak{p}$, that is to say the set of all $x = (x_1, \dots, x_n) \in k^n$ such that $f(x) = 0$ whenever $f \in \mathfrak{p}$, then (provided k is infinite) $A_\mathfrak{p}$ can be identified with the ring of all rational functions on k^n which are defined at almost all points of V; it is the local ring of k^n **along the variety** V. This is the prototype of the local rings which arise in algebraic geometry.

Proposition 10.2.7. *Let A, B be two rings, S a subset of A, T a subset of B and $\rho : A \to B$ a homomorphism such that $\rho(S) \subseteq T$. There exists a unique homomorphism $\tilde{\rho}$ from S^{-1} to $T^{-1}B$ such that $\tilde{\rho}(a/1) = \rho(a)/1$ for all $a \in A$.*

Suppose further that T is contained in the multiplicative subset of B generated by $\rho(S)$. Then, if ρ is surjective (resp. injective) so is $\tilde{\rho}$.

Proof. The first assertion amounts to saying that there exists a unique homomorphism $\tilde{\rho} : S^{-1}A \to T^{-1}B$ giving a commutative diagram:

$$\begin{tikzcd} A \arrow[r, "\rho"] \arrow[d, "i_A^S"'] & B \arrow[d, "i_B^T"] \\ S^{-1}A \arrow[r, "\tilde{\rho}"] & T^{-1}B \end{tikzcd}$$

Now the relation $\rho(S) \subseteq T$ implies that $i_B^T(\rho(S))$ is invertible in $T^{-1}B$ for all $s \in S$ and it is sufficient to apply Proposition 10.2.4 to $i_B^T \circ \rho$. It follows easily from the definition that, for all $a \in A$ and $s \in \bar{S}$ (multiplicative subset of A generated by S),

$$\tilde{\rho}(a/s) = \rho(a)/\rho(s)$$

Suppose that T is contained in the multiplicative subset generated by $\rho(S)$, which is precisely $\rho(\bar{S})$. Then it follows from the formula above that, if ρ is surjective, so is $\tilde{\rho}$. Suppose now that ρ is injective. Let a/s be an element of the kernel of $\tilde{\rho}$. As the multiplicative subset generated by T is $\rho(\bar{S})$, there is an element $s_1 \in S$ such that $\rho(s_1)\rho(a) = 0$, whence $\rho(s_1 a) = 0$ and consequently $s_1 a = 0$ since ρ is injective; then $a/s = 0$, which proves that $\tilde{\rho}$ is injective. □

Corollary 10.2.8. *Let A be a ring, S a subset of A and ρ an injective homomorphism from A to a ring B such that the elements of $\rho(S)$ are invertible in B. The unique homomorphism $\tilde{\rho} : S^{-1}A \to B$ such that $\rho = \tilde{\rho} \circ i_A^S$ is then injective.*

Corollary 10.2.9. *Let A be a ring and S, T two subsets of A such that $S \subseteq T$. Then there exists a unique homomorphism $i_A^{T,S} : S^{-1}A \to T^{-1}A$ such that $i_A^T = i_A^{T,S} \circ i_A^S$.*

Proof. For all $a \in A$, $i_A^{T,S}$ then maps the element a/s in $S^{-1}A$ to the element a/s in $T^{-1}A$. □

Corollary 10.2.10. *Let A, B, C be three rings, S (resp. T, U) a multiplicative subset of A (resp. B, C), $\rho : A \to B$, $\nu : B \to C$ two homomorphism and $\eta = \nu \circ \rho$ the composite homomorphism. Suppose that $\rho(S) \subseteq T$ and $\nu(T) \subseteq U$. Let $\tilde{\rho} : S^{-1}A \to T^{-1}B$, $\tilde{\nu} : T^{-1}B \to U^{-1}C$, and $\tilde{\eta} : S^{-1}A \to U^{-1}C$ be the induced homomorphisms. Then $\tilde{\eta} = \tilde{\nu} \circ \tilde{\rho}$.*

In particular, if S, T, U are three multiplicative subsets of A such that $S \subseteq T \subseteq U$, then $i_A^{U,S} = i_A^{U,T} \circ i_A^{T,S}$.

Corollary 10.2.11. *Let S be a subset of a ring A, B a subring of $S^{-1}A$ containing the set $T := i_A^S(A)$. Let $j : B \to S^{-1}A$ be the canonical injection, then the unique homomorphism $\eta : T^{-1}B \to S^{-1}A$ such that $\eta \circ i_A^S = j$ is an isomorphism.*

Proof. The mapping η is injective by Corollary 10.2.8. The ring $\eta(T^{-1}B)$ contains T and the inverse of the elements of T. Hence it is equal to $S^{-1}A$. □

10.2.2 Modules of fractions

The canonical homomorphism $i_A^S : A \to S^{-1}A$ allows us to consider every $S^{-1}A$-module as an A-module.

Proposition 10.2.12. *Let A be a ring, S a subset of A, M an A-module and $\tilde{M}$ the A-module $M \otimes_A S^{-1}A$. If i_M^S is the canonical A-homomorphism $x \mapsto x \otimes 1$ of M to $\tilde{M}$, then:*

(a) For all $s \in S$, the homothety $z \mapsto sz$ of M' is bijective.

(b) For every A-module N such that, for all $s \in S$, the homothety $z \mapsto sz$ of N is bijective, and every homomorphism $\phi : M \to N$, there exists a unique homomorphism $\tilde{\phi} : \tilde{M} \to N$ such that $\phi = \tilde{\phi} \circ i_M^S$.

Proof. For every A-module N and all $a \in A$, denote by h_a the homothety $y \mapsto ay$ in N. Then $a \mapsto h_a$ is a ring homomorphism from A to $\mathrm{End}_A(N)$ To say that h_a is bijective means that h_a is an invertible element of $\mathrm{End}_A(N)$. Suppose that, for all $s \in S$, h_s is invertible in $\mathrm{End}_A(N)$. The elements h_a where $a \in A$ and the inverses of the elements h_s where $s \in S$ then generate in $\mathrm{End}_A(N)$ a commutative subring B and the homomorphism $a \mapsto h_a$ from A to B is such that the images of the elements of S are invertible. Then it follows that therc exists a unique homomorphism $\tilde{h}$ of $S^{-1}A$ to B such that

$$\tilde{h}(a/s) = h_a h_s^{-1}.$$

We know that such a homomorphism defines on N an $S^{-1}A$-module structure such that $(a/s) \cdot y = h_s^{-1}(a \cdot y)$. The A-module structure derived from this $S^{-1}A$-module structure by means of the homomorphism i_A^S is precisely the structure given initially.

Conversely, if N is an $S^{-1}A$-module and it is considered as an A-module by means of i_A^S, the homotheties $y \mapsto sy$, for $s \in S$, are bijective, for $y \mapsto (1/s)y$ is its inverse; and the $S^{-1}A$-module structure on N derived from its A-module structure by the process described above is the $S^{-1}A$-module structure given initially. Thus there is a canonical one-to-one correspondence between $S^{-1}A$-modules and A-modules in which the homotheties induced by the elements of S are bijective. Moreover, if N, N' are two A-modules with this property every A-module homomorphism $\phi : N \to N'$ is also a homomorphism of the $S^{-1}A$-module structures of N and

N', as, for all $y \in N$ and all $s \in S$, we may write $\phi(y) = \phi(s \cdot ((1/s)y)) = s \cdot \phi((1/s)y)$, whence $\phi((1/s)y) = (1/s)\phi(y)$; the converse is obvious.

This being so, the statement is just the characterization of the module obtained from M by extending the scalars to $S^{-1}A$, taking account of the above interpretation. □

Let A be a ring, S a subset of A, $\overline{S}$ the multiplicative subset of A generated by S and M an A-module. Then the $S^{-1}A$-module $M \otimes_A S^{-1}A$ is called the **module of fractions of M defined by S** and denoted by $S^{-1}M$.

Proposition 10.2.13. *Let A be a ring. Let $S \subseteq A$ be a multiplicative subset. Let M be an A-module. Then*

$$S^{-1}M = \varinjlim_{s \in S} M_s$$

where the partial ordering on S is given by $s \geq s' \iff s = as'$ for some $a \in A$ in which case the map $M_{s'} \to M_s$ is given by $m/s^e = ma^e/(s')^e$.

Proposition 10.2.14. *Let S be a multiplicative subset of A and M an A-module. For $m/s = 0$ where $m \in M$ and $s \in S$, it is necessary and saflicient that there exist $s' \in S$ such that $s'm = 0$.*

Proof. If $s' \in S$ is such that $s'm = 0$, clearly $m/s = (s'm)/(ss') = 0$. Conversely, suppose that $m/s = 0$. As $1/s$ is invertible in $S^{-1}A$, $m/1 = 0$. For every sub-A-module P of $S^{-1}A$ containing 1, we denote by $\beta(P, m)$ the image of $(m, 1)$ under the canonical mapping of $M \times P$ to $M \otimes_A P$. Then $(MS^{-1}A, m) = 0$, so there exists a finitely generated submodule P of $S^{-1}A$ containing 1 and such that $\beta(P, m) = 0$. For all $t \in S$ we denote by A_t the set of a/t, where $a \in A$. As P is finitely generated, there exists $t \in S$ such that $P \subseteq A_t$, whence $\beta(A_t, m) = 0$. The mapping $a \mapsto a/t$ from A to A_t is surjective; let B be its kernel. Then we have a surjective mapping $h : M \otimes_A A \to M \otimes_A A_t$ whose kernel is $B \otimes_A M$. By definition $\beta(A_t, m) = h(tm)$ and consequently tm can be expressed in the form $\sum_i b_i m_i$, where $b_i \in B$ and $m_i \in M$. Since $b_i/t = 0$ for all i, there exists $t' \in S$ such that $t'tm = 0$, whence the claim. □

Corollary 10.2.15. *The module $S^{-1}M$ can be identified with the set $M \times S$ modulo the equivalence relation*

$$(m, s) \sim (m', s') \iff \exists t \in S \text{ such that } t(ms' - m's) = 0$$

and the $S^{-1}A$-module structure defined by $(a/s)(m, t) = (am, st)$.

Corollary 10.2.16. *Let M be a finitely generated A-module. For $S^{-1}M = 0$, it is necessary and suficient that there exists $s \in S$ such that $sM = 0$.*

Proof. Without any conditions on M, clearly the relation $sM = 0$ for some $s \in S$ implies $S^{-1}M = 0$. Conversely, suppose that $S^{-1}M = 0$ and let $x_1, \ldots, x_n$ be a system of generators of M. The $m_i/1$ generate the $S^{-1}A$-module $S^{-1}M$, hence to say that $S^{-1}M = 0$ amounts to saying that $m_i/1 = 0$ for all i. By Corollary 10.2.15 there exist $s_i \in S$ such that $s_i m_i = 0$ and, taking $s = s_1 \cdots s_n$, we see $sm_i = 0$ for all i and hence $sM = 0$. □

Corollary 10.2.17. *Let M be a finitely generated A-module. For an ideal $\mathfrak{a}$ of A to be such that $\mathfrak{a}M = M$, it is necessary and sufiicient that there exist $a \in \mathfrak{a}$ such that $(1 + a)M = 0$.*

Proof. Clearly the relation $(1+a)M = 0$ implies $M = aM$. To prove the converse, we use the following result: For every ideal $\mathfrak{a}$ of A, the set $S = 1 + \mathfrak{a}$ is a multiplieative subset of A and the set $S^{-1}\mathfrak{a}$ is an ideal contained in the Jacobson radical of $S^{-1}A$. The first assertion is obvious, as well as the fact that $S^{-1}\mathfrak{a}$ is an ideal of $S^{-1}A$. On the other hand, $(1/1) + (a/s) = (s+a)/s$ and $s + \mathfrak{a} \in S$ for all $s \in S$ and $a \in \mathfrak{a}$ by definition of S. Hence $(1/1) + (a/s)$ is invertible in $S^{-1}A$ for all $a/s \in S^{-1}\mathfrak{a}$, which completes the proof of this result. This being done, if we set $N = S^{-1}M$, clearly N is a finitely generated $S^{-1}A$-module. If $\mathfrak{a}M = M$, then $S^{-1}\mathfrak{a}N = N$ and it follows that $N = 0$ by Nakayama's Lemma. The corollary then follows from Corollary 10.2.16. □

Remark 10.2.1. Let M be an A-module, f be an element of A. Consider a sequence (M_n) of A-modules, where $M_n = M$ and for any integers $m \leq n$, let $\varphi_{nm} : M_m \to M_n$ be the multiplication by f^{n-m}. Then it is immediate that (M_n, φ_{nm}) form an inductive system of A-modules, so let $N = \varinjlim M_n$ and $\varphi_n : N \to M_n$ be the canonical homomorphisms. We now define a functorial isomorphism from N to M_f: for each n, let $\theta_n : z \mapsto z/f^n$ be an A-homomorphism from $M_n = M$ to M_f, and since we clearly have $\theta_n \circ \varphi_{nm} = \theta_m$, let $\theta : N \to M_f$ be the induced homomorphism. Since any element of M_f is of the form z/f^n for some n, so θ is surjective. On the other hand, if $\theta(\varphi_n(z)) = 0$, which means $z/f^n = 0$, then there exists an integer $k > 0$ such that $f^k z = 0$, so $\varphi_{n+k,n}(z) = 0$, which means $\varphi_n(z) = 0$. We can then identify M_f with $\varinjlim M_n$ by the isomorphism θ.

Proposition 10.2.18. *Let A, B be two rings, S a multiplicative subset of A, T a multiplicative subset of B and f a homomorphism from A to B such that $f(S) \subseteq T$. Let M be an A-module, N a B-module and $\phi : M \to N$ an A-linear homomorphism. Then there exists a unique $S^{-1}A$-linear map $\tilde{\phi} : S^{-1}M \to T^{-1}N$ such that $\tilde{\phi}(m/1) = \phi(m)/1$ for all $m \in M$.*

Proof. Thc mapping $i_M^T \circ \phi$ from M to $T^{-1}N$ is A-linear. Moreover, if $s \in S$, then $f(s) \in T$, hence the homothety induced by s on $T^{-1}N$ is bijective. The existence and uniqueness of $\tilde{\phi}$ then follow from Proposition 10.2.12. Then, for $m \in M$ and $s \in S$,

$$\tilde{\phi}(m/s) = \phi(m)/f(s)$$

With the same notation, let C be a third ring, U a multiplicative subset of C, g a homomorphism from B to C such that $g(T) \subseteq U$, P a C-module, ψ a B-linear mapping from N to P and $\tilde{\phi}$ the $T^{-1}B$-linear mapping from B to $U^{-1}P$ associated with ψ. Then

$$\widetilde{(\psi \circ \phi)} = \tilde{\psi} \circ \tilde{\phi}$$

where the left hand side is the A-linear mapping $S^{-1}M \to U^{-1}P$ associated with $\psi \circ \phi$. Similarly, if ϕ' is a second A-linear mapping from M to N, then

$$\widetilde{(\phi + \phi')} = \tilde{\phi}' + \tilde{\phi}$$

the left-hand side being the A-linear mapping $S^{-1}M \to T^{-1}N$ associated with $\phi + \phi'$. □

If, in Proposition 10.2.18, we take $B = A$, $T = S$ and $\phi = \mathrm{id}_A$, it is easily seen that $\tilde{\phi}$ is just the mapping $\phi \otimes 1 : M \otimes_A S^{-1}A \to N \otimes_A S^{-1}A$. We shall henceforth denote it by $S^{-1}\phi$. If S is the complement of a prime ideal $\mathfrak{p}$ of A, we write $\phi_{\mathfrak{p}}$ instead of $S^{-1}\phi$.

Proposition 10.2.19. *Let f be a homomorphism from a ring A to a ring B and S a multiplicative subset of A. Then there exists a unique mapping $j : f(S)^{-1}B \to S^{-1}B$ (where B is considered as an A-module by means of f) such that $j(b/f(s)) = b/s$ for all $b \in B$, $s \in S$. If $\tilde{\phi} : S^{-1}A \to f(S)^{-1}B$ is the ring homomorphism associated with f, then $j \circ \tilde{f} = S^{-1}f$. The mapping j is an isomorphism of the $S^{-1}A$-module structure on $f(S)^{-1}B$ defined by $\tilde{f}$ onto that on $S^{-1}B$ and also of the B-module structure on $f(S)^{-1}B$ onto that on $S^{-1}B$ (resulting from the definition $S^{-1}B = S^{-1}A \otimes_A B$).*

Proof. If $b, b' \in B$ and $s, s' \in S$, the conditions $b/s = b'/s'$ and $b/f(s) = b'/f(s')$ are equivalent, as follows from Corollary 10.2.15, which establishes the existence of j and shows that j is bijective. The uniqueness of j is obvious. Clearly j is an additive group isomorphism. If $a \in A$, $b \in B$, $s, t \in S$ then

$$(a/s) \cdot (b/f(t)) = \tilde{f}(a/s)(b/f(t)) = f(a)/f(s)(b/f(t)) = (f(a)b)/f(st)$$

from which its follows that j is $S^{-1}A$-linear. Clearly $j \circ \tilde{f} = S^{-1}f$. Finally, if $b.b' \in B$, $s \in S$, then

$$j(b \cdot (b'/f(s)) = j(bb'/f(s)) = bb'/s = b \cdot (b'/s),$$

which proves the last assertion. □

The mapping j of Proposition 10.2.19 is called the canonical isomorphism of $f(S)^{-1}B$ onto $S^{-1}B$. These two sets are in general identified by means of f. Then $\tilde{f} = S^{-1}f$ and $i_B^S = i_B^{f(S)}$.

10.2.3 Change of multiplicative subset

Let A be a ring, S a multiplicative subset of A and M an A-module. If T is a multiplicative subset of A containing S, it follows from Proposition 10.2.18 that there exists a unique $S^{-1}A$-linear mapping $i_M^{T,S} : S^{-1}M \to T^{-1}M$ such that $i_M^T = i_M^{T,S} \circ i_M^T$. The mapping i_M^S maps the element m/s of $S^{-1}M$ to the element m/s of $T^{-1}M$. It is easily verified that $i_M^{T,S} = i_A^{T,S} \otimes 1_M$. If U is a third multiplicative subset of A such that $T \subseteq U$, then $i_M^{U,S} = i_M^{U,T} \circ i_M^{T,S}$. Moreover, if $\phi : M \to N$ is an A-module homomorphism, the diagram

$$\begin{tikzcd} S^{-1}M \arrow[r, "s^{-1}\phi"] \arrow[d, "i_M^{T,S}"] & S^{-1}N \arrow[d, "i_N^{T,S}"] \\ T^{-1}M \arrow[r, "T^{-1}\phi"] & T^{-1}N \end{tikzcd}$$

is commutative.

Proposition 10.2.20. *Let A be a ring and S, T two multiplicative subsets of A.*

(a) There exists a unique isomorphism i_A from the ring $(ST)^{-1}A$ onto the ring $(S^{-1}T)^{-1}(S^{-1}A)$ such that the diagram

$$\begin{tikzcd} A \arrow[r, "i_A^S"] \arrow[d, "i_A^{ST}"'] & S^{-1}A \arrow[d, "i_{S^{-1}A}^{S^{-1}T}"] \\ (ST)^{-1}A \arrow[r, "i"] & (S^{-1}T)^{-1}(S^{-1}A) \end{tikzcd}$$

(b) *Let M be an A-module. There exists an $(ST)^{-1}A$-isomorphism i_M from the $(ST)^{-1}A$-module $(ST)^{-1}M$ onto the $(S^{-1}T)^{-1}(S^{-1}A)$-module $(S^{-1}T)^{-1}(S^{-1}M)$ such that the diagram*

$$\begin{tikzcd} M \arrow[r, "i_M^S"] \arrow[d, "i_M^{ST}"'] & S^{-1}M \arrow[d, "i_{S^{-1}M}^{S^{-1}T}"] \\ (ST)^{-1}M \arrow[r, "i_M"] & (S^{-1}T)^{-1}(S^{-1}M) \end{tikzcd}$$

Proof. It suffices to prove (a). We use the definition of $(ST)^{-1}A$ as the solution of a universal mapping problem. Let B be a ring and f a homomorphism from A to B such that $f(ST)$ consists of invertible elements. As $f(S)$ consequently consists of invertible elements, there exists a unique homomorphism $f_1 : S^{-1}A \to B$ such that $f = f_1 \circ i_A^S$. For all $t \in T$, $f_1(i_A^S(t)) = f(t)$ is invertible in B by hypothesis, hence $f_1(S^{-1}T)$ consists of invertible elements; then there exists a unique homomorphism f_2 from $(S^{-1}T)^{-1}(S^{-1}A)$ to B such that $f_1 = f_2 \circ i_{S^{-1}A}^{S^{-1}T}$, whence $f = f_2 \circ i$, where $i = i_{S^{-1}A}^{S^{-1}T} \circ i_A^S$.

Moreover, if $f_2' : (S^{-1}T)^{-1}(S^{-1}A) \to B$ is a second homomorphism such that $f_2' \circ i = f$, then $(f_2' \circ i_{S^{-1}A}^{S^{-1}T}) \circ i_A^S = (f_2 \circ i_{S^{-1}A}^{S^{-1}T}) \circ i_A^S$, whence $f_2' \circ i_{S^{-1}A}^{S^{-1}T} = f_2 \circ i_{S^{-1}A}^{S^{-1}T}$ and consequently $f_2' = f_2$. As the images under i of the elements of ST are invertible, the ordered pair $((S^{-1}T)^{-1}(S^{-1}A), i)$ is a solution of the universal mapping problem (relative to A and ST). This shows the existence and uniqueness of i_A. □

Corollary 10.2.21. *If S and T are two multiplicative subsets of A with $S \subseteq T$, then writing $S^{-1}T$ for the image of T in $S^{-1}A$, we have $(S^{-1}T)^{-1}(S^{-1}A) = T^{-1}A$.*

Corollary 10.2.22. *If $S \subseteq A$ is a multiplicative set and $\mathfrak{p}$ is a prime ideal of A disjoint from S then $(S^{-1}A)_{S^{-1}\mathfrak{p}} = A_{\mathfrak{p}}$. In particular if $\mathfrak{p}_1 \subseteq \mathfrak{p}_2$ are prime ideals of A, then $(A_{\mathfrak{p}_2})_{\mathfrak{p}_1} = A_{\mathfrak{p}_1}$.*

Proposition 10.2.23. *Let S, T be multiplicatively closed subsets of A, such that $S \subseteq T$. Then the following statements are equivalent:*

(a) *The homomorphism $i_A^{T,S}$ is bijective.*

(b) *For every A-module M, the homomorphism $i_M^{T,S} : S^{-1}M \to T^{-1}M$ is bijective.*

(c) *For each $t \in T$, $t/1$ is a unit in $S^{-1}A$.*

(d) *For each $t \in T$ there exists $x \in A$ such that $xt \in S$.*

(e) *Every prime ideal which meets T also meets S.*

Proof. It has been seen above that $i_M^{T,S} = i_A^{T,S} \otimes 1_M$, which immediately proves the equivalence of (a) and (b). Also, the equivalence of (c) and (d) is easy to see. By Proposition 10.2.20, since $S \subseteq T$, $T^{-1}A$ is identified with $(S^{-1}T)^{-1}(S^{-1}A)$ and (a) is equivalent to saying that the elements of $S^{-1}T$ are invertible in $S^{-1}A$, so (a) is equivalent to (c). Now by definition, it is clear that (d) implies (e).

So assume (e). To show the injectivity of $i_A^{T,S}$, let $i_A^{T,S}(x/s) = 0$ in $T^{-1}A$, so that $xt = 0$ for some $t \in T$. Now assume that $x/s \neq 0$, which is to say $\mathrm{Ann}(x) \cap S = \varnothing$. Then by Proposition 10.2.3, there is a prime ideal $\mathfrak{p} \supseteq \mathrm{Ann}(x)$ such that $\mathfrak{p} \cap S = \varnothing$. By assumption, we also have $\mathfrak{p} \cap T = \varnothing$, which is a contradiction. This proves $x/s = 0$, so $i_A^{T,S}$ is injective.

For the surjectivity, let $t \in T$. We claim that there exists $x \in A$ such that $xt \in S$. Otherwise, $(t) \cap S = \varnothing$, and by Proposition 10.2.3, there is a prime ideal $\mathfrak{p} \supseteq (t)$ such that $\mathfrak{p} \cap S = \varnothing$. Then we have $\mathfrak{p} \cap T = \varnothing$, which is a contradiction. □

By Proposition 10.2.23, we see that amongst the multiplicative subsets T of A containing S and satisfying the equivalent conditions of Proposition 10.2.23, there exists a greatest, consisting of all the elements of A which divide an element of S. This set can be characterized by another property, which we now define.

A multiplicative subset S of a ring A is called **saturated** if the relation $xy \in S$ implies $x \in S$ and $y \in S$. If this holds, then for any $x \in A \setminus S$ and any $s \in S$ we have $ax \notin S$, which shows $x/1$ is not a unit in $S^{-1}A$, hence there is a maximal ideal $\mathfrak{m}$ contains $x/1$. Now consider the contraction $\mathfrak{m}^c$ in A. It contains x, and is prime since $\mathfrak{m}$ is prime. Hence we see x is contained in a prime ideal $\mathfrak{p}$ disjoint from A, thus $A \setminus S$ is a union of prime ideals of A. In fact this condition is also sufficient: if $A \setminus S = \bigcup \mathfrak{p}_i$ for prime ideals $\mathfrak{p}_i$, then assume $xy \in S$. If $x \in A \setminus S$, then $x \in \mathfrak{p}_i$ for some $\mathfrak{p}_i$. Since $\mathfrak{p}_i$ is an ideal, $xy \in \mathfrak{p}_i$ for any $y \in A$, which means $xy \in A \setminus S$, a contradiction. So $x, y \in S$.

Proposition 10.2.24. *Let S be a multiplicative subset of A and define*

$$\bar{S} = \{x \in A : \textit{there exists } y \in S \textit{ such that } xy \in S\}.$$

*Then S is the smallest saturated multiplicative subset containing S, called the **saturation** of S, and $A \setminus \bar{S}$ is the union of the prime ideals of A not meeting S.*

Proof. It is easy to see $\bar{S}$ is a miltiplicative subset and saturated. In particular, $A \setminus \bar{S} = \bigcup_i \mathfrak{p}_i$, where $\mathfrak{p}_i$ are prime ideals. Now if $\mathfrak{p}$ is a prime ideal such that $\mathfrak{p} \cap S = \varnothing$, then for any $x \in \mathfrak{p}$, if there exists $y \in S$ such that $xy \in S$, then $xy \in \mathfrak{p} \cap S$, which is a contradiction. This shows $\mathfrak{p} \subseteq A \setminus S$, which finishes the proof. □

Corollary 10.2.25. *Let S, T be multiplicatively closed subsets of A, such that $S \subseteq T$. Then $i_M^{T,S}$ is bijective if and only if T is contained in the saturation of S.*

Proposition 10.2.26. *Let A be a ring, S be a multiplicative subset of A. If B is a subring of $S^{-1}A$ containing $i_A^S(A)$, then we have*

$$S^{-1}A = S^{-1}B = T^{-1}B \quad \textit{where} \quad T = \{b \in B : b \textit{ is a unit of } S^{-1}A\}.$$

Proof. By definition of T we have $S \subseteq T$ and $T^{-1}B$ can be identified with a subring of $S^{-1}A$. We can write

$$\begin{tikzcd}
A \arrow[r, "i_A^S"] \arrow[d] & S^{-1}A \arrow[d, "i"] \\
B \arrow[r, "i_B^T"] \arrow[d, hook] & T^{-1}B \arrow[dl, "j"] \\
S^{-1}A &
\end{tikzcd}$$

where i and j the natural maps. Also, by definition we have $i \circ j = 1_{S^{-1}A}$. Also, by the definition of T and Proposition 10.2.23 we see $S^{-1}B = T^{-1}B$. Now, for any $b/t \in T^{-1}B$, we have $t^{-1} = a/s$

where $a \in A$, $s \in S$. Since $b \in B \subseteq S^{-1}A$, we then see

$$b/t = i(b) \cdot i(a/s) = i(b \cdot a/s)$$

whence i is surjective. Thus i and j are mutually inverse, giving an isomorphism $S^{-1}A \cong T^{-1}B$. □

Proposition 10.2.27. *Let M be an A-module. For every submodule N' of the $S^{-1}A$-module $S^{-1}M$, let $\phi(N')$ be the inverse image of N' under i_M^S. Then:*

(a) $S^{-1}\phi(N') = N'$.

(b) For every submodule N of M, the submodule $\phi(S^{-1}N)$ of M consists of those $m \in M$ for which there exists $s \in S$ such that $sm \in N$.

(c) ϕ is an isomorphism of the set of sub-$S^{-1}A$-modules of $S^{-1}M$ onto the set of submodules Q of M which satisfy the following condition:

(MS) If $sm \in Q$, where $s \in S$, $m \in M$, then $m \in Q$.

Proof. Obviously $S^{-1}\phi(N') \subseteq N'$. Conversely, if $n' = m/s \in N'$, then $m/1 \in N'$, hence in $m \in \phi(N')$ and conscquently $n' \in S^{-1}(\phi(N'))$, whence (a). For an element $m \in M$ to be such that $m \in \phi(S^{-1}N)$, it is necessary and sufficient that $m/1 \in S^{-1}N$, that is, there exist $s \in S$ and $n \in N$ such that $m/1 = n/s$, which means there exists $s' \in S$ such that $s'sm = s'n \in N$, whence (b). Finally, the relation $sm \in \phi(N')$ is equivalent by definition to $sm/1 \in N'$ and as $s/1$ is invertible in $S^{-1}A$, this implies $m/1 \in N'$, or $m \in \phi(N')$, hence $\phi(N')$ satisfies condition (MS). On the other hand, it follows from (b) that, if N satisfies (MS), then $\phi(S^{-1}N) = N$, which completes the proof of (c). □

The submodule $\phi(S^{-1}N)$ is called the **saturation** of N in M with respect to S, and the submodules satifying condition (MS) (and hence equal to their saturations) are said to be **saturated** with respect to S. The submodule $\phi(S^{-1}N)$ is the kernel of the composite homomorphism

$$M \xrightarrow{\pi} M/N \xrightarrow{i_{M/N}^S} S^{-1}M/S^{-1}N$$

where π is the canonical homomorphism, as follows from the commutativity of the diagram

$$\begin{tikzcd} M \arrow[r, "\pi"] \arrow[d, "i_M^S"] & M/N \arrow[d, "i_{M/N}^S"] \\ S^{-1}M \arrow[r] & S^{-1}M/S^{-1}N \end{tikzcd}$$

If S is the complement in A of a prime ideal $\mathfrak{p}$, $\phi(S^{-1}N)$ is also called the saturation of N in M with respect to $\mathfrak{p}$.

Corollary 10.2.28. *Let N_1, N_2 be two submodules of an A-modale M. For $S^{-1}N_1 \subseteq S^{-1}N_2$, it is necessary and sufficient that the saturation of N_1 with respect to S be contained in that of N_2.*

Corollary 10.2.29. *If M is a Noetherian (resp. Artinian) A-module, then $S^{-1}M$ is a Noetherian (resp. Artinian) $S^{-1}A$-module. In particular, if the ring A is Noetherian (resp. Artinian), so is the ring $S^{-1}A$.*

10.2.4 Properties of the localization operation

Proposition 10.2.30. *Let A be a ring and S a multiplicative subset of A. Then $S^{-1}A$ is A-flat.*

Proof. If $\phi : M \to N$ is an injective homomorphism of A-modules, it is necessary to establish that $S^{-1}\phi : S^{-1}M \to S^{-1}N$ is injective. Now, if m/s is such that $\phi(m)/s = 0$, this implies the existence of a $t \in S$ such that $t\phi(m) = 0$ or $\phi(tm) = 0$. As ϕ is injective, it follows that $tm = 0$, whence $m/s = 0$ in $S^{-1}M$. □

Corollary 10.2.31. *Formation of fractions commutes with formation of finite sums, finite intersections and quotients. Precisely, if N, P are submodules of an A-module M, then*

(a) $S^{-1}(N + P) = S^{-1}N + S^{-1}P$.

(b) $S^{-1}(N \cap P) = S^{-1}N \cap S^{-1}P$.

(c) The $S^{-1}A$-modules $S^{-1}(M/N)$ and $(S^{-1}M)/(S^{-1}N)$ are isomorphic.

Proof. Part (a) follows readily from the definitions and (b) is easy to verify: if $y/s = z/t$ ($y \in N$, $z \in P$, $s, t \in S$) then $u(ty - sz) = 0$ for some $u \in S$, hence $w = uty = usz \in N \cap P$ and therefore $y/s = w/stu \in S^{-1}(N \cap P)$. Consequently $S^{-1}(N \cap P) \subseteq S^{-1}(N) \cap S^{-1}P$, and the reverse inclusion is obvious.

Now to prove (c), we apply S^{-1} to the exact sequence

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$$

Since localization is exact, we get the claim. □

Proposition 10.2.32. *Let M be a finitely generated A-module, S a multiplicatively closed subset of A. Then $S^{-1}\mathrm{Ann}(M) = \mathrm{Ann}(S^{-1}M)$.*

Proof. If this is true for two A-modules, M, N, it is true for $M + N$:

$$\begin{aligned} S^{-1}(\mathrm{Ann}(M + N)) &= S^{-1}(\mathrm{Ann}(M) \cap \mathrm{Ann}(N)) = \mathrm{Ann}(S^{-1}M) \cap \mathrm{Ann}(S^{-1}N) \\ &= \mathrm{Ann}(S^{-1}M + S^{-1}N) = \mathrm{Ann}(S^{-1}(M + N)) \end{aligned}$$

where we use Corollary 10.2.31. Hence it is enough to prove for M generated by a single element: then $M = A/I$ as A-module, where $\mathfrak{a} = \mathrm{Ann}(M)$. We have

$$S^{-1}(M) = S^{-1}(A/\mathfrak{a}) \cong (S^{-1}A)/(S^{-1}\mathfrak{a})$$

by Corollary 10.2.31, which proves the claim. □

Corollary 10.2.33. *If N, P are submodules of an A-module M and if P is finitely generated, then $S^{-1}(N : P) = (S^{-1}N : S^{-1}P)$.*

Proof. We have $(N : P) = \mathrm{Ann}((N + P)/P)$, so the claim follows by Proposition 10.2.32. □

Proposition 10.2.34. *Let I be a directed set, $(S_i)_{i\in I}$ an inereasing family of multiplicative subsets of a ring A, and $S = \bigcup_i S_i$. We write $\rho_{\beta\alpha} = i_A^{S_\beta, S_\alpha}$. Then $(S_\alpha^{-1}A, \rho_{\beta,\alpha})$ is a direct system of rings and, if for $\alpha \in I$, ρ_α is the canonical mapping of $S_\alpha^{-1}A$ to $\varinjlim S_\alpha^{-1}A$, there exists a unique isomorphism $i : \varinjlim S_\alpha^{-1}A \to S^{-1}A$ such that $i \circ \rho_\alpha = i_A^{S,S_\alpha}$ for all $\alpha \in I$.*

$$\begin{tikzcd}
S_\alpha^{-1}A \arrow[r, "\rho_{\beta\alpha}"] \arrow[drrr, bend right, "\rho_\alpha"'] & S_\beta^{-1}A \arrow[r, "\rho_{\gamma\beta}"] \arrow[drr, bend right, "\rho_\beta"'] & S_\gamma^{-1}A \arrow[r] \arrow[dr, "\rho_\gamma"] & \cdots \arrow[d] & & \\
& & & \varinjlim S_\alpha^{-1}A \arrow[r, "i"] & S^{-1}A
\end{tikzcd}$$

Proof. For $\alpha \preceq \beta \preceq \gamma$, $\rho_{\gamma\alpha} = \rho_{\gamma\beta} \circ \rho_{\beta\alpha}$, hence $(S_\alpha^{-1}A, \rho_{\beta\alpha})$ is a direct system of rings, and we write $B = \varinjlim S_\alpha^{-1}A$. As

$$i_A^{S,S_\alpha} = i_A^{S,S_\beta} \circ \rho_{\beta\alpha}$$

for $\alpha \preceq \beta$, (i_A^{S,S_α}) is a direct system of homomorphisms and $i = \varinjlim i_A^{S,S_\alpha}$ is the unique map such that $i \circ \rho_\alpha = i_A^{S,S_\alpha}$ for all $\alpha \in I$.

The homomorphisms $\rho_\alpha \circ i_A^{S_\alpha}$ are all equal since $\rho_{\alpha\beta} \circ i_A^{S_\alpha} = i_A^{S_\beta}$ for $\alpha \preceq \beta$, so let $\phi : A \to B$ be their common value. Clearly elements of $\phi(S)$ are invertible in B, which shows there exists a homomorphism $\tilde{\phi} : S^{-1}A \to B$ such that $\tilde{\phi} \circ i_A^S = \phi$. Then

$$i \circ \tilde{\phi} \circ i_A^S = i \circ \phi = i \circ \rho_\alpha \circ i_A^{S_\alpha} = i_A^{S,S_\alpha} \circ i_A^{S_\alpha} = i_A^S$$

for all $\alpha \in I$ and consequently $i \circ \tilde{\phi}$ is the identity map of $S^{-1}A$. On the other hand, for all $\alpha \in I$,

$$\tilde{\phi} \circ i \circ \rho_\alpha \circ i_A^{S_\alpha} = \tilde{\phi} \circ i_A^{S,S_\alpha} \circ i_A^{S_\alpha} = \tilde{\phi} \circ i_A^S = \phi = \rho_\alpha \circ i_A^{S_\alpha}$$

whence $\tilde{\phi} \circ i \circ \rho_\alpha = \rho_\alpha$ for all $\alpha \in I$; it follows that $\tilde{\phi} \circ i$ is the identity automorphism of B and consequently i is an isomorphism. □

Corollary 10.2.35. *Under the hypotheses of Proposition 10.2.34, let M be an A-module. We write $\tau_{\beta\alpha} = i_M^{S_\beta,S_\alpha}$ for $\alpha \preceq \beta$. Then $(S_\alpha^{-1}M, \tau_{\beta,\alpha})$ is a direct system of rings and, if for $\alpha \in I$, τ_α is the canonical mapping of $S_\alpha^{-1}M$ to $\varinjlim S_\alpha^{-1}M$, there exists a unique isomorphism $i : \varinjlim S_\alpha^{-1}M \to S^{-1}M$ such that $i \circ \tau_\alpha = i_M^{S,S_\alpha}$ for all $\alpha \in I$.*

Proof. The corollary follows immediately from the definitions $S_\alpha^{-1}M = M \otimes_A S_\alpha^{-1}A$ and $S^{-1}M = M \otimes_A S^{-1}A$ and the fact that taking direct limits commutes with tensor products. □

10.2.5 Ideals under localization

Proposition 10.2.36. *Let S be a multiplicative subset of a commutative ring A, and consider the localization operation. Let $\mathfrak{a}$ be an ideal in A, and $\mathfrak{b}$ an ideal in $S^{-1}A$.*

(a) $(\mathfrak{b}^c)^e = \mathfrak{b}$, *hence every ideal in $S^{-1}A$ is an extended ideal.*

(b) $(\mathfrak{a}^e)^c = \bigcup_{s \in S}(\mathfrak{a} : s)$. *Hence $S^{-1}\mathfrak{a}$ is proper if and only if $\mathfrak{a} \cap S \neq \varnothing$ and $\mathfrak{a}$ is a contracted ideal if and only if no element of S is a zero-divisor in $A/\mathfrak{a}$.*

(c) The assignment $\mathfrak{p} \to S^{-1}\mathfrak{p}$ gives an inclusion-preserving bijection between the set of prime ideals of A disjoint from S and the set of ideals of $S^{-1}A$.

(d) The operation S^{-1} commutes with formation of finite sums, products, intersections and radicals.

Proof. Recall that we always have $\mathfrak{b} \subseteq (\mathfrak{b}^c)^e$. Conversely, if $a/s \in \mathfrak{b}$ then $a/1 \in \mathfrak{b}$, so $a \in \mathfrak{b}^c$. It follows that $a/s \in S^{-1}(\mathfrak{b}^c) = (\mathfrak{b}^c)^e$, so $\mathfrak{b} = (\mathfrak{b}^c)^e$. For (b), by defninition we have

$$\begin{aligned}(\mathfrak{a}^e)^c &= \{a \in A : a/1 \in \mathfrak{a}^e\} = \{a \in A : (sa - r)u = 0 \text{ for some } r \in I \text{ and } u, s \in S\} \\ &= \{a \in A : (\exists s \in S)\, sx \in \mathfrak{a}\} = \bigcup_{s \in S} (\mathfrak{a} : s).\end{aligned}$$

From this, we see $\mathfrak{a}^e = (\bigcup_{s \in S}(\mathfrak{a} : s))^e$, and therefore $1 \in \mathfrak{a}^e$ if and only if $\mathfrak{a} \cap S \neq \varnothing$. From the description of $\mathfrak{a}^{ec}$, we also find that $\mathfrak{a}^{ec} = \mathfrak{a}$ if and only if $\bigcup_{s \in S}(\mathfrak{a} : s) \subseteq \mathfrak{a}$, if and only if no element of S is a zero-divisor in $A/\mathfrak{a}$. This proves (b).

If $\mathfrak{p}$ is prime in A such that $\mathfrak{p} \cap S = \varnothing$, then we see that $(\mathfrak{p} : s) = \mathfrak{p}$ for all $s \in S$, whence $(\mathfrak{p}^e)^c = \mathfrak{p}$. Thus $(\mathfrak{p})^e$ is a bijection on prime ideals of A. If $\mathfrak{p}$ is prime in $S^{-1}A$, then $\mathfrak{p}^c$ is prime in A. Further, by part (b) we have $\mathfrak{p}^c \cap S = \varnothing$.

If $\mathfrak{p}$ is prime in A such that $\mathfrak{p} \cap S = \varnothing$, then $S^{-1}\mathfrak{p}$ is a proper ideal, as we see in (b). Now we prove the extension $\mathfrak{p}^e = S^{-1}\mathfrak{p}$ is prime. Let $x/s, y/t \notin S^{-1}\mathfrak{p}$ but $xy/st \in S^{-1}\mathfrak{p}$. Then by definition for some $p \in \mathfrak{p}, u \in S$ we have

$$u(xy - pst) = 0.$$

That is, $uxy = ustp \in \mathfrak{p}$. Since $\mathfrak{p} \cap S = \varnothing$, we must have $xy \in \mathfrak{p}$. But since $x/s, y/t \notin S^{-1}\mathfrak{p}$, $x \notin \mathfrak{p}$ and $y \notin \mathfrak{p}$. This is a contradiction. Thus the extension and contraction corresponds the prime ideals in $S^{-1}A$ and prime ideals in A disjoint from S.

Finally, we deal with (e). For sums and products, this follows from Proposition 10.1.27; for intersections, from Corallary 10.2.31. As to radicals, we have $S^{-1}\sqrt{\mathfrak{a}} \subseteq \sqrt{S^{-1}\mathfrak{a}}$ from Proposition 10.1.27 since $S^{-1}\mathfrak{a} = \mathfrak{a}^e$. For the converse, let $x/s \in \sqrt{S^{-1}\mathfrak{a}}$, then $x^n/s^n \in S^{-1}\mathfrak{a}$ for some $n > 0$. This means $ux^n \in \mathfrak{a}$ for some $u \in S$. Then $u^n x^n$ also belongs to $\mathfrak{a}$, so $ux \in \sqrt{\mathfrak{a}}$. Moreover, since $x/s = (ux)/(us)$, we get $x/s \in S^{-1}\sqrt{\mathfrak{a}}$. □

Corollary 10.2.37. *There is an inclusion-preserving bijection between the prime ideals of $A_\mathfrak{p}$ and the prime ideals of A contained in $\mathfrak{p}$. Hence $A_\mathfrak{p}$ is a local ring.*

Proof. If $a, b \notin \mathfrak{p}$, then $ab \notin \mathfrak{p}$. So $A - \mathfrak{p}$ is a multiplicative set. The claim now comes from Proposition 10.2.36.

The elements a/s with $a \in \mathfrak{p}$ form an ideal $\mathfrak{m}$ in $A_\mathfrak{p}$. If $b/t \notin \mathfrak{m}$, then $b \notin \mathfrak{p}$, so $b \in A - \mathfrak{p}$ and is a unit in $A_\mathfrak{p}$. By Proposition 10.1.15, $A_\mathfrak{p}$ is a local ring.

Or we can use the correspondence to prove $S^{-1}\mathfrak{p}$ is the unique maximal ideal. □

Corollary 10.2.38. *If $\mathfrak{n}(A)$ is the nilradical of A, the nilradical of $S^{-1}A$ is $S^{-1}\mathfrak{n}(A)$.*

Proof. Note that $\mathfrak{n}(A) = \sqrt{(0)}$. Since $S^{-1}\sqrt{\mathfrak{a}} = \sqrt{S^{-1}\mathfrak{a}}$, we find $S^{-1}\mathfrak{n}(A) = S^{-1}\sqrt{0} = \sqrt{S^{-1}(0)} = \mathfrak{n}(S^{-1}A)$. □

Remark 10.2.2. Thus the passage from A to $A_\mathfrak{p}$ cuts out all prime ideals except those contained in $\mathfrak{p}$. In the other direction, the passage from A to $A/\mathfrak{p}$ cuts out all prime ideals except those containing $\mathfrak{p}$. Hence if $\mathfrak{p}, \mathfrak{q}$ are prime ideals such that $\mathfrak{p} \supseteq \mathfrak{q}$, then by localizing with respect to $\mathfrak{p}$ and taking the quotient mod $\mathfrak{q}$ (in either order: these two operations commute, by Corallary 10.2.31), we restrict our attention to those prime ideals which lie between $\mathfrak{p}$ and $\mathfrak{q}$. In particular, if $\mathfrak{p} = \mathfrak{q}$ we end up with a field, called the **residue field at** $\mathfrak{p}$, which can be obtained

either as the field of fractions of the integral domain $A/\mathfrak{p}$ or as the residue field of the local ring $A_\mathfrak{p}$.

Proposition 10.2.39. *Let A be a ring and S a multiplicative subset of A. For every ideal $\mathfrak{b}$ of $S^{-1}A$, let $\mathfrak{a} = (i_A^S)^{-1}(\mathfrak{b})$ be such that $S^{-1}\mathfrak{a} = \mathfrak{b}$.*

(a) Let π be the canonical homomorphism $A \to A/\mathfrak{a}$. Then the homomorphism from $S^{-1}A$ to $\pi(S)^{-1}(A/\mathfrak{a})$ canonically associated with π is surjective and its kernel is $\mathfrak{b}$, which defines, by taking quotients, a canonical isomorphism of $(S^{-1}A)/\mathfrak{b}$ onto $\pi(S)^{-1}(A/\mathfrak{a})$. Moreover, the canonical homomorphism from $A/\mathfrak{a}$ to $\pi(S)^{-1}(A/\mathfrak{a})$ is injective.

(b) If $\mathfrak{q}$ is a prime ideal of $S^{-1}A$ and $\mathfrak{p} = (i_A^S)^{-1}(\mathfrak{q})$, then there exists an isomorphism of the ring of fractions $A_\mathfrak{p}$ onto the ring $(S^{-1}A)_\mathfrak{q}$, which maps a/b to $(a/1)/(b/1)$, where $a \in A$, $b \in A - \mathfrak{p}$.

Proof. The ring $\pi(S)^{-1}(A/\mathfrak{a})$ can be identified with $S^{-1}(A/\mathfrak{a})$ by means of the canonical isomorphism between these two modules. The exact sequence $0 \to \mathfrak{a} \to A \to A/\mathfrak{a} \to 0$ then induces an exact sequence

$$0 \longrightarrow S^{-1}\mathfrak{a} \longrightarrow S^{-1}A \longrightarrow S^{-1}(A/\mathfrak{a}) \longrightarrow 0$$

whose existence proves the first assertion of (a), taking account of the fact that $\mathfrak{b} = S^{-1}\mathfrak{a}$. Since $\mathfrak{a}$ is saturated with respect S, the conditions $a \in A$, $s \in S$, $as \in \mathfrak{a}$ imply $a \in \mathfrak{a}$; the homothety of ratio s on $A/\mathfrak{a}$ is then injective, which proves the second assertion of (i).

Suppose that $\mathfrak{q}$ is prime and such that $\mathfrak{p}$ is also prime. The set $T = A - \mathfrak{p}$ is a multiplicative subset of A which contains S, whence $ST = T$. Then it follows from Corollary 10.2.21 that there exists a unique isomorphism i of $T^{-1}A = A_\mathfrak{p}$ onto $(S^{-1}T)^{-1}(S^{-1}A)$ such that

$$i(a/b) = (a/1)/(b/1)$$

where $a \in A$ and $b \in T$. On the other hand $S^{-1}T$ obviously does not meet $\mathfrak{q}$. Conversely, let $a/s \in S^{-1}A$; since $1/s$ is invertible in $S^{-1}A$, the condition $a/s \notin \mathfrak{q}$ is equivalent to $i_A^S(a) \notin \mathfrak{q}$ and hence to $a \notin \mathfrak{p}$. It follows that $S^{-1}A - \mathfrak{q} = S^{-1}T$ and hence $(S^{-1}T)^{-1}(S^{-1}A) = (S^{-1}A)_\mathfrak{q}$. □

Proposition 10.2.40. *Let $\rho : A \to B$ be a ring homomorphism and let $\mathfrak{p}$ be a prime ideal of A. Then $\mathfrak{p}$ is the contraction of a prime ideal of S if and only if $\mathfrak{p}^{ec} = \mathfrak{p}$.*

Proof. One direction is trivial. Conversely, suppose that $\mathfrak{p}^{ec} = \mathfrak{p}$ and consider the multiplicative subset $S = \rho(A - \mathfrak{p})$ of B. The hypothesis shows that $S \cap \mathfrak{p}^e = \varnothing$, so there exists a prime ideal $\mathfrak{q}$ of B disjoint with S such that $\mathfrak{p}^e \subseteq \mathfrak{q}$. Then $\mathfrak{q}^c$ contains $\mathfrak{p}$ and is disjoint with $A - \mathfrak{p}$, whence $\mathfrak{q}^c = \mathfrak{p}$. □

Corollary 10.2.41. *Let $\rho : A \to B$ be a ring homomorphism.*

(a) Suppose that there exists a B-module E such that $\rho^*(E)$ is a faithfully flat A-module. Then, for every prime ideal $\mathfrak{p}$ of A, there exists a prime ideal $\mathfrak{P}$ of B such that $\mathfrak{P}^c = \mathfrak{p}$.

(b) Conversely, suppose that B is a flat A-module. If for every prime ideal $\mathfrak{p}$ of A, there exists an ideal $\mathfrak{P}$ of B such that $\mathfrak{P}^c = \mathfrak{p}$, then B is a faithfully flat A-module.

Proof. The hypothesis in (a) implies that, for every ideal $\mathfrak{a}$ of A, we have $\mathfrak{a}^{ec} = \mathfrak{a}$ (Proposition 7.3.13), and it is sufficient to apply Proposition 10.2.40.

Now assume the conditions in (b). It is sufficient to show that, for every maximal ideal $\mathfrak{m}$ of A, there exists a maximal ideal $\mathfrak{M}$ of B such that $\mathfrak{M}^c = \mathfrak{m}$ (Proposition 7.3.15). Now there exists by hypothesis an ideal $\mathfrak{Q}$ of B such that $\mathfrak{Q}^c = \mathfrak{m}$. As $\mathfrak{Q} \neq B$, there exists a maximal ideal $\mathfrak{M}$ of B containing $\mathfrak{Q}$ and consequently $\mathfrak{M}^c = \mathfrak{m}$ since $\mathfrak{M}^c$ cannot contain 1. □

Corollary 10.2.42. *Let $\rho : A \to B$ be a ring homomorphism such that B is a flat A-module. Let $\mathfrak{P}$ be a prime ideal of B and let $\mathfrak{p} = \mathfrak{P}^c$. Then ${}^a\rho_{\mathfrak{p}} : \operatorname{Spec}(B_{\mathfrak{P}}) \to \operatorname{Spec}(A_{\mathfrak{p}})$ is surjective.*

Proof. The map $\rho_{\mathfrak{p}} : A_{\mathfrak{p}} \to B_{\mathfrak{P}}$ is a local homomorphism:

$$(\mathfrak{p}A_{\mathfrak{p}})^e = \left(\frac{\mathfrak{p}}{A - \mathfrak{p}}\right)^e = \frac{\mathfrak{p}^e}{f(A - \mathfrak{p})} = \frac{\mathfrak{q}^{ce}}{f(A - \mathfrak{p})} \subseteq \mathfrak{q}B_{\mathfrak{q}} \neq B_{\mathfrak{q}}.$$

Therefore $B_{\mathfrak{P}}$ is a faithfully flat $A_{\mathfrak{p}}$-module by Proposition 7.3.15, and the claim follows from Corollary 10.2.41. □

Proposition 10.2.43. *Let B be a ring and A a subring of B. For every minimal prime ideal $\mathfrak{p}$ of A there exists a minimal prime ideal $\mathfrak{P}$ of B such that $\mathfrak{P} \cap A = \mathfrak{p}$.*

Proof. Let $\mathfrak{p}$ be a minimal prime of A and $S = A - \mathfrak{p}$. Then the ring $A_{\mathfrak{p}}$ is identified with a subring of $S^{-1}B$ and it has a single prime ideal $\mathfrak{p}A_{\mathfrak{p}}$ since $\mathfrak{p}$ is minimal. As $S^{-1}B$ is not reduced to 0 (since it contains $A_{\mathfrak{p}}$), it has at least one prime ideal $\mathcal{P}$ and therefore $\mathcal{P} \cap A_{\mathfrak{p}} = \mathfrak{p}A_{\mathfrak{p}}$. If $\mathfrak{P}' = (i_B^S)^{-1}(\mathcal{P})$, we have

$$i_A^S(\mathcal{P} \cap A) \subseteq \mathcal{P} \cap A_{\mathfrak{p}} = \mathfrak{p}A_{\mathfrak{p}}.$$

hence $\mathfrak{P}' \cap A \subseteq \mathfrak{p}$, and as $\mathfrak{p}$ is minimal, $\mathfrak{P}' \cap A = \mathfrak{p}$. If $\mathfrak{P}$ is a minimal prime ideal of B contained in $\mathfrak{P}'$, then we also have $\mathfrak{P} \cap A = \mathfrak{p}$, whence the claim. □

10.2.6 Modules of fractions of tensor products and Hom sets

Proposition 10.2.44. *Let A be a ring and S a multiplicative subset of A.*

(a) If M and N are two A-modules, the there is a canonical isomorphism

$$S^{-1}M \otimes_{S^{-1}A} S^{-1}N \cong S^{-1}(M \otimes_A N).$$

(b) If M and N are two $S^{-1}A$-modules, the canonical homomorphism $M \otimes_A N \to M \otimes_{S^{-1}A} N$ derived from the A-bilinear mapping $(x, y) \mapsto x \otimes y$ is bijective.

Proof. Assertion (a) is an immediate consequence of the definition $S^{-1}M = M \otimes_A S^{-1}A$ and the associativity of tensor products. To prove (b), we note first that in M and N, considered as A-modules, the homotheties induced by the elements $s \in S$ are bijective, hence $M = S^{-1}M$ and $N = S^{-1}N$ and similarly $S^{-1}(M \otimes_A N) = M \otimes_A N$. Then (b) is then a special case of (a). □

Corollary 10.2.45. *Let M be an A-module and $\mathfrak{a}$ an ideal of A. The sub-$S^{-1}A$-modules*

$$(S^{-1}\mathfrak{a})(S^{-1}M), \quad \mathfrak{a}(S^{-1}M), \quad (S^{-1}\mathfrak{a})i_M^S(M), \quad S^{-1}(\mathfrak{a}M)$$

of $S^{-1}M$ are identical. In particular, if $\mathfrak{a}$ and $\mathfrak{b}$ are two ideals of A, then

$$(S^{-1}\mathfrak{a})(S^{-1}\mathfrak{b}) = \mathfrak{a}(S^{-1}\mathfrak{b}) = (S^{-1}\mathfrak{a})\mathfrak{b} = S^{-1}(\mathfrak{a}\mathfrak{b}).$$

Proposition 10.2.46. *Let A be a ring and S a multiplicative subset of A.*

(a) If M and N are two A-modules and M is finitely generated (resp. finitely presented), the canonical homomorphism

$$S^{-1}\mathrm{Hom}_A(M,N) \to \mathrm{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}N)$$

is injective (resp. bijectioe).

(b) If M and N are two $S^{-1}A$-modules, the canonical bijection

$$\mathrm{Hom}_{S^{-1}A}(M,N) \to \mathrm{Hom}_A(M,N)$$

is bijective.

Proof. As $S^{-1}A$ is a flat A-module, (a) is a particular case of Proposition 7.2.29. On the other hand, we note that every A-homomorphism of $S^{-1}A$-modules is necessarily $S^{-1}A$-linear, whence (b). □

Proposition 10.2.47. *Let A, B be two rings, $\rho : A \to B$ a homomorphism, S a multiplicative subset of A, and $\tilde{\rho} : S^{-1}A \to S^{-1}B$ the homomorphism corresponding to ρ.*

(a) For every B-module M there exists a unique $S^{-1}A$-isomorphism

$$i : S^{-1}\rho_*(M) \to \tilde{\rho}_*(S^{-1}M)$$

(b) For every A-module M, there exists a unique isomorphism

$$j : (S^{-1}M) \otimes_{S^{-1}A} (S^{-1}B) \to S^{-1}(M \otimes_A B).$$

Proof. If we consider $S^{-1}M$ as an A-module by means of the composite homomorphism $i_M^S \circ \rho$, the homotheties induced by the elements of S are bijective, hence there exists a unique homomorphism i. It is claer that i is surjective; moreover, if $m \in M$, $s \in S$ and $m/\rho(s) = 0$, then there exists $t \in S$ such that $\rho(t)m = 0$, and so $tm = 0$ in $\rho_*(M)$, hence $m/s = 0$ in $S^{-1}\rho_*(M)$.

For (b), as $(S^{-1}M) \otimes_{S^{-1}A} (S^{-1}B) = (M \otimes_A S^{-1}A) \otimes_{S^{-1}A} S^{-1}B$, we see

$$S^{-1}(M \otimes_A B) = (M \otimes_A B) \otimes_B (S^{-1}B)$$

the existence of j follows from the associativity of tensor products. □

10.3 Local rings and passing from local to global

10.3.1 Local rings

Proposition 10.3.1. *Let A be a ring and I the set of non-invertible elements of A. The set I is the union of the ideals of A which are distinct from A. Moreover, the following conditions are equivalent:*

(i) I is an ideal.

(ii) The set of ideals of A distinct from A has a greatest element.

(iii) A has a unique maximal ideal.

Proof. The relation $x \in I$ is equivalent to $1 \notin xA$ and hence $xA \neq A$. If $\mathfrak{a}$ is an ideal of A distinct from A and $x \in \mathfrak{a}$, then $xA \subseteq \mathfrak{a}$, hence $xA \neq A$ and $x \in I$. Hence every ideal of A distinct from A is contained in I and every element $x \in I$ belongs to a principal ideal $xA \neq A$. This proves the first assertion, which immediately implies the equivalence of (i), (ii) and (iii). □

A ring A is called a **local ring** if it satisfies the equivalent conditions of Proposition 10.3.1. The quotient of A by its Jacobson radical (which is then the unique maximal ideal of A) is called the **residue field** of A. Let A, B be two local rings and $\mathfrak{m}$, $\mathfrak{n}$ their respective maximal ideals. A homomorphism $\rho : A \to B$ is called local if $\rho(\mathfrak{m}) \subseteq \mathfrak{n}$. Note that this amounts to saying that $\rho^{-1}(\mathfrak{n}) = \mathfrak{n}$, for $\rho^{-1}(\mathfrak{n})$ is then an ideal containing $\mathfrak{m}$ and not containing 1 and hence equal to $\mathfrak{m}$. Taking quotients, we then derive canonically from ρ an injective homomorphism $A/\mathfrak{m} \to B/\mathfrak{n}$ from the residue field of A to that of B.

Example 10.3.2 (Example of local rings).

(a) A field is a local ring. A ring which is reduced to 0 is not a local ring.

(b) Let A be a local ring and κ its residue field. The ring of formal power series $B = A[[X_1, \dots, X_n]]$ is a local ring, for the non-invertible elements of B are the formal power series whose constant terms are not invertible in A. The canonical injection of A into B is a local homomorphism and the corresponding injection of residue fields is an isomorphism.

(c) Let $\mathfrak{a}$ be an ideal of a ring A which is only contained in a single maximal ideal $\mathfrak{m}$. Then $A/\mathfrak{a}$ is a local ring with maximal ideal $\mathfrak{m}/\mathfrak{a}$ and residue field canonically isomorphic to $A/\mathfrak{m}$. This applies in particular to the case $\mathfrak{a} = \mathfrak{m}^n$, where $\mathfrak{m}$ is any maximal ideal of A (Corollary 10.1.3). If A itself is a local ring with maximal ideal $\mathfrak{m}$, then for every proper ideal $\mathfrak{a}$ of A, $A/\mathfrak{a}$ is a local ring, the canonical homomorphism $A \to A/\mathfrak{a}$ a local homomorphism and the corresponding homomorphism Of residue fields an isomorphism.

(d) Let X be a topological space, x_0 a point of X and A the ring of germs at the point x_0 of real-valued functions continuous in a neighbourhood of x_0. Clearly, for the germ at x_0 of a continuous function f to be invertible in A, it is necessary and sufficient that $f(x_0) \neq 0$, since this implies that $f(x) \neq 0$ in a neighbourhood of x_0. The ring A is therefore a local ring whose maximal ideal $\mathfrak{m}$ is the set of germs of functions which are zero at x_0. Taking quotients, the mapping $f \mapsto f(x_0)$ of A to $\mathbb{R}$ gives an isomorphism of the residue field $A/\mathfrak{m}$ onto $\mathbb{R}$.

Proposition 10.3.3. *Let A be a ring and $\mathfrak{p}$ a prime ideal of A. The ring $A_\mathfrak{p}$ is local, and its maximal ideal is the ideal $\mathfrak{p}A_\mathfrak{p} = \mathfrak{p}_\mathfrak{p}$, generated by the canonical image of $\mathfrak{p}$ in $A_\mathfrak{p}$. Its residue field is canonically isomorphic to the field of fractions of $A/\mathfrak{p}$.*

Proof. Let $S = A - \mathfrak{p}$ and $i_A^S : A \to A_\mathfrak{p}$ be the canonical homomorphism; the hypothesis that $\mathfrak{p}$ is prime implies that $\mathfrak{p}$ is saturated with respect to S, hence $(i_A^S)^{-1}(\mathfrak{p}A_\mathfrak{p}) = \mathfrak{p}$ and, as the ideals of A not meeting S are those contained in $\mathfrak{p}$, the first two assertions are special cases of Proposition 10.2.36. Moreover, if π is the canonical homomorphism $A \to A/\mathfrak{p}$, $\pi(S)$ is the set of nonzero elements of the integral domain $A/\mathfrak{p}$ and hence the last assertion is a special case of Proposition 10.2.39. □

Let A be a ring and $\mathfrak{p}$ a prime ideal of A. The ring $A_\mathfrak{p}$ is called the local ring of A at $\mathfrak{p}$, or the local ring of $\mathfrak{p}$, when there is no ambiguity. If A is a local ring and $\mathfrak{m}$ its maximal ideal, the elements of $A - \mathfrak{m}$ are invertible and hence $A_\mathfrak{m}$ is canonically identified with A.

Example 10.3.4.

(a) Let p be a prime number. The local ring $\mathbb{Z}_\mathfrak{p}$ is the set of rational numbers a/b, where a, b are rational integers with b prime to p. The residue field of $\mathbb{Z}_\mathfrak{p}$ is isomorphic to the prime field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

(b) Let V be an affine algebraic variety, A the ring of regular functions on V, W an irreducible subvariety of V and $\mathfrak{p}$ the (necessarily prime) ideal of A consisting of the functions which are zero at every point of W. The ring $A_\mathfrak{p}$ is called the local ring of W on V.

Proposition 10.3.5. *Let A, B be two rings, $\rho : A \to B$ a homomorphism, $\mathfrak{q}$ a prime ideal of B and $\mathfrak{p} = \mathfrak{q}^c$. Then there is a canonical homomorphism $\rho_\mathfrak{q} : A_\mathfrak{p} \to B_\mathfrak{q}$ which is local.*

Proof. As $\rho(A - \mathfrak{p}) \subseteq B - \mathfrak{q}$, a canonical homomorphism $\rho_\mathfrak{q} : A_\mathfrak{p} \to B_\mathfrak{q}$ is derived from ρ, and is immediate that $\rho_\mathfrak{q}(\mathfrak{p}A_\mathfrak{p}) \subseteq \mathfrak{q}B_\mathfrak{q}$, hence $\rho_\mathfrak{q}$ is local. □

10.3.2 Modules over a local ring

Proposition 10.3.6. *Let A be a ring, $\mathfrak{m}$ an ideal of A contained in the Jacobson radical of A and M an A-module. Suppose that one of the following conditions holds:*

(a) M is finitely generated;

(b) $\mathfrak{m}$ is nilpotent.

Then the relation $(A/\mathfrak{m}) \otimes_A M = 0$ implies $M = 0$.

Proof. The assertion with respect to hypothesis (a) is precisely Nakayama's Lemma. On the other hand, the relation $(A/\mathfrak{m}) \otimes_A M = 0$ is equivalent to $M = \mathfrak{m}M$ and hence implies $M = \mathfrak{m}^n M$ for every integer $n > 0$; whence the assertion with respect to hypothesis (b). □

Corollary 10.3.7. *Let A be a ring, $\mathfrak{m}$ an ideal of A contained in the Jacobson radical of A, M and N two A-modules and $\phi : M \to N$ an A-linear mapping. If N is finitely generated or $\mathfrak{m}$ is nilpotent and*

$$1 \otimes \phi : (A/\mathfrak{m}) \otimes_A M \to (A/\mathfrak{m}) \otimes_A N$$

is surjective, then ϕ is surjective.

Proof. Since $(A/\mathfrak{m}) \otimes_A (N/\phi(M))$ is canonically isomorphic to $((A/\mathfrak{m}) \otimes_A M)/\mathrm{im}(1 \otimes \phi)$, the hypothesis implies $(A/\mathfrak{m}) \otimes_A (N/\phi(M)) = 0$, hence $N/\phi(M) = 0$ by Proposition 10.3.6. □

Corollary 10.3.8. *Let A be a ring, $\mathfrak{m}$ an ideal of A contained in the Jacobson radical of A, M an A-module and $(x_i)_{i \in I}$ a family of elements of M. If M is finitely generated or $\mathfrak{m}$ is nilpotent and the elements $1 \otimes x_i$ generate the $(A/\mathfrak{m})$-module $M/\mathfrak{m}M$, then the x_i generate M.*

Proposition 10.3.9. *Let A be a ring, $\mathfrak{m}$ an ideal of A contained in the Jacobson radical of A and M an A-module. Suppose that one of the following conditions holds:*

(a) M is finitely presented;

(b) $\mathfrak{m}$ is nilpotent.

Then, if $M/\mathfrak{m}M$ is a free $(A/\mathfrak{m})$-module and the canonical homomorphism from $\mathfrak{m} \otimes_A M$ to M is injective, then M is a free A-module. To be precise, if $(x_i)_{i\in I}$ is a family of elements of M such that $(1 \otimes x_i)$ is a basis of the $(A/\mathfrak{m})$-module $M/\mathfrak{m}M$, then (x_i) is a basis of M.

Proof. We already know that the x_i generate M (Corollary 10.3.8). We shall see that they are linearly independent over A. To this end, let us consider the free A-module $L = A^I$. Let (e_i) be its canonical basis and $\phi : A^I \to M$ the A-linear mapping such that $\phi(e_i) = x_i$ for all $i \in I$. If R is the kernel of ϕ, we shall prove that that $\mathfrak{m}R = R$. Let j be the canonical injection $R \to L$; then there is a commutative diagram

$$\begin{tikzcd}
 & \mathfrak{m} \otimes R \arrow[r, "1\otimes j"] \arrow[d, "\alpha"] & \mathfrak{m} \otimes L \arrow[r, "1\otimes\phi"] \arrow[d, "\beta"] & \mathfrak{m} \otimes M \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & R \arrow[r, "j"] & L \arrow[r, "\phi"] & M \arrow[r] & 0
\end{tikzcd}$$

in which the two rows are exact. By hypothesis we have $\ker \gamma = 0$, hence by snake lemma, there is an exact sequence

$$0 \longrightarrow \operatorname{coker} \alpha \longrightarrow \operatorname{coker} \beta \longrightarrow \operatorname{coker} \gamma \longrightarrow 0$$

Now $\operatorname{coker} \beta = (A/\mathfrak{m}) \otimes L$ and $\operatorname{coker} \gamma = (A/\mathfrak{m}) \otimes M$. Since $(1 \otimes e_i)$ is a basis for $(A/\mathfrak{m}) \otimes L$ and its image in $(A/\mathfrak{m}) \otimes M$ is a basis for $(A/\mathfrak{m}) \otimes M$, we see $\operatorname{coker} \alpha = 0$, whence $\mathfrak{m}R = R$.

Under hypothesis (a), $(A/\mathfrak{m}) \otimes_A M$ is a finitely generated module, hence I is necessarily finite and R is a finitely generated A-module. Then by Proposition 10.3.6 we have $R = 0$. Similarly, under hypothesis (b) we also have $R = 0$, so the proof is completed. □

Corollary 10.3.10. *Let A be a local ring and $\mathfrak{m}$ its maximal ideal. For a family (y_i) of elements of M to be a basis of a direct factor of M, it is necessary and sufficient that the family $(1 \otimes y_i)$ be free in $M/\mathfrak{m}M$.*

Proof. If this condition holds, it can be assumed that (x_i) is a subfamily of a family (x_i) of elements of M such that $(1 \otimes x_i)$ is a basis of $M/\mathfrak{m}M$ and Proposition 10.3.9 then proves that (x_i) is a basis of M. □

Corollary 10.3.11. *Let A be a local ring, $\mathfrak{m}$ its maximal ideal and M an A-module. Suppose that one of the following conditions holds:*

(a) M is finitely presented;

(b) $\mathfrak{m}$ is nilpotent.

Then the following properties are equivalent:

(i) M is free;

(ii) M is projective;

(iii) M is flat;

(iv) the canonical homomorphism $\mathfrak{m} \otimes_A M \longrightarrow M$ *is injective;*

(v) $\mathrm{Tor}_A^1(A/\mathfrak{m}, M) = 0$.

Proof. The implications $(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (iv)$ are immediate, and we know that (iv) is equivalent to (v). As $A/\mathfrak{m}$ is a field, $(A/\mathfrak{m}) \otimes_A M$ is a free $(A/\mathfrak{m})$-module and Proposition 10.3.9 shows that (iv) implies (i). □

Proposition 10.3.12. *Let A be a local ring and $\mathfrak{m}$ its maximal radical. Let M and N be two finitely generated free A-modules and $\phi : M \longrightarrow N$ a homomorphism. The following properties are equivalent:*

(i) ϕ is an isomorphism of M onto a direct factor of N;

(ii) $1 \otimes \phi : (A/\mathfrak{m}) \otimes_A M \longrightarrow (A/\mathfrak{m}) \otimes_A N$ *is injective;*

(iii) ϕ is injective and $\operatorname{coker} \phi$ *is a free A-module;*

(iv) the transpose homomorphism $\phi^T : N^* \longrightarrow M^*$ is surjective.

Proof. We know that, if $N/\phi(M)$ is free, then $\phi(M)$ is a direct factor of N, hence (iii) implies (i). Conversely, (i) implies that coker ϕ, isomorphic to a complement of $\phi(M)$ in N, is a finitely generated projective A-module and a fortiori finitely presented, hence this module is free by Corollary 10.3.11 and thus (i) implies (iii).

On the other hand, (i) obviously implies (ii). For simplicity we write $\tilde{M} = (A/\mathfrak{m}) \otimes_A M$ and $\tilde{N} = (A/\mathfrak{m}) \otimes_A N$. As M and N are finitely generated, the duals $\tilde{M}^*$ and $\tilde{N}^*$ of the $(A/\mathfrak{m})$-modules $\tilde{M}$ and $\tilde{N}$ are canonically identified with $M^* \otimes_A (A/\mathfrak{m})$ and $N^* \otimes_A (A/\mathfrak{m})$ and $(1 \otimes \phi)^T$ with $1 \otimes \phi^T$. As $\tilde{M}$ and $\tilde{N}$ are vector spaces over the field $A/\mathfrak{m}$, the hypothesis that $1 \otimes \phi$ is injective implies that $(1 \otimes \phi)^T$ is surjective. Corollary 10.3.7 then shows that ϕ^T is surjective and we have thus proved that (ii) implies (iv).

Finally we show that (iv) implies (i). Suppose that ϕ^T is surjective. As M^* is free, there exists a homomorphism $\psi^T : M^* \longrightarrow N^*$ such that $\phi^T \circ \phi^T = \mathrm{id}$. As M and N are free and finitely generated, there exists a homomorphism $\psi : N \longrightarrow M$ such that the dual of ψ is ψ^T, whence

$$\mathrm{id}_M^T = \mathrm{id}_{M^*} = \phi^T \circ \psi^T = (\psi \circ \phi)^T$$

whence $\psi \circ \phi = \mathrm{id}$. This proves that ϕ is an isomorphism of M onto a submodule which is a direct factor of N. □

Corollary 10.3.13. *Under the hypotheses of Proposition 10.3.12 the following properties are equivalent:*

(i) ϕ is an isomorphism of M onto N;

(ii) M and N have the same rank;

(iii) $1 \otimes \phi : (A/\mathfrak{m}) \otimes_A M \longrightarrow (A/\mathfrak{m}) \otimes_A N$ *is bijective.*

Proof. Clearly (i) implies (ii); (ii) implies that $1 \otimes \phi$ is surjective; moreover the hypothesis that M and N have the same rank implies that so do the vector spaces $(A/\mathfrak{m}) \otimes_A M$ and $(A/\mathfrak{m}) \otimes_A N$ over $A/\mathfrak{m}$, hence $1 \otimes \phi$ is bijective and (ii) implies (iii). Finally, condition (iii) implies, by Proposition 10.3.12, that N is the direct sum of $\phi(M)$ and a free submodule P and ϕ is an isomorphism of M onto $\phi(M)$. If $P \neq 0$, then $(A/\mathfrak{m}) \otimes_A P \neq 0$ and $1 \otimes \phi$ would not be sutjcctive; hence (iii) implies (i). □

Proposition 10.3.14. *Let A be a reduced local ring, $\mathfrak{m}$ its maximal ideal, $(\mathfrak{p}_i)_{i\in I}$ the family of minimal prime ideals of A, K_i the field of fractions of $A/\mathfrak{p}_i$ and M a finitely generated A-module. For M to be free it is necessary and sufficient that*

$$[(A/\mathfrak{m})\otimes_A : (A/\mathfrak{m})] = [K_i \otimes_A M : K] \tag{3.2.1}$$

for all $i \in I$.

Proof. If M is free, clearly the two sides of (3.2.1) are equal to the rank of M for all $i \in I$. Suppose now that the condition is satisfied and denote by n the common value of the two sides of (3.2.1). By Corollary 10.3.8 M has a system of n generators $x_1, \dots, x_n$. Suppose first that A is an integral domain, in which case $\mathfrak{p}_i = 0$ for all $i \in I$. The elements $(1 \otimes x_i)$ generate the vector space $K \otimes M$ over the field of fractions K of A. But as by hypothesis this space is of dimension n over K, the elements $1 \otimes x_i$ are linearly independent over K. It follows that the x_i are linearly independent over A and hence form a basis of M.

Passing to the general case, there exists a surjective homomorphism η from $L = A^n$ onto M. Consider the commutative diagram

$$\begin{tikzcd} L \arrow[r, "\eta"] \arrow[d, "\pi_L"] & M \arrow[d, "\pi_M"] \\ \prod_i((A/\mathfrak{p}_i) \otimes L) \arrow[r, "\tilde{\eta}"] & \prod_i((A/\mathfrak{p}_i) \otimes M) \end{tikzcd}$$

where ϕ_L (resp. π_M) is the mapping $x \mapsto (\phi_i(x))$ (resp. $y \mapsto (\psi_i(y))$), with $\phi_i : L \to (A/\mathfrak{p}_i) \otimes L$ (resp. $\psi_i : M \to (A/\mathfrak{p}_i) \otimes M$) being the canonical mapping, and $\tilde{\eta}$ is the product of the $1_{A/\mathfrak{p}_i} \otimes \eta$. Then as

$$((A/\mathfrak{p}_i)/(\mathfrak{m}/\mathfrak{p}_i)) \otimes_{A/\mathfrak{p}_i} ((A/\mathfrak{p}_i) \otimes_A M) = (A/m) \otimes_A M$$

and $A/\mathfrak{p}_i$ is a local integral domain, it follows from the first part of the argument that each of the M, $1_{A/\mathfrak{p}_i} \otimes \eta$ is an isomorphism; then so is $\tilde{\eta}$. On the other hand, as A is reduced, $\bigcap_i \mathfrak{p}_i = (0)$ whence $\bigcap_i \mathfrak{p}_i L = (0)$ since L is free. As this shows that π_L is injective, it follows that $\tilde{\eta} \circ \pi_L$ is injective, hence η is injective and, as η is sutjective by definition, this shows that M is free. □

10.3.3 Passing from local to global

Proposition 10.3.15. *Let A be a ring, $\mathfrak{m}$ a maximal ideal of A and M an A-module. If there exists an ideal $\mathfrak{a}$ of A such that $\mathfrak{m}$ is the only maximal ideal of A containing $\mathfrak{a}$ and $\mathfrak{a}M = 0$, then the canonical homomorphism $M \to M_\mathfrak{m}$ is bijective.*

Proof. By hypothesis $A/\mathfrak{a}$ is then a local ring with maximal ideal $\mathfrak{m}/\mathfrak{a}$; M can be considered as an $(A/\mathfrak{a})$-module. For all $s \in A - \mathfrak{m}$ the canonical image of s in $A/\mathfrak{a}$ is invertible, hence the homothety $x \mapsto sx$ of M is bijective from the definition of $M_\mathfrak{m}$ as the solution of a universal problem, whence the proposition. □

In particular, if there exists $k > 0$ such that $\mathfrak{m}^k M = 0$, the homomorphism $M \mapsto M_\mathfrak{m}$ is bijective.

Proposition 10.3.16. *Let A be a ring, $\mathfrak{m}$ a maximal ideal of A, M an A-module and $k > 0$ an integer. The canonical homomorphism $M \to M_\mathfrak{m}/\mathfrak{m}^k M_\mathfrak{m}$ is surjectice, has kernel $\mathfrak{m}^k M$ and defines an isomorphism of $M/\mathfrak{m}^k M$ onto $M_\mathfrak{m}/\mathfrak{m}^k M_\mathfrak{m}$.*

Proof. It follows from Proposition 10.3.15 the homomorphism $M/\mathfrak{m}^k M \to (M/\mathfrak{m}^k M)_\mathfrak{m}$ is bijective. On the other hand $(M/\mathfrak{m}^k M)_\mathfrak{m}$ is canonically identified with $M_\mathfrak{m}/(\mathfrak{m}^k M)_\mathfrak{m}$ and hence $(\mathfrak{m}^k M)_\mathfrak{m} = \mathfrak{m}^k M_\mathfrak{m}$, whence there is an isomorphism of $M/\mathfrak{m}^k M$ onto $M_\mathfrak{m}/\mathfrak{m}^k M_\mathfrak{m}$ which maps the class of an element $x \in M$ to the class of $x/1$. □

Corollary 10.3.17. *Let A be a ring, $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ distinct maximal ideals of A, M an A-module and $k_1, \ldots, k_n$ positive integers. The canonical homomorphism from M to $\bigoplus_{i=1}^n M_{\mathfrak{m}_i}/\mathfrak{m}_i^{k_i} M_{\mathfrak{m}_i}$ is surjective and its kernel is $(\bigcap_{i=1}^n \mathfrak{m}_i^{k_i})M$.*

Proposition 10.3.18. *Let A be a commutative ring, and let M be an A-module. The following are equivalent*

(a) $M = 0$.

(b) $M_\mathfrak{p} = 0$ *for every prime ideal* $\mathfrak{p}$.

(c) $M_\mathfrak{m} = 0$ *for every maximal ideal* $\mathfrak{m}$.

Proof. Clearly $(a) \Rightarrow (b) \Rightarrow (c)$. So we only need to show $(c) \Rightarrow (a)$. Assume $M_\mathfrak{m} = 0$ for every maximal ideal $\mathfrak{m}$ but $M \neq 0$. Let x be a non-zero element of M, consider the ideal $\mathrm{Ann}(m)$: It is proper hence contained in a maxiaml ideal $\mathfrak{m}$. Consider the module $M_\mathfrak{m}$. We must have $x/1 = 0$ since $M_\mathfrak{m} = 0$, hence x is killed by some element in $A - \mathfrak{m}$. But this is impossible since $\mathrm{Ann}(x) \subseteq \mathfrak{m}$. □

Proposition 10.3.19. *Let $\phi : M \to N$ be an A-module homomorphism. Then the following are equivalent:*

(a) ϕ *is injective.*

(b) $\phi_\mathfrak{p} : M_\mathfrak{p} \to N_\mathfrak{p}$ *is injective for each prime ideal* $\mathfrak{p}$ *of* A.

(c) $\phi_\mathfrak{m} : M_\mathfrak{m} \to N_\mathfrak{m}$ *is injective for each maximal ideal* $\mathfrak{m}$ *of* A.

Similarly with injective replaced by surjective throughout.

Proof. Since localization is exact, we see $(a) \Rightarrow (b) \Rightarrow (c)$. Now assume (c) and let $M' = \ker \phi$, then the sequence $0 \to M' \to M \to N$ is exact, hence $0 \to M'_\mathfrak{m} \to M_\mathfrak{m} \to N_\mathfrak{m}$ is exact and therefore $M'_\mathfrak{m} \cong \ker \phi_\mathfrak{m} = 0$ by assumption. Hence $M' = 0$ by Proposition 10.3.18, so ϕ is injective. For the other part of the proposition, just reverse all the arrows. □

Corollary 10.3.20. *The localization functor is faithfully exact in the following sense: let A be a commutative ring, and let*

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0 \tag{3.3.1}$$

be a sequence of A-modules. Then (3.3.1) is exact if and only if the induced sequence of $A_\mathfrak{p}$-modules

$$0 \longrightarrow A_\mathfrak{p} \longrightarrow B_\mathfrak{p} \longrightarrow C_\mathfrak{p} \longrightarrow 0$$

is exact for every prime ideal $\mathfrak{p}$ of A, if and only if it is exact for every maximal ideal $\mathfrak{m}$.

Corollary 10.3.21. *Let M be an A-module, N a submodule of M and x an element of M. For $x \in N$, it is necessary and sufficient that, for any maximal ideal $\mathfrak{m}$, the canonical image of x in $M_\mathfrak{m}$ belong to $N_\mathfrak{m}$.*

Corollary 10.3.22. *Let M be an A-module and, for all maximal ideal $\mathfrak{m}$, let $\phi_{\mathfrak{m}} : M \to M_{\mathfrak{m}}$ be the canonical map. The homomorphism $x \mapsto (\phi_{\mathfrak{m}}(x))$ of M to $\bigoplus_{\mathfrak{m}} M_{\mathfrak{m}}$ is injective.*

Corollary 10.3.23. *Let A be an integral domain, K its field of fractions and M a torsion free A-module such that M is canonically identified with a sub-A-module of $K \otimes_A M$. Then, for any maximal ideal $\mathfrak{m}$, $M_{\mathfrak{m}}$ is canonically identified with a sub-A-module of $K \otimes_A M$ and $M = \bigcap_{\mathfrak{m}} M_{\mathfrak{m}}$.*

Proof. As M is identified with a submodule of $K \otimes_A M$, $M_{\mathfrak{m}}$ is identified with a sub-$A_{\mathfrak{m}}$-module of $(K \otimes_A M)_{\mathfrak{m}} = K_{\mathfrak{m}} \otimes_A M = K \otimes_A M$, so $M_{\mathfrak{m}}$ is torsion-free. Moreover, the commutativity of the diagram

$$\begin{tikzcd} M \arrow[r] \arrow[d] & K \otimes_A M \arrow[d] \\ M_{\mathfrak{m}} \arrow[r] & (K \otimes_A M) \end{tikzcd}$$

proves that the canonical mapping $M \mapsto M_{\mathfrak{m}}$ is injective. The corollary then follows from Corollary 10.3.21 applied to the A-module $K \otimes_A M$ and its submodule M. □

Proposition 10.3.24. *For any A-module M, the following statements are equivalent:*

(a) M is flat.

(b) $M_{\mathfrak{p}}$ is flat for each prime ideal $\mathfrak{p}$ of A.

(c) $M_{\mathfrak{m}}$ is flat for each maximal ideal $\mathfrak{m}$ of A.

Proof. By Corollary 10.3.20, the sequence

$$0 \longrightarrow A \otimes M \longrightarrow B \otimes M \longrightarrow C \otimes M \longrightarrow 0$$

is exact if and only if

$$0 \longrightarrow (A \otimes M)_{\mathfrak{p}} \longrightarrow (B \otimes M)_{\mathfrak{p}} \longrightarrow (C \otimes M)_{\mathfrak{p}} \longrightarrow 0$$

is exact for any prime ideal $\mathfrak{p}$, iff for any maximal ideal $\mathfrak{m}$. From Proposition 10.2.44, we have

$$(A \otimes_A M)_{\mathfrak{p}} \simeq A_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} M_{\mathfrak{p}}$$

so the claim follows. □

Proposition 10.3.25. *Let A be an integral domain with field of fractions K. We consider any ring of fractions of A as a subring of K. Then in this sense we have*

$$A = \bigcap_{\mathfrak{p} \in \mathrm{Spec}(A)} A_{\mathfrak{p}} = \bigcap_{\mathfrak{m} \in \mathrm{Max}(A)} A_{\mathfrak{m}}$$

Proof. For $x \in K$ the set $I = \{a \in A \mid ax \in A\}$ is an ideal of A. Now it is easy to see that $x \in A_{\mathfrak{p}}$ if and only if $I \cap (A - \mathfrak{p}) \neq \varnothing$, which is equivalenct to that $I \not\subseteq \mathfrak{p}$, so if $x \in A_{\mathfrak{m}}$ for every maximal ideal $\mathfrak{m}$ then I is not contained in any maximal ideal of A, whence $1 \in I$, that is, $x \in A$. □

Corollary 10.3.26. *Let A be an integral domain and $f \in A$, then $A_f = \bigcap_{f \notin \mathfrak{p}} A_{\mathfrak{p}}$.*

Proof. If A is an integral domain, then A_f is also a domain. Now $\mathrm{Spec}(A_f) = \{\mathfrak{p} \in \mathrm{Spec}(A) \mid f \notin \mathfrak{p}\}$, so by Proposition 10.3.25 we get the claim. □

10.4 The spectrum of a ring

10.4.1 The space Spec(A)

Let A be a ring. The **spectrum of A** is the set of prime ideals of A. It is usually denoted Spec(A). To avoid confusion, we will sometimes write $[\mathfrak{p}]$ for the point of Spec(A) corresponding to the prime $\mathfrak{p}$ of A. Of course, the zero ideal (0) is a prime if A is a domain.

Example 10.4.1. Here are several examples.

(a) Prime ideals in $\mathbb{Z}$ is the form (p) with p prime, and every set $\{(p)\} = V(p)$ is closed. Hence Spec($\mathbb{Z}$) is a line, with one closed point for each prime number in $\mathbb{Z}$, and one non-closed point corresponding to the ideal (0).

(b) As $\mathbb{R}$ is a field, Spec($\mathbb{R}$) consists of a single point, corresponding to the ideal (0).

(c) The maximal ideals of the ring $\mathbb{C}[X]$ are all of the form $(x - a)$ for $a \in \mathbb{C}$. The only non-maximal prime ideal of $\mathbb{C}[X]$ is (0). Thus Spec($\mathbb{C}[X]$) is the complex plane together with a single non-closed point, corresponding to (0).

(d) There are two types of maximal ideals in $\mathbb{R}[X]$, those generated by a polynomial of degree one, and those generated by a polynomial of degree two. The degree one maximal ideals are all of the form $(x - a)$ for $a \in \mathbb{R}$. The maximal ideals of degree two correspond to complex conjugate pairs of elements of $\mathbb{C} - \mathbb{R}$. There is only one non-maximal prime ideal, (0). Therefore Spec($\mathbb{R}[X]$) is the upper-half plane, together with a single non-closed point.

Each element $f \in A$ defines a function, which we also write as f, on the space Spec(A): if $x = \mathfrak{p} \in X = \mathrm{Spec}(A)$, we denote by $\kappa(x)$ or $\kappa(\mathfrak{p})$ the quotient field of the integral domain $A/\mathfrak{p}$, called the **residue field** of X at x, and we define $f(x) \in \kappa(x)$ to be the image of f via the canonical maps

$$A \to A/\mathfrak{p} \to \kappa(\mathfrak{p}).$$

The functions induced by elements of A are called the **regular functions** on Spec(A).

Example 10.4.2. Consider the ring of polynomials $\mathbb{C}[X]$, and let $p(x)$ be a polynomial. If $\alpha \in \mathbb{C}$ is a number, then $(x - \alpha)$ is a prime of $\mathbb{C}[X]$, and in fact is maximal. So $\kappa(x - \alpha)$ is just the field $\mathbb{C}$, and the value of $p(x)$ at the point $(x - \alpha) \in \mathrm{Spec}(\mathbb{C}[X])$ is the number $p(\alpha)$.

More generally, if A is the coordinate ring of an affine variety V over an algebraically closed field K and $\mathfrak{m}$ is the maximal ideal corresponding to a point $x \in V$ in the usual sense, then $\kappa(x) = K$ and $f(x)$ is the value of f at x in the usual sense.

In general, the function f has values in fields that vary from point to point. Moreover, f is not necessarily determined by the values of this function. For example, if K is a field, the ring $A = K[X]/(x^2)$ has only one prime ideal, which is (x); and thus the element $x \in A$, albeit nonzero, induces a function whose value is 0 at every point of Spec(A).

By using regular functions, we make Spec(A) into a topological space. For each subset $S \subseteq A$, let

$$V(S) = \{x \in \mathrm{Spec}(A) : f(x) = 0 \text{ for all } f \in S\} = \{\mathfrak{p} \in \mathrm{Spec}(A) : \mathfrak{p} \supseteq S\}.$$

The impulse behind this definition is to make each $f \in A$ behave as much like a continuous function as possible. Of course the fields $\kappa(x)$ have no topology, and since they vary with x the usual notion of continuity makes no sense. But at least they all contain an element called zero, so one can speak of the locus of points in $\operatorname{Spec}(A)$ on which f is zero; and if f is to be like a continuous function, this locus should be closed. Since intersections of closed sets must be closed, we are led immediately to the definition above: $V(S)$ is just the intersection of the loci where the elements of S vanish.

Proposition 10.4.3. *Let A be a ring.*

(a) If $\mathfrak{a}$ is the ideal generated by E, then $V(E) = V(\mathfrak{a}) = V(\sqrt{\mathfrak{a}})$.

(b) Let $\mathfrak{a}, \mathfrak{b}$ be ideals of A, then $V(\mathfrak{a}) \subseteq V(\mathfrak{b})$ iff $\mathfrak{b} \subseteq \sqrt{\mathfrak{a}}$.

(c) If $(E_i)_{i\in I}$ is any family of subsets of A, then

$$V\Big(\bigcup_{i\in I} E_i\Big) = \bigcap_{i\in I} V(E_i).$$

(d) For any ideals $\mathfrak{a}, \mathfrak{b}$ of A, we have $V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}\mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$.

*In particular, the sets $V(E)$ satisfy the axioms for closed sets in a topological space. The resulting topology is called the **Zariski topology** on* $\operatorname{Spec}(A)$.

Proof. We only prove (d). By Proposition 10.1.23, we have

$$V(\mathfrak{a}\mathfrak{b}) = V(\sqrt{\mathfrak{a}\mathfrak{b}}) = V(\sqrt{\mathfrak{a} \cap \mathfrak{b}}) = V(\mathfrak{a} \cap \mathfrak{b}).$$

Now we only need to prove $V(\mathfrak{a}\cap\mathfrak{b}) = V(\mathfrak{a})\cup V(\mathfrak{b})$. Since $\mathfrak{a}\cap\mathfrak{b}$ is contained in $\mathfrak{a}$ and $\mathfrak{b}$, for either $\mathfrak{a} \subseteq \mathfrak{p}$ or $\mathfrak{b} \subseteq \mathfrak{p}$ we have $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{p}$, whence $V(\mathfrak{a}) \cup V(\mathfrak{b}) \subseteq V(\mathfrak{a} \cap \mathfrak{b})$. Conversely, let $\mathfrak{p} \in V(\mathfrak{a} \cap \mathfrak{b})$ so that $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{p}$. By Proposition 10.1.5, $\mathfrak{a} \subseteq \mathfrak{p}$ or $\mathfrak{a} \subseteq \mathfrak{p}$, so $\mathfrak{p} \in V(\mathfrak{a}) \cup V(\mathfrak{b})$. □

Let X be the prime spectrum of a ring A; for all $f \in A$, let us denote by X_f the set of prime ideals of A not containing f. Then $X_f = X - V(f)$ and X_f is therefore an open set, called the **distinguished** (or **standard**) **open subsets** of X. By Proposition 10.4.3, every closed subset of X is an intersection of closed sets of the form $V(f)$ and hence the X_f form a base of the spectral topology on X.

Proposition 10.4.4. *Ler A be a ring, $f, g \in A$ and $X = \operatorname{Spec}(A)$.*

(a) $D(f) = \varnothing$ iff f is nilpotent and $D(f) = X$ iff f is a unit.

(b) $D(f) = D(g)$ iff $\sqrt{(f)} = \sqrt{(g)}$.

(c) $D(f) \cap D(g) = D(fg)$.

(d) If $\mathfrak{a} \subseteq A$ is an ideal and $\mathfrak{p}$ is a prime of A with $\mathfrak{p} \notin V(\mathfrak{a})$, then there exists an $f \in A$ such that $\mathfrak{p} \in D(f)$ and $D(f) \cap V(I) = \varnothing$.

(e) If $(f_i)_{i\in A}$ is a family of elements in A, then $\bigcup_i D(f_i) = X - V(\{f_i\})$.

Proof. Part (a), (b) and (c) are immediate from the definition of $D(f)$ and Proposition 10.4.3. Now if $\mathfrak{p} \notin V(I)$, then there exists $f \in A$ such that $f \in \mathfrak{a} - \mathfrak{p}$. Then $f \notin \mathfrak{p}$ so that $\mathfrak{p} \in D(f)$. Also, if $\mathfrak{q} \in D(f)$ then $f \notin \mathfrak{q}$ and thus $\mathfrak{a}$ is not contained in $\mathfrak{q}$, which means $D(f) \cap V(\mathfrak{a}) = \varnothing$. This proves (d).

Finally, for (e) we note that

$$\bigcup_{i\in I} D(f_i) = \bigcup_{i\in I}(X - V(f_i)) = X - \bigcap_{i\in I} V(f_i) = X - V\Big(\bigcup_{i\in I}\{f_i\}\Big).$$

This completes the proof. □

For every subset Y of X, let us denote by $I(Y)$ the intersection of the prime ideals of A which belong to Y. Clearly $I(Y)$ is an ideal of A and the mapping $Y \mapsto I(Y)$ is decreasing with respect to inclusion in X and A, and we have

$$I\Big(\bigcup_{i\in I} Y_i\Big) = \bigcap_{i\in I} I(Y_i).$$

Proposition 10.4.5. *Let A be a ring, $\mathfrak{a}$ an ideal of A and Y a subset of $X = \operatorname{Spec}(A)$.*

(a) $V(\mathfrak{a})$ is closed in X and $I(Y)$ is a radical ideal of A.

(b) $I(V(\mathfrak{a}))$ is the radical of $\mathfrak{a}$ and $V(I(Y))$ is the closure of Y in X.

(c) If E is any subset of A and Y is any subset of X, then

$$V(E) = V(I(V(E))), \quad I(Y) = I(V(I(Y))).$$

(d) The mappings I and V define decreasing bijections, one of which is the inverse of the other, between the set of closed subsets of X and the set of radical ideals of A.

Proof. Assertion (a) and the first assertion of (b) follow from the definitions. If a closed set $V(E)$ (for some $E \subseteq A$) contains Y, then $E \subseteq \mathfrak{p}$ for every prime ideal $\mathfrak{p} \in Y$, whence $E \subseteq I(Y)$ and consequently $V(E) \supseteq V(I(Y))$. As $Y \subseteq V(I(Y))$, $V(I(Y))$ is then the smallest closed set of X containing Y, which completes the proof of (b). Finally, it follows from (b) that, if $\mathfrak{a}$ is a prime ideal equal to its radical, then $I(V(\mathfrak{a})) = \mathfrak{a}$ and that, if Y is closed in X, then $V(I(Y)) = Y$. This proves (d). □

Corollary 10.4.6. *For every family $(Y_i)_{i\in I}$ of closed subsets of X, $I(\bigcap_{i\in I} Y_i)$ is the radical of the sum of the ideals $I(Y_i)$.*

Proof. It follows from Proposition 10.4.5 that $I(\bigcap_{i\in I} Y_i)$ is the smallest ideal which is equal to its radical and contains all the $I(Y_i)$; this ideal then contains $\sum_{i\in I} I(Y_i)$ and therefore also the radical of it, whence the corollary. □

Corollary 10.4.7. *The space $X = \operatorname{Spec}(A)$ is Noetherian if A is a Noetherian ring.*

Proof. If A is Noetherian, every ascending chain of prime ideals is stable, whence every descending chain of irreducible closed sets is stable. In other words, $\operatorname{Spec}(A)$ is Noetherian. □

Remark 10.4.1. Note that a ring A can be non-Noetherian even though its spectrum is Noetherian. For example, consider the ring

$$A = k[x_1, x_2, \dots]/(x_1, x_2^2, x_3^3, \dots)$$

where k is a field. Then A is not Noetherian since the ideal

$$\mathfrak{m} = (x_1, x_2, x_3, \dots)/(x_1, x_2^2, x_3^3, \dots)$$

is not finitely generated. However, this is the unique prime ideal of A (in fact maximal), so $\operatorname{Spec}(A)$ is a singleton and hence Noetherian.

Corollary 10.4.8. *Let A be a ring. For a subset Y of $X = \operatorname{Spec}(A)$ to be irreducible, it is necessary and suficient that the ideal $I(Y)$ be prime.*

Proof. Writing $\mathfrak{p} = I(Y)$, we note that, for an element $f \in A$, the relation $f \in \mathfrak{p}$ is equivalent to $Y \subseteq V(f)$. Suppose that Y is irreducible and let f, g be elements of A such that $fg \in \mathfrak{p}$. Then

$$Y \subseteq V(fg) = V(f) \cup V(g).$$

as Y is irreducible and $V(f)$ and $V(g)$ are closed, $Y \subseteq V(f)$ or $Y \subseteq V(g)$, hence $f \in \mathfrak{p}$ or $g \in \mathfrak{p}$, which proves that $\mathfrak{p}$ is prime.

Suppose now that $\mathfrak{p}$ is prime; then $Y = V(\mathfrak{p})$ by Proposition 10.4.5 and, as $\mathfrak{p}$ is prime, $\mathfrak{p} = I(\{\mathfrak{p}\})$, whence $\overline{Y} = V(I(\{\mathfrak{p}\})) = \overline{\{\mathfrak{p}\}}$. As a set consisting of a single point is irreducible, Y is irreducible. □

Corollary 10.4.9. *For a ring A to be such that $X = \operatorname{Spec}(A)$ is irreducible, it is necessary and sufiicient that the quotient of A by its nilradical $\mathfrak{n}$ be an integral domain.*

Proof. By Proposition 10.4.5, $I(X)$ is the radical of the ideal (0), that is $\mathfrak{n}$. □

Remark 10.4.2. Note that a ring A can be non-Noetherian even through $\operatorname{Spec}(A)$ is Noetherian. For example, the ring $A = k[x_1, x_2, \dots]/(x_1^2, x_2^2, \dots)$ has a unique maximal ideal $\mathfrak{m} = (x_1, x_2, \dots)$, whence $\operatorname{Spec}(A)$ is a singleton and is Noetherian. But $\mathfrak{m}$ is not finitely generated, so A is not Noetherian.

Corollary 10.4.10. *The space $X = \operatorname{Spec}(A)$ is a Kolmogoroff space.*

Proof. If $\mathfrak{p}$ and $\mathfrak{q}$ are two different points of X, we have, either $\mathfrak{p} \not\subseteq \mathfrak{q}$ or $\mathfrak{q} \not\subseteq \mathfrak{p}$, hence one of the points $\mathfrak{p}$, $\mathfrak{q}$ does not belong to the closure of the other. □

Proposition 10.4.11. *Let A be a ring. The topology on $X = \operatorname{Spec}(A)$ has the following properties:*

(a) X is quasi-compact.

(b) X has a basis for the topology consisting of quasi-compact opens.

(c) The intersection of any two quasi-compact opens is quasi-compact.

Proof. It suffices to prove that any covering of $\mathrm{Spec}(A)$ by standard opens can be refined by a finite covering. Thus suppose that $\mathrm{Spec}(A) = \bigcup_i D(f_i)$ for a set of elements f_i of A. This means that $\bigcap_i V(f_i) = \varnothing$. According to Proposition 10.4.3 this means that $V(\{f_i\}_{i\in I}) = \varnothing$. Then the ideal generated by the f_i is the unit ideal of A. This means that we can write

$$1 = \sum_{i=1}^{n} a_i f_i.$$

It follows that $\mathrm{Spec}(A) = \bigcup_{i=1}^{n} D(f_i)$. Since $D(f) \cong \mathrm{Spec}(A_f)$, each standard open is quasi-compact, and so their intersection $D(f) \cap D(g) = D(fg)$ is also quasi-compact. □

Proposition 10.4.12. *Let A be a ring and $X = \mathrm{Spec}(A)$.*

(a) The irreducible closed subsets of X are exactly the subsets $V(\mathfrak{p})$, with $\mathfrak{p} \subseteq A$ a prime.

(b) The irreducible components of X are exactly the subsets $V(\mathfrak{p})$, with $\mathfrak{p} \subseteq A$ a minimal prime.

Proof. By Proposition 10.4.5 $V(\mathfrak{p}) = \overline{\{\mathfrak{p}\}}$ is the closure of a singleton and hence irreducible. conversely, let $V(\mathfrak{a}) \subseteq X$ with $\mathfrak{a}$ a radical ideal. If $\mathfrak{a}$ is not prime, then choose $a, b \in A$, $a, b \notin \mathfrak{a}$ with $ab \in \mathfrak{a}$. In this case $V(\mathfrak{a}, a) \cup V(\mathfrak{a}, b) = V(\mathfrak{a})$, but neither $V(\mathfrak{a}, b) = V(\mathfrak{a})$ nor $V(\mathfrak{a}, a) = V(\mathfrak{a})$ since $\sqrt{(\mathfrak{a}, a)} \neq \sqrt{\mathfrak{a}} = \mathfrak{a}$, $\sqrt{(\mathfrak{a}, b)} \neq \mathfrak{a}$. Hence $V(\mathfrak{a})$ is not irreducible. □

Corollary 10.4.13. *Let A be a ring, $X = \mathrm{Spec}(A)$, and $\mathfrak{p} \in X$.*

(a) The set of irreducible closed subsets of X containing $\mathfrak{p}$ is in one-to-one correspondence with primes $\mathfrak{q} \supseteq \mathfrak{p}$.

(b) The set of irreducible component of X containing $\mathfrak{p}$ is in one-to-one correspondence with minimal primes $\mathfrak{q} \supseteq \mathfrak{p}$.

Corollary 10.4.14. *The set of minimal prime ideals of a Noetherian ring A is finite.*

Proof. The spectrum of a Noetherian is a Noetherian topological space, hence has finitely many irreducible components. □

Proposition 10.4.15. *Let A be a ring and $\mathfrak{p}$ be a minimal prime of A. Let $V \subseteq \mathrm{Spec}(A)$ be a quasi-compact open not containing the point $\mathfrak{p}$. Then there exists an $f \in A$, $f \notin \mathfrak{p}$ such that $D(f) \cap V = \varnothing$.*

Proof. Since V is quasi-compact we may write $V = \bigcup_{i=1}^{n} D(g_i)$. Since $\mathfrak{p} \notin V$ we have $g_i \in \mathfrak{p}$ for all i. Since $\mathfrak{p}$ is minimal, we see $\mathfrak{n}(A_\mathfrak{p}) = \mathfrak{p}A_\mathfrak{p}$, so each g_i is nilpotent in $A_\mathfrak{p}$. Hence we can find an $f \in A$, $f \notin \mathfrak{p}$ such that $fg_i^{n_i} = 0$ for some $n_i > 0$. Then $D(f) \cap D(g_i) = D(fg_i^{n_i}) = \varnothing$, so this $D(f)$ works. □

Proposition 10.4.16. *Let A be a ring and $X = \mathrm{Spec}(A)$. Let U be an open subset of X, then U is dense in X if and only if U meets every irreducible components of X. In particular, for an element $f \in A$ to be such that $D(f)$ is dense in X, it is necessary and sufficient that f does not belong to any minimal prime ideal of A. Moreover, every open dense subset of X contains an open subset of the form $D(f)$ with f not a zero divisor.*

Proof. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be the minimal prime ideals of A and set $X_i = V(\mathfrak{p}_i)$. If $\mathfrak{p}_i \in U$ for all i, then $U \cap X_i \neq \varnothing$ so U is dense (in that for this direction we do not need to assume that X has finitely many irreducible components). Conversely, assume that U is dense and let $Z = \bigcup_{X_i \cap U \neq \varnothing} X_i$. Then Z is closed and contains U. But then $Z = X$ since U is dense, so there is no X_i such that $X_i \cap U = \varnothing$. In particular, since for an element $f \in A$, $D(f) \cap V(\mathfrak{p}_i) \neq \varnothing$ if and only if $f \notin \mathfrak{p}_i$, we see (f) is dense if and only if $f \notin \mathfrak{p}_i$ for all i.

On the other hand, if U is an open dense subset of X, the complement of U is of the form $V(\mathfrak{a})$, where $\mathfrak{a}$ is an ideal which is not contained in any of the $\mathfrak{p}_i$; it is therefore not contained in their union, and there then exists $f \in \mathfrak{a}$ contained in S; hence $D(f) \subseteq U$. □

Proposition 10.4.17. *Let A be a ring. Let $X = \operatorname{Spec}(A)$ as a topological space. The following are equivalent*

(a) X is Hausdorff.

(b) X is totally disconnected.

(c) Every prime ideal of A is maximal.

(d) Every quasi-compact open of X is closed.

(e) Every standard open $D(f) \subseteq X$ is closed.

Proof. It is clear that (d) and (e) are equivalent as every quasi-compact open is a finite union of standard opens. The implication (c)⇒(d) follows from Proposition 10.4.15. Assume (d) holds. Let $\mathfrak{p}, \mathfrak{p}'$ be distinct primes of A. Choose an $f \in \mathfrak{p}'$, $f \notin \mathfrak{p}$. Then $\mathfrak{p}' \notin D(f)$ and $\mathfrak{p} \in D(f)$. By (d) the open $D(f)$ is also closed. Hence $\mathfrak{p}$ and $\mathfrak{p}'$ are in disjoint open neighbourhoods whose union is X. Thus X is Hausdorff and totally disconnected. Thus (d) implies (a) and (b). Finally, if (b) holds, then the closure of $\{\mathfrak{p}\}$ must be itself, so we see (c) holds. If X is Hausdorff then every point is closed, so (a) implies (c). These together finish the proof. □

10.4.2 Functoriality of the spactrum

We will now show that $A \mapsto \operatorname{Spec}(A)$ defines a contravariant functor from the category of rings to the category of topological spaces. Let $\rho : A \to B$ be a homomorphism of rings. If $\mathfrak{q}$ is a prime ideal of B, $\rho^{-1}(\mathfrak{q})$ is a prime ideal of A. Therefore we obtain a map

$$^a\rho = \operatorname{Spec}(\rho) : \operatorname{Spec}(B) \to \operatorname{Spec}(A), \quad \mathfrak{q} \mapsto \rho^{-1}(\mathfrak{q}).$$

Proposition 10.4.18. *Let $\rho : A \to B$ be a ring homomorphism.*

(a) For every subset $S \subseteq A$, we have $(^a\rho)^{-1}(V(S)) = V(\rho(S))$, so $^a\rho$ is continuous.

(b) If $\mathfrak{b}$ is an ideal of B, then $\overline{^a\rho(V(\mathfrak{b}))} = V(\rho^{-1}(\mathfrak{b}))$.

Proof. A prime ideal $\mathfrak{q}$ of B contains $\rho(S)$ if and only if $\rho^{-1}(\mathfrak{q})$ contains S, so (a) holds. For part (b), we can rewrite the left hand side as $VI(^a\rho(V(\mathfrak{b})))$. But

$$I(^a\rho(V(\mathfrak{b}))) = \bigcap_{\mathfrak{q} \in V(\mathfrak{b})} \rho^{-1}(\mathfrak{q}) = \rho^{-1}\Big(\bigcap_{\mathfrak{q} \in V(\mathfrak{b})} \mathfrak{q}\Big) = \rho^{-1}(\sqrt{\mathfrak{b}}) = \sqrt{\rho^{-1}(\mathfrak{b})}.$$

and the claim follows by applying V. □

Corollary 10.4.19. *The map ${}^a\rho$ has dense image if and only if every element of* $\ker(\rho)$ *is nilpotent.*

Proof. By letting $\mathfrak{b} = 0$ in Proposition 10.4.18 we get $\overline{{}^a\rho(Y)} = V(\ker\rho)$, so the claim follows from the fact that $V(\mathfrak{a}) = \operatorname{Spec}(A)$ if and only if $\mathfrak{a} \subseteq \mathfrak{n}(A)$. □

Proposition 10.4.20. *Suppose that for any $g \in B$ there exists $f \in A$ such that $g = u\rho(f)$, where u is invertible in B (this is the case if ρ is surjective). Then ${}^a\rho$ is a homeomorphism from X onto ${}^a\rho(X)$. In particular,* $\operatorname{Spec}(A)$ *and* $\operatorname{Spec}(A/\mathfrak{n}(A))$ *are naturally homeomorphic.*

Proof. We show that for any subset $F \subseteq B$, there exist $E \subseteq A$ such that $V(F) = V(\rho(E))$; by virtue of the T_0-axiom and the formula of Proposition 10.4.18(a), this will first imply that ${}^a\rho(X)$ is injective, then, still by virtue of Proposition 10.4.18(a), that ${}^a\rho(X)$ is a homeomorphism. Now, it suffices for each $g \in F$ to take $f \in A$ such that $u\rho(f) = g$ with u invertible in B; the set E of these elements then satisfies the requirement. □

Corollary 10.4.21. *Let $\rho : A \to B$ be a homomorphism of rings. Let $\mathfrak{a}$ be an ideal of A and let $\mathfrak{b}$ be its extension in B. Let $\bar{\rho} : A/\mathfrak{a} \to B/\mathfrak{b}$ be the induced homomorphism. If* $\operatorname{Spec}(A/\mathfrak{a})$ *is identified with its canonical image $V(\mathfrak{a})$ in* $\operatorname{Spec}(A)$*, and* $\operatorname{Spec}(B/\mathfrak{b})$ *with its image $V(\mathfrak{b})$ in* $\operatorname{Spec}(B)$*, then ${}^a\bar{\rho}$ is the restriction of ${}^a\rho$ to $V(\mathfrak{b})$.*

Proof. Let $\mathfrak{q} \in V(\mathfrak{b})$, then $\mathfrak{a} \subseteq \mathfrak{a}^{ec} = \mathfrak{b}^c \subseteq \mathfrak{q}^c$, so ${}^a\rho(V(\mathfrak{b})) \subseteq V(\mathfrak{a})$. Let $\pi_A : A \to A/\mathfrak{a}$, $\pi_B : B \to B/\mathfrak{b}$ be the quotient maps. Then

$$\bar{\rho} \circ \pi_A(a) = \bar{\rho}(a + \mathfrak{a}) = \rho(a) + \mathfrak{b} = \pi_B \circ \rho(a).$$

Hence $\bar{\rho} \circ \pi_A = \pi_B \circ \rho$, which implies ${}^a(\pi_A) \circ {}^a\bar{\rho} = {}^a\rho \circ {}^a(\pi_B)$, so we have the following commutative diagram:

$$\begin{tikzcd}
\operatorname{Spec}(B/\mathfrak{b}) \arrow[r, "{}^a\bar{\rho}"] \arrow[d, "{}^a(\pi_B)"'] & \operatorname{Spec}(A/\mathfrak{a}) \arrow[d, "{}^a(\pi_A)"] \\
V(\mathfrak{b}) \arrow[r, "{}^a\rho"] & V(\mathfrak{a})
\end{tikzcd}$$

which is exactly the claim. □

Proposition 10.4.22. *Let S be a multiplicative subset of A and let $i_A^S : A \to S^{-1}A$ be the canonical homomorphism. Then ${}^a(i_A^S)$ is a homeomorphism of* $\operatorname{Spec}(S^{-1}A)$ *onto the subspace of* $\operatorname{Spec}(A)$ *consisting of prime ideals $\mathfrak{p}$ with $S \cap \mathfrak{p} = \varnothing$.*

Proof. We already know that ${}^a(i_A^S)$ is injective by Proposition 10.2.36, and similar to Proposition 10.4.20, we see ${}^a(i_A^S)$ is closed, so the claim follows. □

Due to Proposition 10.4.22, we may therefore identify $\operatorname{Spec}(S^{-1}A)$ with a subspace of $\operatorname{Spec}(A)$ and write $S^{-1}X$ for $\operatorname{Spec}(S^{-1}A)$, if $X = \operatorname{Spec}(A)$.

Corollary 10.4.23. *Let A be a ring and $f \in A$. Then the canonical map $i_A^{S_f} : A \to A_f$ induces a homeomorphism* $\operatorname{Spec}(A_f) \cong D(f) \subseteq \operatorname{Spec}(A)$*, with the inverse map given by $\mathfrak{p} \to \mathfrak{p}A_f$.*

Corollary 10.4.24. *Let A be a ring and $\mathfrak{p}$ a prime ideal of A. Then the canonical image of* $\operatorname{Spec}(A_\mathfrak{p})$ *in* $\operatorname{Spec}(A)$ *is equal to the intersection of all the open neighborhoods of $\mathfrak{p}$ in* $\operatorname{Spec}(A)$.

Proof. We have that $\operatorname{Spec}(A_f) = \{\mathfrak{q} \in \operatorname{Spec}(A) : f \notin \mathfrak{q}\}$ and $\operatorname{Spec}(A_\mathfrak{p}) = \{\mathfrak{q} \in \operatorname{Spec}(A) : \mathfrak{q} \subseteq \mathfrak{p}\}$, therefore

$$\operatorname{Spec}(A_\mathfrak{p}) = \bigcap_{f \in A - \mathfrak{p}} \operatorname{Spec}(A_f) = \bigcap_{\mathfrak{p} \in D(f)} D(f).$$

That is, $\operatorname{Spec}(A_\mathfrak{p})$ is the intersection of all basic open neighborhoods of the point $\mathfrak{p}$ in $\operatorname{Spec}(A)$. Since every open set is a union of principal open sets, we get the claim. □

Proposition 10.4.25. *Let $\rho : A \to B$ be a homomorphism and S a multiplicative subset of A. Then ${}^a(S^{-1}\rho) : \operatorname{Spec}(S^{-1}B) \to \operatorname{Spec}(S^{-1}A)$ is the restriction of ${}^a\rho$ on $\operatorname{Spec}(S^{-1}B)$ and*

$$\operatorname{Spec}(S^{-1}B) = ({}^a\rho)^{-1}(\operatorname{Spec}(S^{-1}A)).$$

Proof. Since $S^{-1}B = \rho(S)^{-1}B$, we have the following commutative diagram:

$$\begin{tikzcd} A \arrow[r, "\rho"] \arrow[d, "i_A^S"'] & B \arrow[d, "i_B^S"] \\ S^{-1}A \arrow[r, "S^{-1}\rho"] & S^{-1}B \end{tikzcd}$$

whence the first claim. Now, by definition, for $\mathfrak{q} \in \operatorname{Spec}(B)$ we see $\mathfrak{q} \cap \rho(S) = \varnothing$ if and only if $\mathfrak{q}^c \cap S = \varnothing$, so the last claim follows. □

Corollary 10.4.26. *Let $\rho : A \to B$ be a homomorphism and $\mathfrak{p}$ be a prime ideal of A. Then the continuous map ${}^a\nu : \operatorname{Spec}(B \otimes_A \kappa(\mathfrak{p})) \to \operatorname{Spec}(B)$, induced by the homomorphism $\nu : B \to B \otimes_A \kappa(\mathfrak{p})$, induces a homeomorphism from $\operatorname{Spec}(B \otimes_A \kappa(\mathfrak{p}))$ onto the fiber of $\mathfrak{p}$ under the map ${}^a\rho$.*

Proof. The homomorphism ν is the composition of the quotient homomorphism $B \to \mathfrak{p}^e$ and of the canonical homomorphism $B/\mathfrak{p}^e$ in its ring of fractions $(B/\mathfrak{p}^e)_\mathfrak{p}$. According to Proposition 10.4.20 and Corollary 10.4.24, ν^* thus induces a homeomorphism of $\operatorname{Spec}(B \otimes_A \kappa(\mathfrak{p}))$ on the subspace of $\operatorname{Spec}(B)$ consists of the prime ideals $\mathfrak{P}$ of B which contain $\mathfrak{p}^e$ and are disjoint of $\rho(A - \mathfrak{p})$. That is to say, which are lying above $\mathfrak{p}$. □

Example 10.4.27. Let A be an integral domain with just one non-zero prime ideal $\mathfrak{p}$. and let K be the field of fractions of A. Let $B = (A/\mathfrak{p}) \times K$. Define $\rho : A \to B$ by $\rho(x) = (\bar{x}, x)$, where x is the image of $\bar{x}$ in $A/\mathfrak{p}$. Then ${}^a\rho$ is bijective but not a homeomorphism.

In fact, the idals in $A/\mathfrak{p}$ are $(0), A/\mathfrak{p}$, that in K is $(0), K$. So by the claim below the ideals in $(A/\mathfrak{p}) \times K$ are

$$(0) \times (0), (A/\mathfrak{p}) \times (0), (0) \times K, (A/\mathfrak{p}) \times K.$$

Note that $(0) \times (0)$ is not prime: $(a, 0) \cdot (0, b) = 0$ but neither of them is zero. So

$$\operatorname{Spec}(B) = \{(A/\mathfrak{p}) \times (0), (0) \times K\}$$

Since $\operatorname{Spec}(A) = \{0, \mathfrak{p}\}$, ${}^a\rho$ is bijective.

Now $\operatorname{Spec}(B)$ is a two point Hausdorff space, since the prime ideals in B are maximal. But $\operatorname{Spec}(A)$ is non-Hausdorff because it contains 0 and

$$\overline{\{0\}} = \{\mathfrak{p} \subseteq A : \mathfrak{p} \supseteq (0)\} = \{0, \mathfrak{p}\}$$

Therefore ${}^a\rho$ cannot be a homeomorphism.

Example 10.4.28. Let A be a principal ideal domain. In this case, the maximal ideals are of the form (p) for a prime element p of A, and all prime ideals are maximal or the zero ideal. Therefore the closed points of $\operatorname{Spec}(A)$ correspond to equivalence classes of prime elements. Let $\eta \in \operatorname{Spec}(A)$ be the point corresponding to the zero ideal. Then the closure of $\{\eta\}$ is $\operatorname{Spec}(A)$.

As A is a principal ideal domain, every closed subset of $\operatorname{Spec}(A)$ is of the form $V(f)$ for some $f \in A$. Assume $f \neq 0$ and let $f = p_1^{e_1} \cdots p_r^{e_r}$ with pairwise non-equivalent prime elements p_i and integers e_i. Then $V(f)$ consists of those closed points which correspond to the prime divisors of f, that is, $V(f) = \{(p_1), \ldots, (p_r)\}$. Therefore the proper closed subsets are the finite sets consisting of closed points.

If A is a local principal ideal domain, but not a field (i.e., A is a discrete valuation ring), $\operatorname{Spec}(A)$ consists only of two points η and x, where $\mathfrak{p}_x$ is the maximal ideal and $\mathfrak{p} = \{0\}$. The only nontrivial open subset of $\operatorname{Spec}(A)$ is then $\{\eta\}$.

Example 10.4.29. Let $A = R[X]$, where R is a PID. We assume that R is not a field and let K be its field of fractions. Let $X = \operatorname{Spec}(R[X])$. Then the prime elements of $R[X]$ are either of the form p, where p is a prime element of R, or of the form f, where $f \in R[X]$ is a primitive polynomial which is irreducible in $K[X]$

If $p \in R$ is a prime element, then the closure $V(p)$ is homeomorphic to $\operatorname{Spec}((R/p)[X])$. Since $(R/p)[X]$ is a PID but not be a field, we see that (p) is not a maximal ideal, and the prime ideals in $V(p)$ different from (p) are the maximal ideals generated by p and f where $f \in R[X]$ is a polynomial such that its image in $(R/p)[X]$ is irreducible.

The situation is more complicated for prime ideals of the form (f), where f is a primitive irreducible polynomial. If the leading coefficient of f is a unit in R, it is possible to divide in $R[X]$ by f with unique remainder, and therefore $R[X]/(f)$ is finitely generated as R-module. This implies that (f) is not a maximal ideal by Proposition 13.1.62, as otherwise R would be a field.

For other primitive irreducible polynomials f, (f) might be a maximal ideal, namely if R contains only finitely many prime elements (up to equivalence): If $0 \neq a \in R$ is an element which is divisible by all prime elements of R we have, with $f = ax - 1$,

$$R[X]/(f) \cong R[a^{-1}] = K$$

which shows that (f) is a maximal ideal.

10.4.3 The support of a module

Let A be a ring and M an A-module. The set of prime ideals $\mathfrak{p}$ of A such that $M_{\mathfrak{p}} \neq 0$ is called the **support** of M and is denoted by $\operatorname{supp}(M)$. As every maximal ideal of A is prime, it follows immediately from Proposition 10.3.18 that for A-module M to be equal to 0, it is necessary and suffieient that $\operatorname{supp}(M) = \emptyset$.

Example 10.4.30. Let $\mathfrak{a}$ be an ideal of A, then we have $\operatorname{supp}(A/\mathfrak{a}) = V(\mathfrak{a})$. In fact, if $\mathfrak{p}$ is a prime of A such that $\mathfrak{a} \not\subseteq \mathfrak{p}$, then $(A/\mathfrak{a})_{\mathfrak{p}} = 0$; if on the other hand $\mathfrak{a} \subseteq \mathfrak{p}$, then $\mathfrak{a}A_{\mathfrak{p}}$ is contained in the maximal ideal $\mathfrak{p}A_{\mathfrak{p}}$ of $A_{\mathfrak{p}}$ and $(A/\mathfrak{a})_{\mathfrak{p}}$ is isomorphic to $A_{\mathfrak{p}}/\mathfrak{a}A_{\mathfrak{p}}$ and hence is non-zero; whence our assertion.

Proposition 10.4.31. *Let A be a ring and M an A-module.*

(a) If N is a submodule of M, then

$$\operatorname{supp}(M) = \operatorname{supp}(N) \cup \operatorname{supp}(M/N).$$

(b) If M is the sum of a family $(M_i)_{i\in I}$ of submodules, then

$$\operatorname{supp}(M) = \bigcup_{I\in I} \operatorname{supp}(M_i).$$

Proof. From the exact sequence $0 \to N \to M \to N/N \to 0$, we derive, for every prime ideal $\mathfrak{p}$ of A, the exact sequence

$$0 \longrightarrow N_{\mathfrak{p}} \longrightarrow M_{\mathfrak{p}} \longrightarrow (M/N)_{\mathfrak{p}} \longrightarrow 0$$

For $M_{\mathfrak{p}}$ to be reduced to 0, it is necessary and sufficient that $N_{\mathfrak{p}}$ and $(M/N)_{\mathfrak{p}}$ be so. In other words, the relation $\mathfrak{p} \notin \operatorname{supp}(M)$ is equivalent tO $\mathfrak{p} \notin \operatorname{supp}(N)$ and $\mathfrak{p} \notin \operatorname{supp}(M/N)$, which proves (a). Part (b) can be proved similarly. □

Corollary 10.4.32. *Let A be a ring, M an A-module, $(m_i)_{i\in I}$ a system of generators of M and $\mathfrak{a}_i$ the annihilator of m_i. Then* $\operatorname{supp}(M) = \bigcup_{i\in I} V(\mathfrak{a}_i)$.

Proof. We have $\operatorname{supp}(M) = \bigcup_{i\in I} \operatorname{supp}(Am_i)$ by Proposition 10.4.31. On the other hand, Am_i is isomorphic to the A-module $A/\mathfrak{a}_i$ and we have seen that $\operatorname{supp}(A/\mathfrak{a}_i) = V(\mathfrak{a}_i)$, hence the claim. □

Proposition 10.4.33. *Let A be a ring, M an A-module and $\mathfrak{a}$ its annihilator. If M is finitely generated, then* $\operatorname{supp}(M) = V(\mathfrak{a})$ *and* $\operatorname{supp}(M)$ *is therefore closed in* $\operatorname{Spec}(A)$.

Proof. Let $m_1, \dots, m_n$ be a system of generators of M and let $\mathfrak{a}_i$ be the annihilator of m_i for each i. Then $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{a}_i$, hence $V(\mathfrak{a}) = \bigcup_{i=1}^n V(\mathfrak{a}_i)$ and the proposition follows from the Corollary 10.4.32. □

Corollary 10.4.34. *Let A be a ring, M a finitely generated A-module and a an element of A. For a to belong to every prime ideal of the support of M, it is necessary and sufficient that the homothety of M with ratio a be nilpotent.*

Proof. It follows from Proposition 10.4.33 that the intersection of the prime ideals belonging to $\operatorname{supp}(M)$ is the radical of the annihilator $\mathfrak{a}$ of M. To say that a belongs to this radical is equ1valent to say that there exist a power a^n such that $a^n M = 0$. □

Corollary 10.4.35. *Let A be a Noetherian ring, M a finitely generated A-module and $\mathfrak{a}$ an ideal of A. For* $\operatorname{supp}(M) \subseteq V(\mathfrak{a})$, *it is necessary and sufficient that there exist an integer n such that $\mathfrak{a}^n M = 0$.*

Proof. If $\mathfrak{b}$ is the annihilator of M, the relation $\operatorname{supp}(M) \subseteq V(\mathfrak{a})$ is equivalent to $V(\mathfrak{b}) \subseteq V(\mathfrak{a})$ by Proposition 10.4.33 and hence to $\mathfrak{a} \subseteq \sqrt{\mathfrak{b}}$. Since A is Noetherian, this condition is also equivalent to the existence of an integer $n > 0$ such that $\mathfrak{a}^n \subseteq \mathfrak{b}$. □

Lemma 10.4.36. *Let A be a local ring and M and N two finitely generated A-modules. If $M \neq 0$ and $N \neq 0$, then $M \otimes N \neq 0$.*

Proof. Let κ be the residue field of A. By virtue of Proposition 10.3.6, $\kappa \otimes_A M \neq 0$, and $\kappa \otimes_A N \neq 0$, then we deduce that

$$(\kappa \otimes_A M) \otimes_\kappa (\kappa \otimes_A N) \neq 0$$

But, since the tensor product is associative, this tensor product is isomorphic to

$$M \otimes_A (\kappa \otimes_\kappa \kappa) \otimes_A N = M \otimes_A \kappa \otimes_A N$$

and therefore to $\kappa \otimes_A (M \otimes_A N)$, whence the lemma. □

Proposition 10.4.37. *Let M, N be two finitely generated modules over a ring A, then*

$$\operatorname{supp}(M \otimes_A N) = \operatorname{supp}(M) \cap \operatorname{supp}(N).$$

Proof. We need to prove that, if $\mathfrak{p}$ is a prime ideal of A, the relations "$(M \otimes_A N)_\mathfrak{p} \neq 0$" and "$M_\mathfrak{p} = 0$ and $N_\mathfrak{p} \neq 0$" are equivalent. As the $A_\mathfrak{p}$-modules $M_\mathfrak{p} \otimes_{A_\mathfrak{p}} N_\mathfrak{p}$ and $(M \otimes_A N)_\mathfrak{p}$ are isomorphic, our assertion follows from Lemma 10.4.36. □

Corollary 10.4.38. *Let M be a finitely generated A-module and $\mathfrak{n}$ its annihilator. For every ideal $\mathfrak{a}$ of A, $\operatorname{supp}(M/\mathfrak{a}M) = V(\mathfrak{a}) \cap V(\mathfrak{n}) = V(\mathfrak{a} + \mathfrak{n})$.*

Proof. We have $M/\mathfrak{a}M = M \otimes_A (A/\mathfrak{a})$ and $A/\mathfrak{a}$ is finitely generated, so the claim follows from Proposition 10.4.37. □

Lemma 10.4.39. *Let A, B be two local rings, $\rho : A \to B$ a local homomorphism and M a finitely generated A-module. If $M \neq 0$, then $\rho_*(M) \neq 0$.*

Proof. Let $\mathfrak{m}$ be the maximal ideal of A and $\kappa = A/\mathfrak{m}$ the residue field. The hypothesis implies that $B \otimes_A \kappa = B/\mathfrak{m}B \neq 0$ and $M \otimes_A \kappa = M/\mathfrak{m}M \neq 0$ by Proposition 10.3.6. Since the tensor product is associative, we have

$$(M \otimes_A B) \otimes_A \kappa = M \otimes_A (B \otimes_A \kappa) = M \otimes_A (\kappa \otimes_\kappa (B \otimes_A \kappa)) = (M \otimes_A \kappa) \otimes_\kappa (B \otimes_A \kappa)$$

therefore $M \otimes_A B \neq 0$. □

Proposition 10.4.40. *Let A, B be two rings, $\phi : A \to B$ a homomorphism and $\phi^* : \operatorname{Spec}(B) \to \operatorname{Spec}(A)$ the induced map. Then for every A-module M,*

$$\operatorname{supp}(M \otimes_A B) \subseteq \phi^{*-1}(\operatorname{supp}(M)).$$

If also M is finitely generated, then the equality holds.

Proof. Let $\mathfrak{q}$ be a prime ideal of B and $\mathfrak{p} = \phi^{-1}(\mathfrak{q})$. Suppose that $\mathfrak{q}$ belongs to $\operatorname{supp}(M \otimes_A B)$, then

$$(M \otimes_A B) \otimes_B B_\mathfrak{q} = M \otimes_A B_\mathfrak{q} = (M \otimes_A A_\mathfrak{p}) \otimes_A B_\mathfrak{q}.$$

since the homomorphism $A \to B \to B_\mathfrak{q}$ factors into $A \to A_\mathfrak{p} \to B_\mathfrak{q}$. The hypothesis $M \otimes_A B \otimes_B B_\mathfrak{q} \neq 0$ implies therefore $M \otimes_A A_\mathfrak{p} \neq 0$, whence the first assertion. As the homomorphism $\phi_\mathfrak{q} : A_\mathfrak{p} \to B_\mathfrak{q}$ is local, the second assertion follows from Lemma 10.4.39. □

Proposition 10.4.41. *Let A be a ring and M a finitely generated A-module. For every prime ideal $\mathfrak{p} \in \operatorname{supp}(M)$, there exists a non-zero A-homomorphism $\eta : M \to A/\mathfrak{p}$.*

Proof. Let $\mathfrak{p} \in \operatorname{supp}(M)$. As M is finitely generated and $M \neq 0$,

$$M_{\mathfrak{p}}/\mathfrak{p}M_{\mathfrak{p}} = M_{\mathfrak{p}} \otimes_A (A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}) \neq 0$$

Let $\kappa = A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ be the field of fractions of the integral domain $A/\mathfrak{p}$. Since $M_{\mathfrak{p}}/\mathfrak{p}M_{\mathfrak{p}}$ is a vector space over κ which is not reduced to 0, there exists a non-zero linear form $u : M_{\mathfrak{p}}/\mathfrak{p}M_{\mathfrak{p}} \to \kappa$. If $x_1, \ldots, x_n$ is a system of generators of M, and $\bar{x}_i$ is the image of x_i in the $(A/\mathfrak{p})$-module $M_{\mathfrak{p}}/\mathfrak{p}M_{\mathfrak{p}}$. Let $\alpha \in A/\mathfrak{p}$ be such that $\alpha u(\bar{x}_i) \in A/\mathfrak{p}$ for $1 \leq i \leq n$, then $v = \alpha u$ is a non-zero $(A/\mathfrak{p})$-linear mapping from $M_{\mathfrak{p}}/\mathfrak{p}M_{\mathfrak{p}}$ to $A/\mathfrak{p}$. The composition

$$M \longrightarrow M_{\mathfrak{p}} \longrightarrow M_{\mathfrak{p}}/\mathfrak{p}M_{\mathfrak{p}} \xrightarrow{v} A/\mathfrak{p}$$

is therefore the required homomorphism. □

10.4.4 Clopen subsets of the spectrum

Lemma 10.4.42. *Let A be a ring. Let $e \in A$ be an idempotent. In this case*

$$\operatorname{Spec}(A) = D(e) \amalg D(1-e).$$

Proof. Note that an idempotent e of a domain is either 1 or 0. Hence we see that

$$D(e) = \{\mathfrak{p} \in \operatorname{Spec}(A) : e \neq 0 \text{ in } A/\mathfrak{p}\} = \{\mathfrak{p} \in \operatorname{Spec}(A) : e = 1 \text{ in } A/\mathfrak{p}\}.$$

Similarly we have

$$D(1-e) = \{\mathfrak{p} \in \operatorname{Spec}(A) : e \neq 1 \text{ in } A/\mathfrak{p}\} = \{\mathfrak{p} \in \operatorname{Spec}(A) : e = 0 \text{ in } A/\mathfrak{p}\}.$$

Since the image of e is either 1 or 0 we deduce that $D(e)$ and $D(1-e)$ cover all of $\operatorname{Spec}(A)$. □

Lemma 10.4.43. *Let A_1 and A_2 be rings. Let $A = A_1 \times A_2$. The maps $A \to A_1, (x, y) \mapsto x$ and $A \to A_2, (x, y) \mapsto y$ induce continuous maps $\operatorname{Spec}(A_1) \to \operatorname{Spec}(A)$ and $\operatorname{Spec}(A_2) \to \operatorname{Spec}(A)$. The induced map*

$$\operatorname{Spec}(A_1) \amalg \operatorname{Spec}(A_2) \to \operatorname{Spec}(A)$$

is a homeomorphism. In other words, the spectrum of $A = A_1 \times A_2$ is the disjoint union of the spectrum of A_1 and the spectrum of A_2.

Proof. Write $1 = e_1 + e_2$ with $e_1 = (1, 0)$ and $e_2 = (0, 1)$. Note that e_1 and $e_2 = 1 - e_1$ are idempotents. Thus $\operatorname{Spec}(A) = D(e_1) \amalg D(e_2)$ by the previous lemma. Now consider the localization A_{e_1}: $\{0\} \times A_2$ is mapped to zero in it, so $A_1 = A_{e_1}$. Similarly we have $A_{e_2} = A_2$. Thus by Corollary 10.4.23 $D(e_1) = \operatorname{Spec}(A_1), D(e_2) = \operatorname{Spec}(A_2)$. □

We already know that an idempotent element gives an open and closed subset of $\operatorname{Spec}(A)$. We now prove a converse.

Proposition 10.4.44. *Let A be a ring. For each $U \subseteq \operatorname{Spec}(A)$ which is open and closed there exists a unique idempotent $e \in A$ such that $U = D(e)$. This induces a one-to-one correspondence between open and closed subsets $U \subseteq \operatorname{Spec}(A)$ and idempotents $e \in A$.*

Proof. Let $U \subseteq \operatorname{Spec}(A)$ be open and closed, and V be its complement. We can write U and V as unions of standard opens such that

$$U = \bigcup_{i=1}^{n} D(f_i) \quad \text{and} \quad W = \bigcup_{j=1}^{m} D(g_j).$$

Since $\operatorname{Spec}(A) = U \amalg V$, we observe that the collection $\{f_i, g_j\}$ must generate the unit ideal in A by Proposition 10.4.4. So the following sequence is exact

$$0 \longrightarrow A \xrightarrow{\alpha} \bigoplus_{i=1}^{n} A_{f_i} \oplus \bigoplus_{j=1}^{m} A_{g_j} \xrightarrow{\beta} \bigoplus_{i_1,i_2} A_{f_{i_1} f_{i_2}} \oplus \bigoplus_{i,j} A_{f_i g_j} \oplus \bigoplus_{j_1,j_2} A_{g_{j_1} g_{j_2}}$$

However, notice that for any pair i, j, $D(f_i g_j) = D(f_i) \cap D(g_j) = \varnothing$ since $D(f_i) \subseteq U$ and $D(g_j) \subseteq V$. Therefore by Corollary 10.4.23 we see $\operatorname{Spec}(A_{f_i g_j}) = D(f_i g_j) = \varnothing$, which implies $A_{f_i g_j}$ is the zero ring for each pair i, j. Consider the element $(1, \ldots, 1, 0, \ldots, 0) \in \bigoplus_{i=1}^{n} A_{f_i} \oplus \bigoplus_{j=1}^{m} A_{g_j}$ whose coordinates are 1 in each A_{f_i} and 0 in each A_{g_j}. It is sent to 0 under the map

$$\beta : \bigoplus_{i=1}^{n} A_{f_i} \oplus \bigoplus_{j=1}^{m} A_{g_j} \to \bigoplus_{i_1,i_2} A_{f_{i_1} f_{i_2}} \oplus \bigoplus_{j_1 . j_2} A_{g_{j_1} g_{j_2}}$$

so by the exactness of the sequence, there must be some element of A whose image under α is $(1, \ldots, 1, 0, \ldots, 0)$, which we denote by e. We see that $\alpha(e^2) = \alpha^2(e) = (1, \ldots, 1, 0, \ldots, 0) = \alpha(e)$. Since α is injective, $e = e^2$ in A and so e is an idempotent of A. We claim that $U = D(e)$. Notice that for any j, the map $A \mapsto A_{g_j}$ maps e to 0. Therefore there must be some positive integer k_j such that $g_j^{k_j} e = 0$ in A. Multiplying by e as necessary, we see that $(g_j e)^{k_j} = 0$, so $g_j e$ is nilpotent in A. By Proposition 10.4.4 $D(e) \cap D(g_j) = D(e g_j) = \varnothing$. So since $V = \bigcup_{j=1}^{m} D(g_j)$, we get $D(e) \cap V = \varnothing$; and then $D(e) \subseteq U$. Furthermore, for any i, the map $A \mapsto A_{f_i}$ maps e to 1, so there must be some l_i such that $f^{l_i}(e - 1) = 0$ in A. Hence $f_i^{l_i} e = f_i^{l_i}$. Suppose $\mathfrak{p} \in \operatorname{Spec}(A)$ contains e, then $\mathfrak{p}$ contains $f_i^{l_i} e = f_i^{l_i}$, and since $\mathfrak{p}$ is prime, $f_i \in \mathfrak{p}$. So $V(e) \subseteq V(f_i)$, implying that $D(f_i) \subseteq D(e)$. Therefore $U = \bigcup_{i=1}^{n} D(f_i) \subseteq D(e)$, and $U = D(e)$. Therefore any open and closed subset of $\operatorname{Spec}(A)$ is the standard open of an idempotent as desired. □

Corollary 10.4.45. *Let A be a nonzero ring. Then $\operatorname{Spec}(A)$ is connected if and only if A has no nontrivial idempotents.*

Proposition 10.4.46. *Let A be a ring. Let $\mathfrak{a}$ be a finitely generated ideal. Assume that $\mathfrak{a} = \mathfrak{a}^2$. Then $V(\mathfrak{a})$ is open and closed in $\operatorname{Spec}(A)$, and $A/\mathfrak{a} \cong A_e$ for some idempotent $e \in A$.*

Proof. By Nakayama's Lemma there exists an element $f = 1 + a$, $a \in \mathfrak{a}$ in A such that $f\mathfrak{a} = 0$. It follows that $V(\mathfrak{a}) = D(f)$ by a simple argument. Also, $0 = fa = a + a^2$, and hence

$$f^2 = (1 + a)^2 = 1 + 2a + a^2 = 1 + a = f,$$

so f is an idempotent. Consider the canonical map $A \to A_f$. It is surjective since $x/f^n =$

$x/f = xf/f^2 = x/1$. Any element of $\mathfrak{a}$ is in the kernel since $f\mathfrak{a} = 0$, and $x/1 = 0$ in A_f implies $f^n x = fx = (1+a)x = 0$, which means $x \in \mathfrak{a}$. □

10.4.5 Glueing properties of localization

In this part we show that given an open covering $\mathrm{Spec}(A) = \bigcup_{i=1}^n D(f_i)$ by standard opens, and given an element $h_i \in A_{f_i}$ for each i such that $h_i = h_j$ as elements of $A_{f_i f_j}$, then there exists a unique $h \in A$ such that the image of h in A_{f_i} is h_i. This result can be viewed as a sheaf property for $\mathrm{Spec}(A)$, and will play an important rule when we consider schemes.

Proposition 10.4.47. *Let A be a ring, and let $f_1, \dots, f_n \in A$ generate the unit ideal of A. Then the following sequence is exact:*

$$0 \longrightarrow A \xrightarrow{\alpha} \bigoplus_i A_{f_i} \xrightarrow{\beta} \bigoplus_{ij} A_{f_i f_j} \tag{4.5.1}$$

where the maps $\alpha : A \to \bigoplus_i A_{f_i}$ and $\beta : \bigoplus_i A_{f_i} \to \bigoplus_{i,j} A_{f_i f_j}$ are defined as

$$\alpha(x) = (x/1, \dots, x/1), \quad \beta(x_1/f_1^{r_1}, \dots, x_n/f_n^{r_n}) = x_i/f_i^{r_i} - x_j/f_j^{r_j}.$$

Proof. First let $x \in A$ such that $\alpha(x) = 0$. This means $x/1 = 0$ in A_{f_i} and so there exists n_i for each i such that

$$f_i^{n_i} x = 0.$$

Since $f_1, \dots, f_n$ generate A, we can find $a_i \in A$ such that $1 = \sum_{i=1}^n a_i f_i$. Then for all $N \geq \sum_i n_i$, we have

$$1^N = \Big(\sum_{i=1}^n a_i f_i\Big) = \sum \binom{N}{u_1, \dots, u_n} a_i^{u_1} \cdots a_n^{u_n} f_1^{u_1} \cdots f_n^{u_n}.$$

where each term has a factor of at least $f_i^{n_i}$ for some i. Therefore,

$$x = 1^N \cdot x = \sum \binom{N}{u_1, \dots, u_n} a_i^{u_1} \cdots a_n^{u_n} f_1^{u_1} \cdots f_n^{u_n} x = 0.$$

Thus, if $\alpha(x) = 0$, then $x = 0$ and so α is injective.

Now we check that the image of α equals the kernel of β. First, note that for $x \in A$ we have $\beta(\alpha(x)) = 0$, therefore the image of α is in the kernel of β. Now assume we have $x_1, \dots, x_n \in A$ such that

$$\beta\Big(\frac{x_1}{f_1^{r_1}}, \dots, \frac{x_n}{f_n^{r_n}}\Big) = 0.$$

Then, for all pairs i, j, there exists an n^{ij} such that

$$f_i^{n_{ij}} f_j^{n_{ij}} (x_i f_j^{r_j} - x_j f_i^{r_i}) = 0.$$

Choosing N so $N \geq n_{ij}$ for all i, j, we see that

$$f_i^N f_j^N (x_i f_j^{r_j} - x_j f_i^{r_i}) = 0.$$

Define elements $\tilde{x}_i$ and $\tilde{f}_i$ of A as follows:

$$\tilde{f}_i = f_i^{N+r_i}, \quad \tilde{x}_i = f_i^N x_i$$

so that $x_i/f_i^{r_i} = \tilde{x}_i/\tilde{f}_i$. Then we can use this to rewrite the above equation to get the following equality, for all i, j,

$$\tilde{f}_j \tilde{x}_i = \tilde{f}_i \tilde{x}_j.$$

Since $f_1, \ldots, f_n$ generate A, we clearly have that $\tilde{f}_1, \ldots, \tilde{f}_n$ also generate A. Therefore, there exist $a_1, \ldots, a_n$ in A so that

$$1 = \sum_{i=1}^n a_i \tilde{f}_i.$$

Therefore, we finally conclude that for all i,

$$\frac{x_i}{f_i^{r_i}} = \frac{\tilde{x}_i}{\tilde{f}_i} = \sum_{j=1}^n \frac{a_j \tilde{f}_j \tilde{x}_i}{\tilde{f}_i} = \sum_{j=1}^n \frac{a_j \tilde{f}_i \tilde{x}_j}{\tilde{f}_i} = \frac{\sum_{j=1}^n a_j \tilde{x}_j}{1}.$$

which means

$$\alpha\Big(\sum_{j=1}^n a_j \tilde{x}_j\Big) = \Big(\frac{x_1}{f_1^{r_1}}, \ldots, \frac{x_n}{f_n^{r_n}}\Big).$$

as required. □

Corollary 10.4.48. *Let A be a ring. Let $f_1, \ldots, f_n$ be elements of A generating the unit ideal. Let M be an A-module. Then the following sequence is exact:*

$$0 \longrightarrow M \xrightarrow{\alpha} \bigoplus_i M_{f_i} \xrightarrow{\beta} \bigoplus_{i,j} M_{f_i f_j} \tag{4.5.2}$$

Proof. This can be proved as Proposition 10.4.47, using the definition of M_f. □

Proposition 10.4.49. *Let A be a ring. Let $f_1, \ldots, f_n \in A$ and M be an A-module. Then $M \to \bigoplus M_{f_i}$ is injective if and only if the homomorphism*

$$\psi : M \to \bigoplus_{i=1}^n M, \quad m \mapsto (f_1 m, \ldots, f_n m)$$

is injective.

Proof. The map $M \to \bigoplus_{i=1}^n M_{f_i}$ is injective if and only if for all $m \in M$ and $e_1, \ldots, e_n \geq 1$ such that $f_i^{e_i} m = 0$, $1 \leq i \leq n$ we have $m = 0$. This clearly implies that ψ is injective. Conversely, suppose ψ is injective and $m \in M$ and $e_1, \ldots, e_n \geq 1$ are such that $f_i^{e_i} m = 0$. Let $N \geq e_i$ for all i, then $f_i^N m = 0$ for all i, which is $\psi^N(m) = 0$. Since ψ is injective, this implies $m = 0$. □

Proposition 10.4.50. *Let $(f_i)_{i \in I}$ be a finite family of elements of a ring A generating the unit ideal of A. Then the ring $B = \prod_{i \in I} A_{f_i}$ is a faifully flat A-module.*

Proof. We know each of the A_{f_i} is a flat A-module, hence so is B. On the other hand, if $\mathfrak{p}$ is a prime ideal of A, there exists an index i such that $f_i \notin \mathfrak{p}$ and $\mathfrak{p}_f = \mathfrak{p}A_f$ is therefore a prime

ideal of A_f. Then $\mathfrak{p}B \subseteq \mathfrak{p}A_{f_i} \times \prod_{j \neq i} A_{f_j} \neq B$ since $\mathfrak{p}A_{f_i} \neq A_{f_i}$. This suffices to imply that B is a faithfully flat A-module. □

Proposition 10.4.51. *Let $(f_i)_{i \in I}$ be a finite family of elements of a ring A generating the unit ideal of A.*

(a) For an A-module M to be zero, it is necessary and sufficient that, for every index i, the A_{f_i}-module M_{f_i} is zero.

(b) For an A-module M to be finitely generated (resp. finitely presented), it is necessary and sufficient that, for every index i, the A_{f_i}-module M_{f_i} be finitely generated (resp. finitely presented).

(c) Let $\phi : M \to N$ be a homomorphism of A-modules. Then ϕ is injective (resp. surjective) if and only if for every index i, the homomorphism $\phi_{f_i} : M_{f_i} \to N_{f_i}$ is injective (resp. surjective).

Proof. If $M = 0$ then clearly $M_{f_i} = 0$ for all i. Conversely, if each M_{f_i} is zero, then the A-module $P = \bigoplus_{i \in I} M_{f_i}$ is zero. But $P = M \otimes_A \prod_{i \in I} A_{f_i}$, so the claim in (a) follows from Proposition 10.4.50. Also, (c) follows immediately from (a).

Now if M is finitely generated (resp. finitely presented) then clearly every M_{f_i} is finitely generated (resp. finitely presented). Conversely, if all the M_{f_i} are finitely generated (resp. finitely presented), then P is a finitely generated (resp. finitely presented) B-module (for we can obviously suppose that for each i there is an exact sequence $A_f^m \to A_f^n \to M_{f_i} \to 0$, where m and n are independent of i). Again by Proposition 10.4.50, we see M is finitely generated (resp. finitely presented). □

Corollary 10.4.52. *Let $(f_i)_{i \in I}$ be a finite family of elements of a ring A generating the unit ideal of A. Then A is Noetherian if and only if for every index $i \in I$, then ring A_{f_i} is Noetherian.*

Proof. This follows from Proposition 10.4.51 by applying to ideals of A. □

Corollary 10.4.53. *Let $(f_i)_{i \in I}$ be a finite family of elements of a ring A generating the unit ideal of A. For an A-algebra B to be of finite type (resp. finitely presented) over A, it is necessary and sufficient that, for every index i, the A_{f_i}-algebra B_{f_i} be of finite type (resp. finitely presented) over A_{f_i} .*

Proof. One direction is clear. Conversely, assume that each B_{f_i} is of finite type (finite presented) over A_{f_i}. Since A_{f_i} is finitely presented, we then see each B_{f_i} is of finite type (finite presented) over A. For each $i \in I$ take a finite generating set S_i of B_{f_i}. Without loss of generality, we may assume that the elements of S_i are in the image of the localization map $B \to B_{f_i}$, so we take a finite set T_i of preimages of the elements of T_i in B. Let T be the union of these sets. This is still a finite set. Consider the algebra homomorphism $A[X_t]_{t \in T} \to B$ induced by T. Since it is an algebra homomorphism, the image B' is an A-submodule of the A-module B, so we can consider the quotient module B/B'. Now it is clear that Proposition 10.4.51 implies both of the claims (note that $\{f_i\}$ also generates the unit ideal in $A[X_t]$). □

Corollary 10.4.54. *Let $\rho : A \to B$ be a ring map and $\{g_i\}_{i \in I}$ elements of B generating the unit ideal of B. Then for B to be of finite type (finite presented) over A, it is necessary and sufficient that for every index $i \in I$, the algebra B_{g_i} is of finite type (finite presented) over A.*

Proof. Choose h_i in B such that $1 = \sum_i g_i h_i$. We first prove that, if B_{g_i} is of finite type, then B is of finite type. For this, for each $i \in I$ choose a finite subset S_i which generate B_{g_i} as an A-algebra and let T_i be its preimage in B (as in the proof of Corollary 10.4.53). Consider the A-subalgebra $B' \subseteq B$ generated by $\{g_i\}$, $\{h_i\}$ and T_i for all $i \in I$. Since localization is exact, we see that $B'_{g_i} \to B_{g_i}$ is injective. On the other hand, it is surjective by our choice of T_i. The elements $\{g_i\}$ generate the unit ideal in B' as $h_i \in B'$, so $B' \to B$ viewed as an B'-module homomorphism is an isomorphism by Proposition 10.4.51.

Now we consider the case for finite presentation. Assume that each B_{g_i} is finitely presented. We already know that B is of finite type, so we may identify B with $A[x_1, \dots, x_n]/\mathfrak{a}$ for some ideal $\mathfrak{a}$. Moreover, we may choose elements $\tilde{g}_i, \tilde{h}_i \in A[x_1, \dots, x_n]$ whose image in B is g_i and h_i. Then we see

$$B_{g_i} = A[x_1, \dots, x_n, y_i]/(\mathfrak{a}_i + (1 - y_i\tilde{g}_i)),$$

where $\mathfrak{a}_i$ is the ideal of $A[x_1, \dots, x_n, y_i]$ generated by $\mathfrak{a}$. By Proposition 7.2.26, we may choose a finite list of elements $f_{ij} \in \mathfrak{a}$ such that the image of f_{ij} in $\mathfrak{a}_i + (1 - y_i\tilde{g}_i)$ generate the ideal $\mathfrak{a}_i + (1 - y_i\tilde{g}_i)$. If we set

$$B' = A[x_1, \dots, x_n]/(\sum_i \tilde{g}_i\tilde{h}_i - 1, f_{ij}),$$

there is then a surjective A-algebra map $B' \to B$. The classes of the elements $\tilde{g}_i$ in B' generate the unit ideal and by construction the maps $B'_{g_i} \to B_{g_i}$ are injective, so we conclude that $B' \to B$ is injective, hence an isomorphism. □

Proposition 10.4.55. *Let $\mathfrak{a}$ be an ideal of A, $f \in A$ such that $A_f/\mathfrak{a}_f$ is an A-algebra of finite presentation. Then $\mathfrak{a}_f$ is finitely generated in A_f.*

Proof. By hypothesis, there exists a polynomial algebra $B = A[T_1, \dots, T_n]$ and a surjective A-homomorphism $\rho : B \to A_f/\mathfrak{a}_f$, whose kernel $\mathfrak{b}$ is finitely generated. Let $\pi : A_f \to A_f/\mathfrak{a}_f$ be the canonical homomorphism; for each $1 \le i \le n$, there exists $t_i \in A$ such that $\pi(t_i/s^k) = \rho(T_i)$ (we can choose an integer k for all index i). Consider then the A_f-algebra $C = A_f[T_1, \dots, T_n]$ and the homomorphism $\varphi : C \to A_f$ such that $\varphi(T_i) = t_i/s^k$. The homomorphism φ is clearly surjective, and so is the composition $\rho' = \pi \circ \varphi : C \to A_f/\mathfrak{a}_f$.

$$\begin{tikzcd}
 & B = A[T_1, \dots, T_n] \arrow[d, "\rho"] \\
A_f \arrow[r, "\pi"] & A_f/\mathfrak{a}_f \\
 & C = A_f[T_1, \dots, T_n] \arrow[u, "\rho'"'] \arrow[ul, "\varphi"]
\end{tikzcd}$$

On ther other hand, any polynomial in C is of the form P/s^m, where $P \in B$, and we have $\rho'(P/s^m) = (1/s^m)\rho(P)$. As $1/s$ is invertible in A_f, the relation $\rho'(P/s^m) = 0$ in $A_f/\mathfrak{a}_f$ is equivalent to $\rho(P) = 0$, and therefore the kernel $\mathfrak{b}'$ of ρ' is generated by the image of $\mathfrak{b}$ in C, and a fortiori is finitely generated in C. As $\mathfrak{b}' = \varphi^{-1}(\pi^{-1}(0)) = \varphi^{-1}(\mathfrak{a}_f)$ and φ is surjective, we see $\mathfrak{a}_f = \varphi(\mathfrak{b}')$, so $\mathfrak{a}_f$ is finitely generated in A_f. □

Remark 10.4.3. If B is an A-algebra of finite presentation, B' is an A-algebra of finite type, and $\rho : B' \to B$ is a surjective homomorphism, then the kernel $\mathfrak{b}$ of ρ is finitely generated in B'. In

faactm there exists a surjective homomorphism $\psi : C \to B'$, where C is a polynomial algebra over A; as $\rho \circ \psi$ is surjective, $\ker(\rho \circ \psi)$ is a finitely generated ideal in C by Proposition 10.4.55. As we have $\mathfrak{b} = \psi(\ker(\rho \circ \psi))$, $\mathfrak{b}$ is then finitely generated in B'.

Conversely, if B' is an A-algebra of finite presentation, $\rho : B' \to B$ is a surjective homomorphism, and if $\mathfrak{b} = \ker \rho$ is finitely generated in B', then B is an A-algebra of finite presentation. In fact, we have a surjective homomorphism $\psi : C \to B'$ where C is a polynomial algebra and $\ker \psi$ is finitely generated in C. As $\ker(\rho \circ \psi)$ is generated by $\ker \psi$ and a system of elements whose image in B' generate $\mathfrak{b}$, it is finitely generated and therefore B is an A-algebra of finite presentation.

10.5 Finitely generated projective modules

10.5.1 Local characterization

Proposition 10.5.1. *Let A be a ring, $\phi : M \to N$ an A-module homomorphism and $\mathfrak{p}$ a prime ideal of A.*

(a) Suppose that $\phi_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is suriective and that N is finitely generated. Then there exists $f \in A - \mathfrak{p}$ such that $\phi_f : M_f \to N_f$ is surjective.

(b) Suppose that $\phi_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is bijectioe, that M is finitely generated and that N is finitely presented. Then there exists $f \in A - \mathfrak{p}$ such that $\phi_f : M_f \to N_f$ is bijective.

Proof. Let P and Q be the kernel and cokernel of ϕ. If $f \in A$, the kernel and cokernel of ϕ_f (resp. $\phi_{\mathfrak{p}}$) are P_f and Q_f (resp. $P_{\mathfrak{p}}$ and $Q_{\mathfrak{p}}$). In the case (a), $\phi_{\mathfrak{p}}$ is surjective so $Q_{\mathfrak{p}} = 0$; as N is finitely generated, so is Q and therefore there exists $f \in A - \mathfrak{p}$ such that $fQ = 0$, whence $Q_f = 0$.

Under the hypotheses of (b), the sequence $0 \to P_f \to M_f \to N_f \to 0$ is exact, hence P_f is finitely generated. Now, $(P_f)_{\mathfrak{p}P_f} = P_{\mathfrak{p}} = 0$, hence there exists $g/f^d \in A_f - \mathfrak{p}A_f$ (whence $g \in A - \mathfrak{p}$) such that $(g/f^d)P_f = 0$. Then as $1/f$ is invertible, we have $(g/1)P_f = 0$, whence $P_{fg} = (P_f)_{g/1} = 0$. Since $fg \in A - \mathfrak{p}$ and $Q_{fg} = 0$, we get the claim. □

Corollary 10.5.2. *If N is finitely presented and $N_{\mathfrak{p}}$ is a free $A_{\mathfrak{p}}$-module of rank p, there exists $f \in A - \mathfrak{p}$ such that N_f is a free A_f-module of rank p.*

Proof. There exist by hypothesis elements $x_1, \ldots, x_p$ such that the $x_i/1$ form a basis of the free $A_{\mathfrak{p}}$-modulc $N_{\mathfrak{p}}$. Consider the homomorphism $\phi : A^p \to N$ such that $\phi(e_i) = x_i$, (e_i) being the canonical basis of A^p. As $\phi_{\mathfrak{p}}$ is bijective by hypothesis, there exists $f \in A - \mathfrak{p}$ such that ϕ_f is bijective, by virtue of Proposition 10.5.1. □

Remark 10.5.1. In the language of algebraic geometry, Corallary 10.5.2 shows that if $\mathscr{F}$ is a coherent sheaf over a scheme X such that $\mathscr{F}|_x$ is free of rank n for some point $x \in X$, then there exist a neighborhood U of x such that $\mathscr{F}|_U$ is free of rank n.

Corollary 10.5.3. *Let N be a finitely generated A-module and consider the function ϕ on $X = \operatorname{Spec}(A)$ defined by*

$$\phi(\mathfrak{p}) = \dim_{\kappa(\mathfrak{p})}(N_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} \kappa(\mathfrak{p})).$$

Then ϕ is upper semi-continuous, i.e., for any $n \in \mathbb{Z}$, the set $\{\mathfrak{p} \in X : \phi(\mathfrak{p}) < n\}$ is open.

Proof. Note that $\phi(\mathfrak{p}) = [N_\mathfrak{p}/\mathfrak{p}N_\mathfrak{p} : \kappa(\mathfrak{p})]$. By Nakayama's Lemma, this number is equal to the minimal number of generators of $N_\mathfrak{p}$ as an $A_\mathfrak{p}$ module. Let $m_1, \dots, m_r$ be such a minimal generating set with $r < n$. Write $m_i = x_i/f$ for $x_i \in N$ and $f \in A - \mathfrak{p}$, then we get a map $\phi : A_f^r \to N_f$ defined by $\phi(e_i/1) = x_i/f$, such that $\phi_\mathfrak{p}$ is surjective. By Proposition 10.5.1 there exist some $g \in A - \mathfrak{p}$ such that $\phi_g : A_{fg}^r \to N_{fg}$ is surjective. Then for any $\mathfrak{q} \in D(fg)$, by localizing we see $\phi_\mathfrak{q} : A_\mathfrak{q}^r \to N_\mathfrak{q}$ is also surjective, whence $\phi(\mathfrak{q}) \leq r < n$. Therefore the set $\{\mathfrak{p} \in X : \phi(\mathfrak{p}) < n\}$ is open. □

Theorem 10.5.4. *Let A be a ring and P an A-module. Then the following properties are equivalent:*

(i) P is a finitely generated projective module.

(ii) P is a finitely presented module and, for every maximal ideal $\mathfrak{m}$ of A, $P_\mathfrak{m}$ is a free $A_\mathfrak{m}$-module.

(iii) P is a finitely generated module, for all $\mathfrak{p} \in \operatorname{Spec}(A)$, the $A_\mathfrak{p}$-module $P_\mathfrak{p}$ is free and, if we denote its rank by $\operatorname{rg}_\mathfrak{p}$, the function $\mathfrak{p} \mapsto \operatorname{rg}_\mathfrak{p}$ is locally constant in the topological space $\operatorname{Spec}(A)$.

(iv) There exists a finite family $(f_i)_{i\in I}$ of elements of A, generating the ideal A, such that for all $i \in I$, the A_{f_i}-module P_{f_i} is free of finite rank.

(v) For every maximal ideal $\mathfrak{m}$ of A, there exists $f \in A - \mathfrak{m}$ such that $P_\mathfrak{m}$ is free of finite rank.

Proof. We know that a finitely generated projective module is finitely presented (Proposition 7.2.25). If P is a projective A-module, $P_\mathfrak{m} = P \otimes_A A_\mathfrak{m}$ is a projective $A_\mathfrak{m}$-module. Finally, as $A_\mathfrak{m}$ is a local ring, every finitely presented projective $A_\mathfrak{m}$-module is free (Corollary 10.3.11). This shows (i) implies (ii). Also, (ii) implies (v) by Corollary 10.5.2.

Now assume (v), and let E be the set of $f \in A$ such that P_f is a finitely generated free A_f-module. The hypothesis implies that E is contained in no maximal ideal of A, hence E generates the ideal A and there therefore exist a finite family $(f_i)_{i\in I}$ of elements of E that generates A, whence (iv).

Assume (iv) and consider the ring $B = \prod_{i\in I} A_{f_i}$ and the B-module $M = \bigoplus_{i\in I} P_{f_i} = P \otimes_A B$. For every index i, there exists a free A_{f_i}-module L_i such that P_i is a direct factor of L_i and it may be assumed that all the L_i have the same rank; then $L = \bigoplus_{i\in I} L_i$ is a free B-module of which M is a direct factor, in other words M is a finitely generated projective B-module. As B is a faithfully flat A-module, we conclude that P is a finitely generated projective A-module by Proposition 7.3.17.

Finally, we show that (iv) implies (iii) and (iii) implies (v). If (iv) holds, then it follows from Proposition 10.4.51 that P is finitely generated. On the other hand, for every prime ideal $\mathfrak{p}$ of A, there exists an index i such that $f_i \notin \mathfrak{p}$; then $P_\mathfrak{p} = (P_{f_i})_{\mathfrak{p}_{f_i}}$ and hence by hypothesis $P_\mathfrak{p}$ is free and of the same rank as P_{f_i}, which proves (iii).

Assume (iii), let $\mathfrak{m}$ be a maximal ideal of A; write $\operatorname{rg}_\mathfrak{m} = n$ and let $x_1, \dots, x_n$ be a basis of $P_\mathfrak{m}$. We can assume that the x_i are canonical images of elements $p_i \in P$ to within multiplication by an invertible element of $A_\mathfrak{m}$. Let (e_i) be the canonical basis of A^n and $\phi : A^n \to P$ the homomorphism such that $\phi(e_i) = p_i$. As P is finitely generated, it follows from Proposition 10.5.1 that there exists $f \in A - \mathfrak{m}$ such that ϕ_f is surjective. We conclude that ϕ_{fg} is also surjective for all $g \in A - \mathfrak{m}$ and by hypothesis there exists $g \in A - \mathfrak{m}$ such that $\operatorname{rg}_\mathfrak{p} = n$ for $\mathfrak{p} \in D(g)$. Then, replacing f by fg, we may assume that $\operatorname{rg}_\mathfrak{p} = n$ for all $\mathfrak{p} \in D(f)$. Then $\phi_\mathfrak{p} : A_\mathfrak{p}^n \to P_\mathfrak{p}$ is a surjective homomorphism and $P_\mathfrak{p}$ and $A_\mathfrak{p}^n$ are both free $A_\mathfrak{p}$-modules of the same rank; hence

by Corollary 10.3.13 $\phi_{\mathfrak{p}}$ is bijective for all $\mathfrak{p} \in D(f)$. Let $\mathfrak{p}'$ be a prime ideal of A_f and let $\mathfrak{p}$ be its inverse image in A under the canonical mapping; if $(A_f^n)_{\mathfrak{p}'}$ and $(P_f)_{\mathfrak{p}'}$ are identified with $A_{\mathfrak{p}}^n$ and $P_{\mathfrak{p}}$ under the canonical isomorphisms, $(\phi_f)_{\mathfrak{p}'}$ is then identified with $\phi_{\mathfrak{p}}$ and is consequently bijective. We conclude that ϕ is bijective, which establishes (v). □

Corollary 10.5.5. *Suppose that the equivalent properties of the statement of Theorem 10.5.4 hold. Let n be a positive integer such that, for every family $(x_1, \dots, x_n)$ of elements of P, there exists a family $(a_1, \dots, a_n)$ of elements of A, which are not all divisors of zero and for which $\sum_{i=1}^n a_i x_i = 0$. Then, for all $\mathfrak{p} \in \operatorname{Spec}(A)$, $\operatorname{rg}_{\mathfrak{p}} \leq n$.*

Proof. Let $\mathfrak{p}$ be a prime ideal of A, set $\operatorname{rg}_{\mathfrak{p}} = r$ and let $(y_1, \dots, y_r)$ be a basis of the free $A_{\mathfrak{p}}$-module $P_{\mathfrak{p}}$. There exist elements $(x_1, \dots, x_r)$ of P and $s \in A - \mathfrak{p}$ such that $y_i = x_i/s$ for all i. If $r > n$, then there exist a family $(a_1, \dots, a_r)$ of elements of A such that $\sum_{i=1}^r a_i x_i = 0$, which are not all divisors of zero (for example take $(a_1, \dots, a_n)$ as in the hypothesis and let $a_i = 0$ for $i > n$). But then we have $\sum_{i=1}^r (a_i/1) y_i = 0$ and therefore $a_i = 0$ in $A_{\mathfrak{p}}$, which implies a_i is a divisor of zero, contradiction. □

Corollary 10.5.6. *Every finitely presented flat module is projective.*

Proof. If P is a finitely presented flat A-module and $\mathfrak{m}$ a maximal ideal of A, the $A_{\mathfrak{m}}$-module $P_{\mathfrak{m}}$ is flat and finitely presented and hence free (Corollary 10.3.11). Condition (ii) of Theorem 10.5.4 therefore holds. □

10.5.2 Rank of finitely generated projective modules

Definition 10.5.7. *Let P be a finitely generated projective A-module. For every prime ideal $\mathfrak{p}$ of A, the rank of the free $A_{\mathfrak{p}}$-module P, is called the rank of P at $\mathfrak{p}$ and is denoted by $\operatorname{rg}_{\mathfrak{p}}(P)$.*

By Theorem 10.5.4 the integer-valued function $\mathfrak{p} \mapsto \operatorname{rg}_{\mathfrak{p}}(P)$ is locally constant on $X = \operatorname{Spec}(A)$. It is therefore constant if X is connected and in particular if the ring A is an integral domain.

Definition 10.5.8. *Let n be a positive integer. A projective A-module P is said to be **of rank n** if it is finitely generated and $\operatorname{rg}_{\mathfrak{p}}(P) = n$ for every prime ideal $\mathfrak{p}$ of A.*

Clearly every finitely generated flee A-module L is of rank n in the sense of the above definition, n being equal to the dimension (or rank) of L. A projective module of rank 0 is zero. If A is not reduced to 0 and a projective A-module P is of rank n, the integer n is determined uniquely; it is then denoted by $\operatorname{rg}(P)$.

Theorem 10.5.9. *Let P be an A-module and n a psotive integer. The following properties are equivalent:*

(i) P is projective of rank n.

(ii) P is finitely generated and, for every maximal ideal $\mathfrak{m}$ of A, the $A_{\mathfrak{m}}$-module $P_{\mathfrak{m}}$ is free of rank n.

(iii) P is finitely generated and, for every prime ideal $\mathfrak{p}$ of A, the $A_{\mathfrak{p}}$-module $P_{\mathfrak{p}}$ is free of rank n.

(iv) For every maximal ideal $\mathfrak{m}$ of A, there exists $f \in A - \mathfrak{m}$ such that the $A_{\mathfrak{m}}$-module $P_{\mathfrak{m}}$ is free of rank n.

Proof. By definition and Theorem 10.5.4, (i) and (iii) are equivalent; (ii) implies (iii), as, for every prime ideal $\mathfrak{p}$ of A, there exists a maximal ideal $\mathfrak{m}$ containing $\mathfrak{p}$ and, writing $\mathfrak{p}' = \mathfrak{p}_\mathfrak{m}$, $P_\mathfrak{p}$ is isomorphic to $(P_\mathfrak{m})_{\mathfrak{p}'}$. If $P_\mathfrak{m}$ is free of rank n, so then is $P_\mathfrak{p}$. Property (iii) implies (i) by virtue of Theorem 10.5.4 and the fact that, iff $f \in A - \mathfrak{m}$ and $\mathfrak{m}' = \mathfrak{m}_f$, $P_\mathfrak{m}$ is isomorphic to $(P_f)_{\mathfrak{m}_f}$ and therefore the ranks of P_f and $P_\mathfrak{m}$ are equal. Finally, this last argument and Theorem 10.5.4 show that (iv) implies (ii). □

Corollary 10.5.10. *If A is an integral domain and P is a projective A-module, then* $\mathrm{rg}_\mathfrak{p}(P) = \mathrm{rank}(P)$ *for all prime ideal $\mathfrak{p}$ of A.*

Proof. It is sufficient to apply Theorem 10.5.9(iii) with $\mathfrak{p} = (0)$. □

Let E and F be two finitely generated projective A-modules. We know that $E \oplus F$, $E \otimes_A F$, $\mathrm{Hom}_A(E, F)$ and the dual E^* of E are projective and finitely generated, so is the exterior power $\bigwedge^p E$ for every integer $p > 0$. Also, it follows immediately from definition and the exactness of localization that, for every prime ideal $\mathfrak{p}$ of A,

$$\mathrm{rg}_\mathfrak{p}(E \oplus F) = \mathrm{rg}_\mathfrak{p}(E) + \mathrm{rg}_\mathfrak{p}(F), \quad \mathrm{rg}_\mathfrak{p}(E \times F) = \mathrm{rg}_\mathfrak{p}(E)\mathrm{rg}_\mathfrak{p}(F),$$

$$\mathrm{rg}_\mathfrak{p}(\mathrm{Hom}_A(E, F)) = \mathrm{rg}_\mathfrak{p}(E)\mathrm{rg}_\mathfrak{p}(F), \quad \mathrm{rg}_\mathfrak{p}(E^*) = \mathrm{rg}_\mathfrak{p}(E), \quad \mathrm{rg}_\mathfrak{p}(\bigwedge^p E) = \binom{\mathrm{rg}_\mathfrak{p}(E)}{p}.$$

If the ranks of E and F are defined, so are those of $E \oplus F$, $E \otimes_A F$, $\mathrm{Hom}_A(E, F)$, E^* and $\bigwedge^p E$ and the above equations also hold with the index $\mathfrak{p}$ omittcd. Moreover:

Corollary 10.5.11. *For a finitely generated firqjective A-module P to be of rank n, it is necessary and sufficient that $\bigwedge^n P$ be of rank* 1.

Proposition 10.5.12. *Let B be a A-algebra and P a projective A-module of rank n. The B-module $B \otimes_A P$ is then projective of rank n.*

Proof. We know that $B \otimes_A P$ is projective and finitely generated. If $\mathfrak{q}$ is a prime ideal of B and $\mathfrak{p}$ its inverse image in A, then

$$(B \otimes_A P)_\mathfrak{q} = (P \otimes_A B) \otimes_B B_\mathfrak{q} = P \otimes_A B_\mathfrak{q} = (P \otimes_A A_\mathfrak{p}) \otimes_A B_\mathfrak{q}$$

and, as, by hypothesis, $P \otimes_A A_\mathfrak{p}$ is a free $A_\mathfrak{p}$-module of rank n, $(B \otimes_A P)_\mathfrak{q}$ is a free $B_\mathfrak{q}$-module of rank n. □

Proposition 10.5.13. *Let A be a semi-local ring and P a finitely generated projective A-module. If the rank of P is defined, P is a free A-module.*

Proof. Suppose first that $A = \prod_{i=1}^n K_i$ where K_i are fields. Then the K_i are then identified with the minimal ideals of A and, for all i, the sum $\mathfrak{p}_i = \sum_{j \neq i} K_j$ is a maximal ideal of A, and the $\mathfrak{p}_i$'s are the only prime ideals of A. Every finitely generated A-module P is therefore the direct sum of its isotypical components P_i, P_i being isomorphic to a direct sum of a finite number r, of A-modules isomorphic to K_i (**??**); the ring $A_{\mathfrak{p}_i}$ is identified with K_i and annihilates the P_j of index $j \neq i$, hence $n = \mathrm{rg}_{\mathfrak{p}_i}(P)$; if all the r_i are equal to the same number r, P is isomorphic to A^r, whence the proposition in this case. In the general case, let $\mathfrak{r}$ be the Jacobson radical of A and $B = A/\mathfrak{r}$; as B is a product of fields, the projective B-module $P \otimes_A B$ is free by the remarks

preceding Proposition 10.5.12. Also P is a flat A-module and the proposition then follows from Proposition 10.3.9. □

10.5.3 Projective modules of rank 1

Theorem 10.5.14. *Let A be a ring and M a finitely generated A-module.*

(a) If there exists an A-module N such that $M \otimes_A N$ is isomorphic to A, the module M is projective of rank 1.

(b) Conversely, if M is projective of rank 1 and M^* is the dual of M, the canonical homomorphism $v : M^* \otimes_A M \to A$ corresponding to the canonical bilinear form $(x^*, x) \mapsto \langle x^*, x\rangle$ on $M^* \times M$ is bijective.

Proof. First assume that $M \otimes_A N \cong A$ for some A-module N. It is required to prove that, for every maximal ideal $\mathfrak{m}$ of A, the $A_\mathfrak{m}$-module $M_\mathfrak{m}$ is free of rank 1. We are free to replace A by $A_\mathfrak{m}$ and hence may assume that A is a local ring. Let $k = A/\mathfrak{m}$. The isomorphism $\eta : M \otimes_A N \to A$ defines an isomorphism

$$\eta \otimes 1_k : (M/\mathfrak{m}M) \otimes_k (N/\mathfrak{m}N) \to k$$

as the rank over k of $(M/\mathfrak{m}M) \otimes_k (N/\mathfrak{m}N)$ is the product of the ranks of $M/\mathfrak{m}M$ and $N/\mathfrak{m}N$, these latter are necessarily equal to 1, in other words $M/\mathfrak{m}M$ is monogenous. It follows that M is monogenous by Corollary 10.3.8. On the other hand, the annihilator of M also annihilates $M \otimes_A N$ and hence is zero, which proves that M is isomorphic to A.

For (b), assume that M is projective of rank 1. It is sufficient to prove that, for every maximal ideal $\mathfrak{m}$ of A, $v_\mathfrak{m}$ is an isomorphism. As M is finitely presented, $(M^*)_\mathfrak{m}$ is canonically identified with the dual $(M_\mathfrak{m})^*$ (Proposition 10.2.46) and, as $M_\mathfrak{m}$ is free of rank 1 like its dual $(M_\mathfrak{m})^*$, clearly the canonical homomorphism $v_\mathfrak{m} : (M_\mathfrak{m})^* \otimes_{A_\mathfrak{m}} (M_\mathfrak{m}) \to A_\mathfrak{m}$ is bijcctive, which completes the proof. □

Remark 10.5.2. If M is projective of rank 1 and N is such that $M \otimes_A N$ is isomorphic to A, then N is isomorphic to M^*, for there are isomorphisms

$$N \to N \otimes_A A \to N \otimes M \otimes M^* \to A \otimes M^* \to M^*.$$

Now let $A^n \to M$ be a surjective homomorphism. Then by applying the dual functor $\mathrm{Hom}(-, A)$ we get an injection $N \cong M^* \to (A^n)^* \cong A^n$. If we further assume that A is Noetherian, then N is a finitely generated A-module.

In the language of algebraic geometry, Theorem 10.5.14 and the argument above show that a coherent sheaf $\mathscr{F}$ on a Noetherian scheme X is invertible (locall of rank 1) if and only if there exist a coherent sheaf $\mathscr{G}$ such that $\mathscr{F} \otimes_{\mathscr{O}_X} \mathscr{G} \cong \mathscr{O}_X$. This justifies the terminology invertible: it means that $\mathscr{F}$ is an invertible element of the monoid of coherent sheaves under the operation $\otimes$.

Proposition 10.5.15. *Let M and N be projective A-modules of rank 1. Then $M \otimes_A N$, $\mathrm{Hom}_A(M, N)$ and the dual M^* of M are projective of rank 1.*

Let us now note that every finitely generated A-module is isomorphic to a quotient module of $L = A^n$. We may therefore speak of the set $F(A)$ of classes of finitely generated A-modules

with respect to isomorphism. We denote by $P(A)$ the subset of $F(A)$ consisting of the classes of projective A-modules of rank 1 and by $\mathrm{cl}(M)$ the image in $P(A)$ of a projective A-module M of rank 1. It is immediate that, for two projective A-modules M, N of rank 1, $\mathrm{cl}(M \otimes_A N)$ depends only on $\mathrm{cl}(M)$ and $\mathrm{cl}(N)$. As definition we set

$$\mathrm{cl}(M) + \mathrm{cl}(N) = \mathrm{cl}(M \otimes_A N) \tag{5.3.1}$$

and an internal law of composition is thus defined on $P(A)$.

Proposition 10.5.16. *The set $P(A)$ of classes of projective A-modules of rank 1, with the law of composition (5.3.1), is a commutative group. If M is a projective A-module of rank 1 and M^* is its dual, then*

$$\mathrm{cl}(M^*) = -\mathrm{cl}(M), \quad \mathrm{cl}(A) = 0.$$

Proof. The associativity and commutativity of the tensor product show that the law of composition (6) is associative and commutative. The isomorphism between $A \otimes_A M$ and M prove that $\mathrm{cl}(A)$ is the identity element under this law and, by virtue of Theorem 10.5.14, $\mathrm{cl}(M) + \mathrm{cl}(M^*) = \mathrm{cl}(A)$, whence the proposition. □

Let B be an A-algebra and M a projective A-module of rank 1. Then $B \otimes_A M$ is a projective B-module of rank 1 by Proposition 10.5.12. Then there exists a mapping called canonical $\phi : P(A) \to P(B)$ such that

$$\phi(\mathrm{cl}(M)) = \mathrm{cl}(B \otimes_A M).$$

The equation $(M \otimes_A B) \otimes_B (N \otimes_A B) = (M \otimes_A N) \otimes_A B$ for two A-modules M, N proves that the mapping ϕ is a group homomorphism.

Remark 10.5.3. Condition (v) of Theorem 10.5.4 (equivalent to the fact that P is projective and finitely generated) may also be expressed by saying that the sheaf of modules P over $X = \mathrm{Spec}(A)$ associated with P is locally free and of finite type and may therefore be interpreted as the sheaf of sections of a vector bundle over X. Conversely, every vector bundle over X arises from a finitely generated projective module, which is determined to within a unique isomorphism. The projective modules of rank n thus correspond to the vector bundles all of whose fibres have dimension n. In particular, the vector bundles of rank 1 correspond to the projective modules of rank 1. If we denote by $\mathcal{O}_X$ the structure sheaf of X and by $\mathcal{O}_X^\times$ the sheaf of units of $\mathcal{O}_X$ (whose sections over an open set U of X are the invertible elements of the ring of sections of $\mathcal{O}_X$ over U), it follows that the group $P(A)$ is isomorphic to the first cohomology group $H^1(X, \mathcal{O}_X^\times)$.

10.5.4 Non-degenerate submodules and invertible submodules

In this part and the two following, A denotes a ring, S a multiplicative subset of A consisting of elements which are not divisors of zero in A, and B the ring $S^{-1}A$. The ring A is then canonically identified with a subring of B. The elements of S are therefore invertible in B. One of the most important special cases for applications is that where A is an integral domain and S is the set of nonzero elements of A; in this case B is the field of fractions of A.

Let M be a sub-A-module of B. Then M is called **non-degenerate** if $B \cdot M = B$. Note that if B is a field, this condition simply means that M is not reduced to 0.

Proposition 10.5.17. *Let M be a sub-A-module of B. The following conditions are equivalent:*

(i) M is non-degenerate;

(ii) M meets S;

(iii) If $i_M : M \to B$ is the canonical injection, then $S^{-1}i_M : S^{-1}M \to B$ is bijective.

Proof. Part (i) implies (ii), for if $B \cdot M = B$, there exists $a \in A$, $s \in S$ and $x \in M$ such that $(a/s)x = 1$, hence $ax = s$ belongs to $S \cap M$. To see that (ii) implies (iii), note that $S^{-1}i$ is already injective, since localization is a exact functor. Moreover, if $x \in M \cap S$, the image under $S^{-1}i$ of $x/x \in S^{-1}M$ in B is equal to 1 and $S^{-1}i$ is therefore surjective. Finally, (iii) clearly implies (i). □

Corollary 10.5.18. *If M and N are two non-degenerate sub-A-modules of B, the A-modules $M + N$, $M \cdot N$ and $M \cap N$ are non-degenerate.*

Proof. The assertion is trivial for $M + N$. On the other hand if $s \in S \cap M$ and $t \in S \cap N$, then $st \in S \cap (M \cdot N)$ and $st \in S \cap (M \cap N)$. □

Given two sub-A-modules M and N of B, let us denote by $(N : M)$ the sub-A-module of B consisting of those $b \in B$ such that $bM \subseteq N$. If every $b \in (N : M)$ is mapped to the homomorphism $h_b : x \mapsto bx$ of M to N, a canonical homomorphism $b \mapsto h_b$, is obtained from $(N : M)$ to $\mathrm{Hom}_A(M, N)$.

Proposition 10.5.19. *Let M, N be two sub-A-modules of B. If M is non-degenerate, the canonical homomorphism from $(N : M)$ to $\mathrm{Hom}_A(M, N)$ is bijective.*

Proof. Let $s \in S \cap M$. If $b \in (N : M)$ is such that $bx = 0$ for all $x \in M$, then $bs = 0$ whence $b = 0$ since s is not a divisor of 0 in B. On the other hand, let $f \in \mathrm{Hom}_A(M, N)$ and set $b = f(s)/s$; for all $x \in M$, there exists $t \in S$ such that $tx \in A$. Then

$$f(x) = f(stx)/(st) = (txf(s))/(st) = bx$$

whence $b \in (N : M)$ and $f = h_b$, which proves the proposition. □

In particular, $(A : M)$ is canonically identified with the dual M^* of M, the canonical bilinear form on $M^* \times M$ being identified with the restriction to $(A : M) \times M$ of the multiplication $B \times B \to B$.

Definition 10.5.20. *A sub-A-module M of B is called **invertible** if there exists a sub-A-module N such that $M \cdot N = A$.*

Example 10.5.21. If b is invertible element of B, the A-module Ab is invertible, as is seen by taking $N = Ab^{-1}$.

Proposition 10.5.22. *Let M be an invertible sub-A-module of B. Then:*

(a) There exists $s \in S$ such that $As \subseteq M \subseteq As^{-1}$ (and in particular M is nondegenerate).

(b) $(A : M)$ is the only sub-A-module N of B such that $M \cdot N = A$.

(c) M is finitely generated and $(A : M) = A$ if and only if $M = A$.

Proof. If there exists a sub-A-module N such that $M \cdot N = A$, then

$$B \cdot M = B \cdot (B \cdot M) \supseteq B \cdot (M \cdot N) = B \cdot A = B$$

hence M is non-degenerate. Similarly N is non-degenerate. If $t_1 \in S \cap M$ and $t_2 \in S \cap N$, the element $s = t_1 t_2$ belongs to $S \cap M \cap N$, whence $Ms \subseteq M \cdot N = A$ and therefore $As \subseteq M \subseteq As^{-1}$.

On the other hand, obviously $N \subseteq (A : M)$, whence

$$A = M \cdot N \subseteq M \cdot (A : M) \subseteq A$$

whence $A = M \cdot (A : M)$. Multiplying the two sides by N, we deduce then $N = (A : M)$, this prove (b). Now since $M \cdot N = A$, then there is an equation

$$\sum_i x_i y_i, \quad x_i \in M, y_i \in N,$$

so M is generated by (x_i) since $x = \sum_i (xy_i)x_i$ for each $x \in M$. Moreover, if $(A : M) = A$ then since M is invertible we have $M \cdot A = A$, which implies $M = A$. □

Theorem 10.5.23. *Let M be a non-degenerate sub-A-module of B. The following properties are equivalent:*

(i) M is invertible.

(ii) M is projective.

(iii) M is projective of rank 1.

(iv) M is a finitely generated A-module and, for every maximal ideal $\mathfrak{m}$ of A, the $A_\mathfrak{m}$-module $M_\mathfrak{m}$ is principal.

Proof. Let us show first the equivalence of properties (i), (ii) and (iii). If (i) holds and N is sub-A-module of B such that $M \cdot N = A$, then there is a relation

$$\sum_i m_i n_i = 1$$

For all $x \in M$, set $v_i(x) = n_i x$, the v_i are linear forms on M and by $x = \sum_i v_i(x) m_i$ for all $x \in M$. This proves that M is projective by **??** and generated by the x_i; hence M is a finitely generated projective module.

Let $\mathfrak{m}$ be a maximal ideal of A. We show that the integer $r = \mathrm{rg}_\mathfrak{m}(M)$ is equal to 1. Let $S_\mathfrak{m}$ be the image of S in $A_\mathfrak{m}$. As the elements of S are not divisors of 0 in A, those of $S_\mathfrak{m}$ are not divisors of 0 in $A_\mathfrak{m}$, since $A_\mathfrak{m}$ is a flat A-module. Then $(S_\mathfrak{m})^{-1} A_\mathfrak{m} \neq 0$ and, as $M_\mathfrak{m}$ is a free $A_\mathfrak{m}$-module of rank r, $(S_\mathfrak{m})^{-1} M_\mathfrak{m}$ is a free $(S_\mathfrak{m})^{-1} A_\mathfrak{m}$-module of rank r. Also note that $(S_\mathfrak{m})^{-1} A_\mathfrak{m}$ (resp. $(S_\mathfrak{m})^{-1} M_\mathfrak{m}$) is canonically identified with $(S^{-1}A)_\mathfrak{m}$ (resp. $(S^{-1}M)_\mathfrak{m}$). Now $S^{-1}M = B$ by Proposition 10.5.17(iii) and hence $(S^{-1}M)_\mathfrak{m}$ is a free $(S^{-1}A)_\mathfrak{m}$ of rank 1, which proves that $r = 1$ and shows the implication $(i) \Rightarrow (iii)$.

The implication $(iii) \Rightarrow (ii)$ is trivial. Let us show that $(ii) \Rightarrow (i)$. There exists by hypothesis a family (not necessarily finite) $(f_i)_{i \in I}$ of linear forms on M and a family $(m_i)_{i \in I}$ of elements of M such that, for all $x \in M$, the family $(f_i(x))$ has finite support and $x = \sum_i m_i f_i(x)$ (**??**). Since

M is non-degenerate, $f_i(x) = n_i x$ for some $n_i \in (A : N)$ by virtue of Proposition 10.5.19. Taking x as an element of $M \cap S$, it is seen that of necessity $n_i = 0$ except for a finite number of indices and $\sum_i m_i n_i = 1$. This obviously implies $M \cdot (A : M) = A$, whence (i).

By definition we have (iii) implies (iv). Let us show the converse. Since M is non-degenerate, its annihilator is zero by Proposition 10.5.17, then so is the annihilator of $M_{\mathfrak{m}}$. As $M_{\mathfrak{m}}$ is assumed to be a monogenous $A_{\mathfrak{m}}$-module, it is therefore free of rank 1 and it then follows from Theorem 10.5.9 that M is projective of rank 1. □

Corollary 10.5.24. *Every invertible sub-A-module of B is flat and finitely presented.*

Proof. This follows from Theorem 10.5.23(iii). □

Proposition 10.5.25. *Let M, N be two sub-A-modules of B. Suppose that M is invertible.*

(a) The canonical homomorphism $M \otimes_A N \longrightarrow M \cdot N$ is bijective.

(b) $(N : M) = N \cdot (A : M)$ and $N = (N : M) \cdot M$.

Proof. Let i_N be the canonical injection from N to B. Since M is a flat A-module by Corollary 10.5.24, $1 \otimes i_N : M \otimes_A N \longrightarrow M \otimes_A B$ is injective. But, as $B = S^{-1}A$, the B-module $M \otimes_A B$ is equal to $S^{-1}M$ and hence is identified with B since M is non-degenerate. If this identification is made, the image of $1 \otimes i_N$ is $M \cdot N$, whence (a).

Now write $M^{-1} := (A : M)$, then we have

$$M^{-1} \cdot N \subseteq (N : M) = M^{-1} \cdot M \cdot (N : M) \subseteq M^{-1} \cdot N$$

which proves $M^{-1} \cdot N = (N : M)$, whence $N = M \cdot (N : M)$. □

10.5.5 The class group of invertible submodules

Under multiplication, the sub-A-modules of B form a commutative monoid, with A as identity element. Then the invertible modules are the invertible elements and therefore form a commutative group $\mathfrak{I}$. We have seen that the inverse of $M \in \mathfrak{I}$ is $M^{-1} := (A : M)$.

Let $A^\times$ (resp. $B^\times$) be the multiplicative group of invertible elements of A (resp. B) and let i_A^S denote the canonical injection $A \longrightarrow B$. For all $b \in B^\times$, $\theta(b) = bA$ is an invertible sub-A-module. The mapping $\theta : B^\times \longrightarrow \mathfrak{I}$ is a homomorphism whose kernel is $i_A^S(A^\times)$. Its cokernel will be denoted by $\mathfrak{C}$ or $\mathfrak{C}(A)$. The group $\mathfrak{C}$ is called the **group of classes of invertible sub-A-modules** of B. The following exact sequence has been constructed

$$1 \longrightarrow A^\times \xrightarrow{i_A^S} B^\times \xrightarrow{\theta} \mathfrak{I} \xrightarrow{\pi} \mathfrak{C} \longrightarrow 1$$

where 1 denotcs the group consisting only of the identity element and π is the canonical mapping $\mathfrak{I} \longrightarrow \mathfrak{C}$.

As every invertible sub-A-module M of B is projective of rank 1, the element $\mathrm{cl}(M) \in P(A)$ is defined.

Proposition 10.5.26. *The mapping $\mathrm{cl} : \mathfrak{I} \longrightarrow P(A)$ defines, by taking quotients, an isomorphism from $\mathfrak{C}$ onto the kernel of the canonical homomorphism*

$$\phi : P(A) \longrightarrow P(B).$$

In other words, there is an exact sequence

$$1 \longrightarrow A^\times \xrightarrow{i_A^S} B^\times \xrightarrow{\theta} \mathfrak{I} \xrightarrow{\mathrm{cl}} P(A) \xrightarrow{\phi} P(B)$$

Proof. It follows from Proposition 10.5.25 and the definition of addition in $P(A)$ that $\mathrm{cl}(M \cdot N) = \mathrm{cl}(M) + \mathrm{cl}(N)$ for M, N in $\mathfrak{I}$, which shows that cl is a homomorphism. If $M \in \mathfrak{I}$ is isomorphic to A, there exists $b \in B$ such that $M = Ab$ and, as M is invertible, there exists $b' \in B$ such that $bb' = 1$, in othe rwords $b \in B^\times$. The converse is immediate. Hence the kernel of cl is contained in $\theta(B^\times)$.

Let us now determine the image of cl. If $M \in \mathfrak{I}$, then $M \otimes_A B = S^{-1}M = B$, whence $\mathrm{cl}(M) \in \ker \phi$. Conversely, let P be a projective A-module of rank 1 such that $P(B) = P \otimes_A B$ is B-isomorphic to B. As P is a flat A-module, the injection $i : A \to B$ defines an injection $i \otimes i_B : P \to P \otimes_A B = B$ and P is thus identified with a sub-A-module of B. By virtue of Proposition 10.5.17(iii) P is non-degenerate and Theorem 10.5.23 shows that P is invertible. The kernel of ϕ is therefore equal to the image of cl. □

Corollary 10.5.27. *For two invertible sub-A-modules of B to have the same image in $\mathfrak{C}$, it is necessary and sufficient that they be isomorphic.*

Corollary 10.5.28. *If the ring B is semi-local, the group $\mathfrak{C}$ of classes of invertible sub-A-modules of B is canonically identified with the group $P(A)$ of classes of projective A-modules of rank* 1.

Proof. In this case $P(B) = 0$ by Proposition 10.5.13. □

Example 10.5.29. Let A be an integral domain and S is the set of nonzero elements of A, so that B is the field of fractions of A. The invertible sub-A-modules of B are also called in this case **invertible fractional ideals**. Those which are monogenous free A-modules are just the fractional principal ideals.

10.5.6 Exercise

Exercise 10.5.1. let A be a commutative ring. The following are equivalent:

(a) For every prime ideal $\mathfrak{p}$, the localization $A_\mathfrak{p}$ is an integral domain.

(b) For every maximal ideal $\mathfrak{m}$, the localization $A_\mathfrak{m}$ is an integral domain.

(c) For $x, y \in A$ such that $xy = 0$ we have $\mathrm{Ann}(x) + \mathrm{Ann}(y) = A$.

Proof. It is clear that (a) implies (b); for $(b) \Rightarrow (c)$, let $xy = 0$, assume $\mathrm{Ann}(x) + \mathrm{Ann}(y) \subseteq \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$, then $xy/1 = 0$ in $A_\mathfrak{m}$. Then, since $A_\mathfrak{m}$ is an integral domain, we have $x/1 = 0$ or $y/1 = 0$. Assume $x/1 = 0$, then $xs = 0$ for some $s \in A - \mathfrak{m}$. But $\mathrm{Ann}(x) \subseteq \mathfrak{m}$, this is an contradiction. Similar for $y/1 = 0$.

We show that $(c) \Rightarrow (a)$. First we have the following observation: If $\mathfrak{p}$ is a prime ideal, then for any $x \in A$ such that $x/1 \neq 0 \in A_\mathfrak{p}$ then $\mathrm{Ann}(x) \subseteq \mathfrak{p}$. In fact, assume $tx = 0$ for $t \in A$. Then $t \notin A - \mathfrak{p}$, hence $t \in \mathfrak{p}$. Now, suppose that $x/s \cdot y/t = 0 \in A_\mathfrak{p}$. Then $xyz = 0$ for some $z \in A - \mathfrak{p}$. It will suffice to prove that $x/1 = 0$ or $y/1 = 0$. Suppose otherwise, namely that $x/1 \neq 0$ and $y/1 \neq 0$. Then, $xz/1 \neq 0$ since $z/1$ is invertible. By the observation, we know that $\mathrm{Ann}(xz) \subseteq \mathfrak{p}$ and $\mathrm{Ann}(y) \subseteq \mathfrak{p}$, thus $\mathrm{Ann}(x) + \mathrm{Ann}(y) \subseteq \mathfrak{p}$, which is a contradiction. □

Exercise 10.5.2. Let A be a ring. Suppose that, for each prime ideal $\mathfrak{p}$, the local ring $A_\mathfrak{p}$ has no nilpotent element $\neq 0$. Show that A has no nilpotent element $\neq 0$. If each $A_\mathfrak{p}$ is an integral domain, is A necessarily an integral domain?

Proof. By corollary 10.2.38, we have $\mathfrak{n}(A_\mathfrak{p}) = \mathfrak{n}(A)_\mathfrak{p}$ so $\mathfrak{n}(A)_\mathfrak{p} = 0$ for any prime ideal $\mathfrak{p}$. By Proposition 10.3.18, $\mathfrak{n}(A) = 0$.

The answer for next question is no. Suppose that $A = \prod_{i=1}^n k_i$, where $k_i = k$ an algebraic closed field. This is not integral domain, for example $(1, \dots, 0) \cdot (0, \dots, 1) = 0$. Then $\operatorname{Spec}(A) = \{\mathfrak{p}_i := 0 \times \prod_{i \neq j} k_j\}$. Consider the localization $A_{\mathfrak{p}_i}$:

$$A - \mathfrak{p}_i = \{(x_1, \dots, x_n) \in A : x_i \neq 0\}$$

We define a map $\varphi_i : A_{\mathfrak{p}_i} \to k_i$ by

$$\frac{x}{s} \mapsto \frac{x_i}{s_i}$$

This is surjective of course, since we can choose $s_i = 1$. To show the injectivity, let $x_i/s_i = y_i/t_i$, then since k_i is a field, we have

$$x_i t_i = y_i s_i.$$

Let $e_i = (0, \dots, 1, \dots, 0)$, then $e_i \in A - \mathfrak{p}_i$, and

$$e_i(xt - ys) = x_i t_i - y_i s_i = 0$$

so $x/s = y/t$. Hence φ_j is an isomorphism. In particular, $A_{\mathfrak{p}_i}$ is an integral domain. □

Exercise 10.5.3. Let A be a ring and let Σ be the set of all multiplicatively closed subsets S of A such that $0 \notin S$. Show that Σ has maximal elements, and that $S \in \Sigma$ is maximal if and only if $A - S$ is a minimal prime ideal of A.

Moreover, by replace 0 with any ideal I, we can show $S \in \Sigma$ is maximal if and only if $A - \mathfrak{p}$ is a minimal prime ideal among those containing I.

Proof. By Zorn's lemma, Σ has a maximal element. For any set $S \in \Sigma$, it is clear that $A - S$ has the prime property. When S is maximal in Σ, we claim that $A - S$ is an ideal. Let $a \in A$, consider the smallest multiplicatively closed subsets containing a and S: When $a \in S$, it is S, and when $a \notin S$, it is

$$S_a := \{sa^n : s \in S, n \in \mathbb{N}\}$$

Now assume $a, b \in A - s$, then S_a and S_b both contains S properly. By the maximality, $0 \in S_a, S_b$, so there are $s_a, s_b \in S, m, n \in \mathbb{N}$ such that

$$s_a a^n = s_b b^m = 0$$

Now assume $a + b \in S$, then $s_a s_b(a + b) \in S$. Consider the power

$$(s_a s_b(a + b))^{m+n} = (s_a s_b)^{m+n}(a + b)^{m+n} = 0$$

since every term of the sum is zero. This is a contradiction since $(s_a s_b(a + b))^{m+n} \in S$. So $a + b \in A - S$.

Let $r \in A$ and $a \notin S$. If $ra \in S$, then $rs_a a \in S$, and $(rs_a a)^n = 0 \in S$, contradiction. Hence $A - S$ is a prime ideal. Since for any prime ideal $\mathfrak{p}$, $A - \mathfrak{p}$ is multiplicatively closed and does not contain (0), it follows that $A - S$ is minimal.

Now assume $\mathfrak{p}$ is a minimal prime ideal, then $A - \mathfrak{p} \in \Sigma$. By Zorn's lemma, there is a maximal elements $T \in \Sigma$ such that $A - \mathfrak{p} \subseteq T$. Then $A - T$ is prime and contained in $\mathfrak{p}$, by assumption we have $T = A - \mathfrak{p}$. So $A - \mathfrak{p}$ is maximal. □

Exercise 10.5.4. Let A be an integral domain and M an A-module. An element $x \in M$ is a torsion element of M if $\mathrm{Ann}(x) \neq 0$, that is if x is killed by some non-zero element of A.

Show that the torsion elements of M form a submodule of M. This submodule is called the **torsion submodule** of M and is denoted by $T(M)$. If $T(M) = 0$, the module M is said to be torsion-free. Show that

(a) If M is any A-module, then $M/T(M)$ is torsion-free.

(b) If $f : M \to N$ is a module homomorphism, then $f(T(M)) \subseteq T(N)$.

(c) The functor T is left-exact.

(d) If M is any A-module, then $T(M)$ is the kernel of the mapping $x \mapsto 1 \otimes x$ of M into $K \otimes_A M$, where K is the field of fractions of A.

Proof. Let

$$0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N$$

be an exact sequence. Consider the sequence

$$0 \longrightarrow T(L) \xrightarrow{T(f)} T(M) \xrightarrow{T(g)} T(N)$$

where $T(f) = f|_{T(M)}$. Clearly $T(g) \circ T(f) = 0$. Since we have $\ker T(f) \subseteq \ker f$, we see $T(f)$ is injective.

Let $m \in \ker T(g)$, then m is also in $\ker g$, so there is $\ell \in L$ such that $f(\ell) = m$. m is torsion, so there is $r \in A$ such that $rm = 0$. Then $f(r\ell) = rf(\ell) = rm = 0$, and $r\ell = 0$ since f is injective. This implies $\ell \in T(L)$, so $T(f)(\ell) = m$.

Let $S = A - \{0\}$, then we have

$$(K \otimes_A M = S^{-1}A \otimes_A M = A \otimes_{S^{-1}A} S^{-1}M \cong S^{-1}M).$$

Now $1 \otimes m$ is $m/1$ in $S^{-1}M$, so $1 \otimes m = 0$ if and only if there is $a \in A$ such that $am = 0$. □

Exercise 10.5.5. Let S be a multiplicatively closed subset of an integral domain A. Show that $T(S^{-1}M) = S^{-1}T(M)$. Deduce that the following are equivalent:

(a) M is torsion-free.

(b) $M_{\mathfrak{p}}$ is torsion-free for all prime ideals $\mathfrak{p}$.

(c) $M_{\mathfrak{m}}$ is torsion-free for all maximal ideals $\mathfrak{m}$.

Proof. Let $m/s \in T(S^{-1}M)$, then there is $y/t \in S^{-1}A$ such that $ym/st = 0$. Hence $\exists u \in S$ such that

$$uym = 0$$

This implies $m \in T(m)$, so $m/s \in S^{-1}T(M)$.

Let $m/s \in S^{-1}T(M)$. Then there is $r \in A : rm = 0$. Then $r/1 \cdot m/s = 0$ so $m/s \in T(S^{-1}M)$.

M is torsion free if and only if $T(M) = 0$. Use Proposition 10.3.18. □

Chapter 11

Graded rings and filtrations

11.1 Graduation on rings and modules

11.1.1 Graded ring and graded module

Definition 11.1.1. *Given an abelian group G and a set Δ, a **graduation** of type Δ on G is a family $(G_\lambda)_{\lambda\in\Delta}$, of which G is the direct sum. The set G with the structure defined by its group law and the graduation is called a **graded group** of type Δ.*

The set Δ is called the **set ef degrees** of G. An element $x \in G$ is called **homogeneous** if it belongs to one of the G_λ, **homogeneous of degree $\boldsymbol{\lambda}$** if $x \in G_\lambda$. The element 0 is therefore homogeneous of all degrees; but if $x \neq 0$ is homogeneous, it belongs to only one of the G_λ; the index λ such that $x \in G_\lambda$ is then called the degree of x (or sometimes the weight of x) and is sometimes denoted by $\deg(x)$. Every $x \in G$ may be written uniquely as a sum $\sum_\lambda x_\lambda$ of homogeneous elements with $x_\lambda \in G_\lambda$; y_λ is called the **homogeneous component** of degree λ, or simply the component of degree λ of x.

Example 11.1.2. Given any commutative monoid Δ with identity element 0 and abelian group G, a graduation $(G_\lambda)_{\lambda\in\Delta}$ is defined on G by taking $G_0 = G$ and $G_\lambda = \{0\}$ for $\lambda \neq 0$; this graduation is called **trivial**.

Example 11.1.3. Let Δ and Δ' be two sets and ρ a mapping of Δ into Δ'. Let $(G_\lambda)_{\lambda\in\Delta}$ be a graduation of type Δ on a commutative group G; for $\mu \in \Delta'$, let G_μ be the sum of the G_λ's such that $\rho(\lambda) = \mu$; clearly $(G_\mu)_{\mu\in\Delta'}$ is a graduation of type Δ' on G, said to be **derived** from (G_λ) by means of the mapping ρ.

When Δ is a commutative group written additively and ρ the mapping $\lambda \mapsto -\lambda$ of Δ onto itself, (G_μ) is called the **opposite graduation** of (G_λ).

Example 11.1.4. If $\Delta = \Delta_1 \times \Delta_2$ is a product of two sets, a graduation of type Δ is called a **bigraduation** of types Δ_1, Δ_2. For all $\lambda \in \Delta_1$, let $G_\lambda = \bigoplus_{\mu\in\Delta_2} G_{\lambda\mu}$; for all $\mu \in \Delta_2$, let $G_\mu = \bigoplus_{\lambda\in\Delta_1} G_{\lambda\mu}$; clearly $(G_\lambda)_{\lambda\in\Delta_1}$ is a graduation of type Δ_1 and $(G_\mu)_{\mu\in\Delta_2}$ is a graduation of type Δ_2 on G; these graduations are called the **partial graduations** derived from the bigraduation $(G_{\lambda\mu})$. Note that $G_{\lambda\mu} = G_\lambda \cap G_\mu$. Conversely, if $(G_\lambda)_{\lambda\in\Delta_1}$ and $(G_\mu)_{\mu\in\Delta_2}$ are two graduations on G such that G is the direct sum of the $G_{\lambda\mu} = G_\lambda \cap G_\mu$, these subgroups form a bigraduation of types Δ_1, Δ_2 on G, of which $(G_\lambda)_{\lambda\in\Delta_1}$ and $(G_\mu)_{\mu\in\Delta_2}$ are the partial graduations.

Example 11.1.5. Let Δ_0 be a commutative monoid written additively, with identity element denoted by 0; let I be any set and $\Delta_0^{\oplus I}$ denote the submonoid of the product set Δ_0^I consisting of the families $(\lambda_i)_{i\in I}$ of finite support. Let $\rho : \Delta \to \Delta_0$ be the surjective (codiagonal) homomorphism of Δ into Δ_0 defined by $\rho((\lambda_i)) = \sum_i \lambda_i$. From every graduation of type Δ a graduation of type Δ_0 is derived by means of ρ; it is called the **total graduation** associated with the given "multigraduation" of type Δ.

Often the set Δ may also endow some algebraic structure and one want to have operations between different components of the graduation (G_λ). In the following, we may always assume that Δ is a commutative monoid, and consider graduations of type Δ on rings and modules.

Definition 11.1.6. *Let Δ be a commutative moniod. Given a ring A and a graduation (A_λ) of type Δ on the additwe group A, this graduation is said to be **compatible** with the ring structure on A if*

$$A_\lambda A_\mu \subseteq A_{\mu+\lambda} \quad \textit{for all } \lambda, \mu \in \Delta.$$

*The ring A with this graduation is called a **graded ring** of type Δ.*

Proposition 11.1.7. *If the elements of Δ are cancellable and (A_λ) is a graduation of type Δ compatible with the structure of a ring A, then A_0 is a subring of A.*

Proof. As $A_0A_0 \subseteq A_0$, by definition, it suffices to prove that $1 \in A_0$. Let $1 = \sum_{\lambda\in\Delta} e_\lambda$ be the decomposition of 1 into its homogeneous components. If $x \in A_\mu$ then $x = x \cdot 1 = \sum_\lambda xe_\lambda$; comparing the components of degree μ, (since every element in Δ is cancellable) we get $x = xe_0$. Since this relation is true for every homogeneous element of A, it is true for all $x \in A$; in particular $1 = 1 \cdot e_0 = e_0 \in A_0$. □

Definition 11.1.8. *Let A be a graded ring of type Δ, (A_λ) its graduation and M a left A-module; a graduation (M_λ) of type Δ on the addition group M is compatible with the A-module structure on M if*

$$A_\lambda M_\mu \subseteq M_{\lambda+\mu} \quad \textit{for all } \lambda, \mu \in \Delta.$$

*The module M with this graduation is then called a **graded module** of type Δ over the graded ring A.*

When the elements of Δ are cancellable, it follows from Proposition 11.1.7 that the M_λ are A_0-modules. Clearly if A is a graded ring of type Δ, the A is itself a left graded A-module of type Δ.

Let A be a graded ring and M be a graded A-module. An element $x \in M$ is **homogeneous** if $x \in M_\lambda$ for some λ, and λ is then called the **degree** of x. A general element $x \in M$ can be written uniquely in the form $x = \sum_\lambda x_\lambda$ with $x_i \in M_\lambda$; x_λ is called the **homogeneous term of x of degree λ**.

Example 11.1.9. On any ring A the trivial graduation of type Δ is compatible with the ring structure. If A is graded by the trivial graduation, for a graduation (M_λ) of type Δ on an A-module M to be compatible with the A-module structure, it is necessary and sufficient that the M_λ be submodules of M.

Example 11.1.10. Let A be a graded ring of type Δ, M a graded A-module of type Δ and ρ a homomorphism of Δ into a commutative monoid Δ' whose identity element is denoted by 0.

Then A is a graded ring of type Δ' and M a graded module of type Δ' for the graduations of type Δ' derived from ρ and the graduations of type Δ on A and M: this follows immediately from the relation $\rho(\lambda + \mu) = \rho(\lambda) + \rho(\mu)$.

In particular, if $\Delta = A_1 \times A_2$ is a product of two commutative monoids, the projections π_1 and π_2 are homomorphisms and the corresponding graduations are just the parlial graduations derived from the graduations of type Δ; these partial graduations are thus compatible with the ring structure of A and the module structure of M. Similarly, if $\Delta = \Delta_0^{\oplus I}$ (where Δ_0 is a commutative monoid with identity element denoted by 0), the total graduation of type Δ_0 derived from the graduation of type Δ on A (resp. M) by means of the codiagonal homomorphism is compatible with the ring structure on A (resp. with the module structure on M).

Example 11.1.11. Let A be a graded ring of type Δ, M a graded A-module of type Δ and A_0 an element of Δ; for $\lambda \in \Delta$, let $M'_\lambda = M_{\lambda+\lambda_0}$, and let M' be the submodule $M' = \bigoplus_{\lambda\in\Delta} M'_\lambda$ is an A-module and the M'_λ form on M' a graduation of type A compatible with the A-module structure of M'; the graded A-module M' of type Δ thus defined is said to be obtained by shifting by λ_0 the graduation of M and it is denoted by $M(\lambda_0)$. When Δ is a group, the underlying A-module of the graded A-module M' is identified with M since in this case $\lambda \mapsto \lambda + \lambda_0$ is an isomorphism of Δ onto itself.

Example 11.1.12. Let A be a ring. The polynomial ring $A[X]$ in one indeterminate is graded of type $\mathbb{N}$ by the subgroups AX^n. Similarly, the polynomial ring $A[X_1, \dots, X_n]$ is graded of type $\mathbb{N}$ by the subgroups of homogeneous polynomials.

The graduations most often used are of type $\mathbb{Z}$ or of type $\mathbb{Z}^n$; when we speak of graded (resp. bigraded, trigraded, etc.) modules and rings without mentioning the type, it is understood that we mean graduations of type $\mathbb{Z}$ (resp. $\mathbb{Z}^2$, $\mathbb{Z}^3$ etc.); a graded ring (resp. module) of type $\mathbb{N}$ is also called a **graded ring (resp. module) with positive degrees**.

Now we introduce the morphisms between graded rings and modules.

Definition 11.1.13. *Let A, B be two graded rings with the same type Δ. and (A_λ), (B_λ) their respective graduations. A ring homomorphism $\rho : A \to B$ is called **graded** if $\rho(A_\lambda) \subseteq B_\lambda$ for all $\lambda \in \Delta$.*

*Let M, N be two graded modules of type Δ over a graded ring A of type Δ. Let $\phi : M \to N$ be an A-homomorphism and δ an element of Δ; ϕ is called **graded of degree δ** if $\phi(M_\lambda) \subseteq N_{\lambda+\delta}$ for all $\lambda \in \Delta$.*

An A-homomorphism $\phi : M \to N$ is called **graded** if there exists $\delta \in \Delta$ such that ϕ is graded of degree δ. If $\phi \neq 0$ and every element of Δ is cancellable, then the degree δ of ϕ is uniquely determined.

If $\rho : A \to B$ and $\nu : B \to C$ are two graded homomorphisms of graded rings of type Δ, so is $\nu \circ \rho : A \to B$; for a mapping $\rho : A \to B$ to be a graded ring isomorphism, it is necessary and sufficient that ρ be bijective and that ρ and the inverse mapping ρ^{-1} be graded homomorphisms. It also suffices for this that f be a bijective graded homomorphism. Thus it is seen that graded homomorphisms can be taken as the morphisms of the category of graded ring structure of type Δ.

Similarly, if $\phi : M \to N$ and $\psi : N \to P$ are two graded homomorphisms of graded A-modules of type Δ of respective degrees δ and γ, $\psi \circ \phi : M \to P$ is a graded homomorphism of degree $\delta + \gamma$. If δ admits an inverse $-\delta$ in Δ and $\phi : M \to N$ is a bijective graded homomorphism of degree δ, the inverse mapping $\phi^{-1} : N \to M$ is a bijective graded homomorphism

of degree $-\delta$. It follows as above that the graded homomorphisms of degree 0 can be taken as the morphisms of the category of graded A-module of type Δ.

Example 11.1.14. If M is a graded A-module and $M(\lambda_0)$ is a graded A-module obtained by shifting, the $\mathbb{Z}$-linear mapping of $M(\lambda_0)$ into M which coincides with the canonical injection on each $M_{\lambda+\lambda_0}$ is a graded homomorphism of degree λ_0 (which is bijective when Δ is a group).

Example 11.1.15. If a is a homogeneous element of degree δ belonging to the centre of A, the homothety $x \mapsto ax$ of any graded A-module M is a graded homomorphism of degree δ.

Remark 11.1.1. A graded A-module M is called a graded free A-module if there exists a basis $(x_i)_{i\in I}$ of M consisting of homogeneous elements. Suppose it is and Δ is a commutative group; let λ_i be the degree of x_i and consider for each i the shifted A-module $A(-\lambda_i)$; if e_i denotes the element 1 of A considered as an element of degree λ_i in $A(-\lambda_i)$, the A-linear mapping $\phi : \bigoplus_{i\in I} A(-\lambda_i) \to M$ such that $\phi(e_i) = x_i$ for all i is a graded A-module isomorphism.

Example 11.1.16. A direct system $(A_\alpha, f_{\beta\alpha})$ of graded rings of type Δ is a direct system of rings such that each A_α is graded of type Δ and each $f_{\beta\alpha}$ is a homomorphism of graded ring. If (A_α^λ) is the graduation of A_α and we write

$$A = \varinjlim A_\alpha, \quad A^\lambda = \varinjlim A_\alpha^\lambda,$$

it follows that (A^λ) is a graduation of A and this graduation is compatible with the ring structure on A. The graded ring A is called the **direct limit** of the direct system of graded rings $(A_\alpha, f_{\beta\alpha})$. If $f_\alpha : A_\alpha \to A$ is the canonical mapping, then f_α is a homomorphism of graded rings.

Similarly, a direct system $(M_\alpha, \phi_{\beta\alpha})$ of graded A-modules of type Δ is a direct system of A-modules such that each M_α is graded of type Δ and each $\phi_{\beta\alpha}$ is a homomorphism of graded A-modules of degree 0. If (M_α^λ) is the graduation of M_α and

$$M = \varinjlim M_\alpha, \quad M^\lambda = \varinjlim M_\alpha^\lambda,$$

then (M^λ) is a graduation of M and this graduation is compatible with the module structure on M. The graded module M is called the **direct limit** of the direct system of graded A-modules $(M_\alpha, \phi_{\beta\alpha})$. If $\phi_\alpha : M_\alpha \to M$ is the canonical mapping, then ϕ_α is a homomorphism of graded modules of degree 0.

Proposition 11.1.17. *Let A be a graded ring of type Δ, M a graded A-module of type Δ, (M_λ) its graduation and N a sub-A-module of M. The following properties are equivalent:*

(i) $N = \bigoplus_\lambda (N \cap M_\lambda)$.

(ii) The homogeneous components of every element of N belongs to N

(iii) N can be generated by homogeneous elements.

Proof. Every element of N can be written uniquely as a sum of elements of the M_λ, and hence it is immediate that (i) and (ii) are equivalent and that (i) implies (iii). We show that (iii) implies (ii). Then let $(x_i)_{i\in I}$ be a family of homogeneous generators of N and let δ_i be the degree of x_i.

Every element of N can be written as $\sum_i a_i x_i$ with $a_i \in A$; if $a_{i\mu}$ is the component of a_i of degree μ, the conclusion follows from the relation

$$\sum_{i\in I}\Big(\sum_{\mu\in\Delta} a_{i\mu}x_i\Big) = \sum_{\mu\in\Delta}\Big(\sum_{\mu+\delta_i=\lambda} a_{i\mu}x_i\Big).$$

This completes the proof. □

When a submodule N of M has the equivalent properties stated in Proposition 11.1.17, clearly the $N \cap M_\lambda$ form a graduation compatible with the A-module structure of N, called the graduatuin imluced by that on M; N with this graduation is called a graded submodule of M.

Corollary 11.1.18. *If N is a graded submodule of M and (x_i) is a generating system of N, then the homogeneous componmts of the (x_i) form a genetating system of N.*

Corollary 11.1.19. *If N is a finitely generated submodule of M, then N admits a finite generating system consists of homogeneous elements.*

A graded submodule of A is called a **graded ideal** of the graded ring A. For every subring B of A, if we set $B_\lambda = B \cap A_\lambda$ then $B_\lambda B_\mu \subseteq B_{\lambda+\mu}$, thus the graduation induced on B by that on A is compatible with the ring structure on B; B is then called a **graded subring** of A.

If N is a graded submodule of a graded A-module M and $(M_\lambda)_{\lambda\in\Delta}$ is the graduation of M, the submodules $(M_\lambda + N)/N$ of M/N form a gnoduation compatible with the structure of this quotient module. For, if $N_\lambda = M_\lambda \cap N$, then $(M_\lambda + N)/N$ is identified with M_λ/N_λ and it follows from Proposition 11.1.17 that M/N is their direct sum. Moreover,

$$A_\lambda(M_\mu + N) \subseteq A_\lambda M_\mu + N \subseteq M_{\lambda+\mu} + N$$

which establishes our assertion. The graduation $((M_\lambda + N)/N)_{\lambda\in\Delta}$ is called the **quotient graduation** of that on M by N and the quotient module M/N with this graduation is called the **graded quotient module** of M by the graded submodule N; the canonical homomorphism $\pi : M \to M/N$ is a graded homomorphism of degree 0 for this graduation.

If $\mathfrak{a}$ is a graded ideal of A, the quotient graduation on $A/\mathfrak{a}$ is compatible with the ring structure on $A/\mathfrak{a}$. The ring $A/\mathfrak{a}$ with this graduation is called the **quotient graded ring** of A by $\mathfrak{a}$. The canonical homomorphism $\pi : A \to A/\mathfrak{a}$ is a homomorphism of graded rings for this graduation.

Proposition 11.1.20. *Let A be a graded ring of type Δ, M and N two graded A-modules of type Δ and $\phi : M \to N$ a graded A-homomorphism of degree δ. Then:*

(a) $\operatorname{im}\phi$ *is a graded submodule of N.*

(b) If δ is a regular element of Δ, then $\ker\phi$ *is a graded submodule of M.*

(c) If $\delta = 0$, the bijection $M/\ker\phi \to \operatorname{im}\phi$ canonically associated with ϕ is an isomorphism of graded modules.

Proof. Assertion (a) follows immediately from the definitions and Proposition 11.1.17(iii). If x is an element of M such that $\phi(x) = 0$ and $x = \sum x_\lambda$ is its decomposition into homogeneous

components (where x_λ is of degree λ), then

$$\sum_\lambda \phi(x_\lambda) = \phi(x) = 0$$

and $\phi(x_\lambda)$ is of degree $\lambda + \delta$; if δ is regular the relation $\lambda + \delta = \mu + \delta$ implies $\lambda = \mu$, hence the $\phi(x_\lambda)$ are the homogeneous components of $\phi(x)$ and necessarily $\phi(x_\lambda) = 0$ for all $\lambda \in \Delta$, which proves (b). The bijection $\pi : M/\ker\phi \to \operatorname{im}\phi$ canonically associated with ϕ is then a graded homomorphism of degree δ, as follows from the definition of the quotient graduation; whence (c) when $\delta = 0$. □

Corollary 11.1.21. *Let A, B be two graded rings of type Δ and $\rho : A \to B$ a graded homomorphism of graded rings. Then* $\operatorname{im}\rho$ *is a graded subring of B,* $\ker\rho$ *a graded ideal of type Δ and the bijection* $A/\ker\rho \to \operatorname{im}\rho$ *canonically associated with ρ is an isomorphism of graded rings.*

Proof. It suffices to apply Proposition 11.1.20 to ρ considered as a homomorphism of degree 0 of graded $\mathbb{Z}$-modules. □

Proposition 11.1.22. *Let A be a graded ring of type Δ and M a graded A-module of type Δ.*

(a) Every sum and every intersection of graded submodules of M is a graded submodule.

(b) If x is a homogeneous element of M of degree μ which is cancellable in Δ, then the annihilator of x is a graded ideal of A.

(c) If the elements of Δ are cancellable, the annihilator ef a graded submodule of M is a graded ideal of A.

Proof. If (N_i) is a family of graded submodules of M, property (iii) of Proposition 11.1.17 shows that the sum of the N_i is generated by homogeneous elements and property (ii) of Proposition 11.1.17 proves that the homogeneous components of every element of $\bigcap_i N_i$ belongs to $\bigcap_i N_i$; whence (a).

To prove (b), it suffices to note that $\operatorname{Ann}(x)$ is the kernel of the homomorphism $a \mapsto ax$ of the A-module A into M and that this homomorphism is graded of degree μ; the conclusion follows from Proposition 11.1.20(b). Finally (c) is a consequence of (a) and (b) for the annihilator of a graded submodule N of M is the intersection of the annihilators of the homogeneous elements of N, by virtue of Proposition 11.1.17. □

Example 11.1.23. Let M be a graded A-module and E a submodule of M; it follows from Proposition 11.1.22(a) that there exists a largest graded submodule N_1 of M contained in E and a smallest graded submodule N_2 of M containing E; N_1 is the set of $x \in E$ all of whose homogeneous components belong to E and N_2 is the submodule of M generated by the homogeneous components of a generating system of E.

Let Δ be a commutative monoid, A a graded ring of type Δ, $(A_\lambda)_{\lambda\in\Delta}$ its graduation and E an A-algebra. A graduation $(E_\lambda)_{\lambda\in\Delta}$ of type Δ on the additive group E is said to be **compatible** with the A-algebra structure on E if it is compatible both with the A-module and with the ring structure on E, in other words, if, for all λ, μ in Δ,

$$A_\lambda E_\mu \subseteq E_{\lambda+\mu}, \quad E_\lambda E_\mu \subseteq E_{\lambda+\mu}. \tag{1.1.1}$$

The A-algebra E, with this graduntion, is then called a **graded algebra** of type Δ over the graded ring A.

When the graduation on A is trivial (that is, $A_0 = A$, $A_\lambda = \{0\}$ for $\lambda \neq 0$), condition (1.1.1) means that the E_λ are sub-A-modules of E. This leads to the definition of the notion of graded algebra of type Δ over a non-graded commutative ring A: A is given the trivial graduation of type Δ and the above definition is applied.

When we consider graded A-algebras E with a unit element 1, it will always be understood that 1 is of degree 0. It follows that if an invertible element $x \in E$ is homogeneous and of degree p, its inverse x^{-1} is homogeneous and of degree $-p$: it suffice to decompose x^{-1} as a sum of homogeneous elements in the relation $x^{-1}x = xx^{-1} = 1$.

Let E and F be two graded algebras of type Δ over a graded ring A of type Δ. An A-algebra homomorphism $u : E \to F$ is called a **graded algebra homomorphism** is $u(E_\lambda) \subseteq F_\lambda$ for all $\lambda \in \Delta$ (where (E_λ) and (F_λ) denote the respective graduations of E and F); where E and F are associative and unital and u is unital, this condition means that u is a graded ring homomorphism.

Remark 11.1.2. Let E be a graded A-algebra of type $\mathbb{N}$. Then E often is identified with a graded A-algebra of type $\mathbb{Z}$ by writing $E_n = \{0\}$ for $n < 0$.

Remark 11.1.3. The definition can also be interpreted by saying that E is a graded A-module and that A-linear map

$$m : E \otimes_A E \to E$$

defining the multiplication on E, is homogeneous of degree 0 when $E \otimes_A E$ is given its graduation of type Δ.

To define a graded A-algebra structure of type Δ on the graded ring A, with E as underlying graded A-module, therefore amounts to defining for each ordered pair (λ, μ) of elements of Δ a $\mathbb{Z}$-bilinear map

$$m_{\lambda\mu} : E_\lambda \times E_\mu \to E_{\lambda+\mu}$$

such that for every triple of indices (λ, μ, ν) and for $\alpha \in A_\lambda$, $x \in E_\mu$, $y \in E_\mu$, we have $\alpha m_{\mu\nu}(x, y) = m_{\lambda+\mu,\nu}(\alpha x, y) = m_{\mu,\lambda+\nu}(x, \alpha y)$.

Example 11.1.24.

(a) Let B be a graded ring of type Δ; if B is given its canonical $\mathbb{Z}$-algebra structure, B is a graded A-algebra ($\mathbb{Z}$ being given the trivial graduation).

(b) Let M be a magma and $\phi : M \to \Delta$ a homomorphism. For all $\lambda \in \Delta$, we write $M_\lambda = \phi^{-1}(\lambda)$; then $M_\lambda M_\nu \subseteq M_{\lambda+\mu}$. Let A be a graded commutative ring of type Δ and $(A_\lambda)_{\lambda\in\Delta}$ its graduation; we shall define a graded A-algebra structure on the algebra $E = A^{\oplus M}$ of the magma M. To this end, let E_λ denote the additive subgroup of E generated by the elements of the form αm such that $\alpha \in A_\mu$, $m \in M_\nu$, and $\mu + \nu = \lambda$. As the M_λ are pairwise disjoint, E is the direct sum of the $A_\mu M_\nu$ and hence is the direct sum of E_λ and it is immediate that E_λ satisfy the condition (1.1.1). Therefore it defines on E the desired graded A-algebra structure. If M admits an identity element e, it may also be supposed that $\phi(e) = 0$. A particular case is the one where the graduation of the ring A is trivial; then E_λ is the sub-A-module of E generated by M_λ. More particularly, if we take

$M = \mathbb{N}^{\oplus I}$, $\Delta = \mathbb{N}$ and ϕ the map such that $\phi((n_i)) = \sum_i n_i$, the ring A having the trivial graduation, a graduation is thus obtained on the polynomial algebra $A[X_i]_{i\in I}$, for which the degree of a homogeneous polynomial is the total degree.

We now take M to be the free monoid $\Delta(X)$ of a set X and ϕ the homomorphism $\Delta(X) \to \mathbb{N}$ which associates with each word its length. Thus a graded A-algebra structure is obtained on the free associated algebra of the set X.

Let E be a graded algebra of type Δ over a graded ring A of type Δ. If F is a sub-A-algebra of E which is a graded sub-A-module, then the graduation (F_λ) on F is compatible with its A-algebra structure, since $F_\lambda = F \cap E_\lambda$; in this case F is called a graded subalgebra of E and the canonical injection $F \to E$ is a graded algebra homomorphism.

Similarly, if $\mathfrak{a}$ is a left (resp. right) ideal of E which is a graded sub-A-module, then $E_\lambda \mathfrak{a}_\mu \subseteq \mathfrak{a}_{\lambda+\mu}$ (resp. $\mathfrak{a}_\lambda E_\mu \subseteq \mathfrak{a}_{\lambda+\mu}$), since $\mathfrak{a}_\lambda = \mathfrak{a} \cap E_\lambda$; then $\mathfrak{a}$ is called a graded ideal of the algebra E. If $\mathfrak{b}$ is a graded two-sided ideal of E the quotient graduation on the module $E/\mathfrak{b}$ is compatible with the algebra structure on $E/\mathfrak{b}$ and the canonical homomorphism $E \to E/\mathfrak{b}$ is a graded algebra homomorphism.

If $u : E \to F$ is a graded algebra homomorphism, then $\operatorname{im}(u)$ is a graded sub-algebra of F and $\ker u$ is a graded two-sided ideal of E and the bijection $E/\ker u \to \operatorname{im} u$ canonically associated with u is a graded algebra isomorphism.

Proposition 11.1.25. *Let A be a graded commutative ring of type Δ, E a graded A-algebra of type Δ and S a set of homogeneous elements of E. Then the sub-A-algebra (resp. left ideal, right ideal, two-sided ideal) generated by S is a graded subalgebra (resp. graded ideal).*

Proof. The subalgebra of E generated by S is the sub-A-module generated by the finite products of elements of S, which are homogeneous. Simialrly, the left (resp. right) ideal generated by S is the sub-A-module generated by the elements of the form $u_1(u_2(\cdots(u_n s))\cdots)$ (resp. $(\cdots((s u_n)u_{n-1})\cdots)u_2)u_1$ where $s \in S$ and the $u_j \in E$ are homogeneous and these products are homogeneous, whence in the case the conclusion by Proposition 11.1.17. Finally, the two-sided ideal generated by S is the union of the sequence $(\mathfrak{J}_n)_{n\geq 1}$, where $\mathfrak{J}_1$ is the left ideal generated by S and $\mathfrak{J}_{2n}$ (resp. $\mathfrak{J}_{2n+1}$) is the right (resp. left) ideal generated by $\mathfrak{J}_{2n-1}$ (resp. $\mathfrak{J}_{2n}$), which completes the proof. □

Let $(A_\alpha, \phi_{\beta\alpha})$ is a directed direct system of graded commutative rings of type Δ and for each α let E_α be a graded A_α-algebra of type Δ; for $\alpha \leq \beta$ let $f_{\beta\alpha} : E_\alpha \to E_\beta$ be an A_α-homomorphism of graded algebras and suppose that $f_{\gamma\alpha} = f_{\gamma\beta} \circ f_{\beta\alpha}$ for $\alpha \leq \beta \leq \gamma$; then we shall write $(E_\alpha, f_{\beta\alpha})$ a directed direct system of graded algebras of type Δ over the directed direct system $(A_\alpha, \phi_{\beta\alpha})$ of graded commutative rings of type Δ. Then we know that $E = \varinjlim E_\alpha$ has canonically a graded module structure of type Δ over the graded ring $A = \varinjlim A_\alpha$ and a multiplication such that $E^\lambda E^\mu \subseteq E^{\lambda+\mu}$ (where (E^λ) denotes the graduation on E); then this multiplication and the graded A-module structure on E define on E a graded A-algebra structure of type Δ. The set E with this structure is called a direct limit of the direct system $(E_\alpha, f_{\beta\alpha})$ of graded algebras. Moreover, if F is a graded A-algebra of type Δ and (u_α) a direct system of A_α-homomorphism $u_\alpha : E_\alpha \to F$, $u = \varinjlim u_\alpha$ is an A-homomorphism of graded algebras.

11.1.2 Graduation on tensor products and Hom sets

Let Δ be a commutative monoid with its identity element denoted by 0, A a graded ring of type Δ and M, N graded A-modules of type Δ. Let (A_λ) (resp. (M_λ), (N_λ)) be the graduation of A (resp. M, N); the tensor product $M \otimes_{\mathbb{Z}} N$ of the $\mathbb{Z}$-modules M and N is the direct sum of the $M_\lambda \otimes_{\mathbb{Z}} N_\mu$ and hence the latter form a bigraduation of types Δ, Δ on this $\mathbb{Z}$-module. Consider on $M \otimes_{\mathbb{Z}} N$ the total graduation of type Δ associated with this bigraduation; it consists of the sub-$\mathbb{Z}$-modules $P_\lambda = \sum_{\mu+\nu=\lambda}(M_\mu \otimes_{\mathbb{Z}} N_\nu)$. It is known that the $\mathbb{Z}$-module $M \otimes_A N$ is the quotient of $M \otimes_{\mathbb{Z}} N$ by the sub-$\mathbb{Z}$-module Q generated by the elements $(ax) \otimes y - x \otimes (ay)$, where $x \in M$, $y \in N$ and $a \in A$; if, for all $\lambda \in \Delta$, x_λ, y_λ, a_λ are the homogeneous components of degree λ of x, y, a respectively, clearly $(ax) \otimes y - x \otimes (ay)$ is the sum of the homogeneous elements $(a_\nu x_\mu) \otimes y_\lambda - x_\mu \otimes (a_\nu y_\lambda)$, in other words Q is a graded sub-$\mathbb{Z}$-module of $M \otimes_{\mathbb{Z}} N$ and the quotient

$$M \otimes_A N = (M \otimes_{\mathbb{Z}} N)/Q$$

therefore has canonically a graded $\mathbb{Z}$-module structure of type Δ. Moreover, the graduation which we have just defined on $M \otimes_A N$ is compatible with its A-module structure. For if $x \in M_\lambda$, $y \in N_\mu$, $a \in A_\nu$, the element $a(x \otimes y)$ belong to $(M \otimes_{\mathbb{Z}} N)_{\lambda+\mu+\nu}$ and hence its image in $M \otimes_A N$ belongs to $(M \otimes_A N)_{\lambda+\mu+\nu}$, which establishes our assertion. When we speak of $M \otimes_A N$ as a graded A-module, we always mean with the structure thus defined, unless otherwise mentioned. Note that $(M \otimes_A N)$ can be defined as the additive group of $M \otimes_A N$ generated by the $x_\mu \otimes y_\nu$, where $x_\mu \in M_\mu$, $y_\nu \in N_\nu$ and $\mu + \nu = \lambda$.

Let M' (resp. N') be another graded A-module and $\phi : M \to M'$, $\psi : N \to N'$ graded homomorphisms of respective degrees α and β. Then it follows immediately from the above remark that $\phi \otimes \psi$ is a graded A-module homomorphism of degree $\alpha + \beta$.

Similarly, a graduation (compatible with the A-module structure) is similarly defined on the tensor product of any finite number of graded A-modules; it is moreover immediate that the associativity isomorphisms such as $(M \otimes N) \otimes P \to M \otimes (N \otimes P)$ are isomorphisms of graded modules.

Proposition 11.1.26. *Let M and N be graded A-modules of type Δ, P a graded A-module of type Δ and let f be a A-bilinear map of $M \times N$ to P such that*

$$f(x_\lambda, y_\mu) \in P_{\lambda+\mu} \quad \textit{for } x_\lambda \in M_\lambda,\ y_\nu \in N_\mu,\ \lambda, \mu \in \Delta.$$

Then $f(x, y) = \tilde{f}(x \otimes y)$ where $\tilde{f} : M \otimes_A N \to P$ is a graded A-module homomorphism of degree 0.

Proof. It is clear that $\tilde{f}$ is A-linear, and the given condition implies that it is a homomorphism of graded modules. □

Let B be another graded ring of type Δ and $\rho : A \to B$ a homomorphism of graded rings; then B is a graded A-module of type Δ via the map ρ. If E is a graded A-module of type Δ and $B \otimes_A E$ is given the graded A-module structure of type Δ defined above, the canonical B-module structure is compatible with the graduation of

$$\rho_!(E) = B \otimes_A E.$$

The graded B-module thus obtained is said to be obtained by extending the ring of scalars to

B by means of f and when we speak of $\rho_!(E)$ as a graded B-module, we always mean this structure, unless otherwise mentioned.

Now we define graduations on the Hom sets. For simplicity we suppose that Δ is a group. Let A be a graded ring of type Δ and M, N two graded A-modules of type Δ. Let H_λ denote the additive group of graded homomorphisms of degree λ of M into N; in the additive group $\mathrm{Hom}_A(M,N)$ of all homomorphisms of M into N (with the un-graded A-module structures) the sum (for $\lambda \in \Delta$) of the H_λ is direct. For, if there is a relation $\sum_\lambda \phi_\lambda = 0$ with $\phi_\lambda \in H_\lambda$ for all λ, it follows that $\sum_\lambda \phi_\lambda(x_\mu) = 0$ for all μ and all $x_\mu \in M_\mu$. As the elements of Δ are cancellable, $\phi_\lambda(x_\mu)$ is the homogeneous component of $\sum_\lambda \phi_\lambda(x_\mu)$ of degree $\lambda+\mu$; hence $\phi_\lambda(x_\mu) = 0$ for every ordered pair (μ,λ) and every $x_\mu \in M_\mu$, which implies $\phi_\lambda = 0$ for all $\lambda \in \Delta$. We shall denote (in this paragraph) by $\mathrm{HomHomgr}_A(M,N)$ the additive subgroup of $\mathrm{Hom}_A(M,N)$ the sum of the H_λ and we shall call it the additive group of graded A-module homomorphisms of M into N. For the canonical A-module structure on $\mathrm{Hom}_A(M,N)$, $\mathrm{Homgr}_A(M,N)$ is a submodule and the graduation (H_λ) is compatible with the A-module structure: for if $a_\nu \in A_\nu$, $x_\mu \in N_\nu$ and $\phi_\lambda \in H_\lambda$, then by definition $(a_\nu\phi_\lambda)(x_\mu) = a_\nu\phi_\lambda(x_\mu) \in N_{\lambda+\mu+\nu}$ and hence $a_\nu\phi_\lambda \in H_{\lambda+\nu}$.

Let M' and N' be two graded A-modules of type Δ. and $\phi : M' \to M$, $\psi : N \to N'$ graded homomorphisms of respective degrees α and β. Then it is immediate that $\mathrm{Hom}(\phi,\psi) : \eta \mapsto \psi\circ\eta\circ\phi$ maps $\mathrm{Homgr}_A(M,N)$ into $\mathrm{Homgr}_A(M',N')$ and that its restriction to $\mathrm{Homgr}_A(M,N)$ is a graded homomorphism into $\mathrm{Homgr}_A(M',N')$ of degree $\alpha+\beta$. In particular, $\mathrm{Homgr}_A(M,M)$ is a graded subring of $\mathrm{End}_A(M)$, which is denoted by $\mathrm{Homgr}_A(M)$.

If M and N are graded A-modules, the set $\mathrm{Homgr}_A(M,N)$ is in general distinct from $\mathrm{Hom}_A(M,N)$. However there is a special case where these tow sets equal.

Proposition 11.1.27. *Let A be a graded ring of type Δ and M a finitely generated graded A-module of type Δ. Then for any graded A-module N of type Δ, we have* $\mathrm{Homgr}_A(M,N) = \mathrm{Hom}_A(M,N)$.

Proof. Assume that M is generated by homogeneous elements $x_1\ldots,x_n$; let d_i be the degree of x_i. Let $\phi \in \mathrm{Hom}_A(M,N)$ and for all $\lambda \in \Delta$ let $z_{i,\lambda}$ denote the homogeneous component of $\phi(x_i)$ of degree $\lambda + d_i$. We show that there exists a homomorphism $\phi_\lambda : M \to N$ such that $\phi_\lambda(x_i) = z_{i,\lambda}$. for all i. For this, it suffices to prove that if $\sum_i a_i x_i = 0$ with $a_i \in A$ for $1 \le i \le n$, then $\sum_i a_i z_{i,\lambda} = 0$ for all $\lambda \in \Delta$, for then the formula $\sum_i a_i x_i \mapsto \sum_i a_i z_{i,\lambda}$ defines a map and satisfies the condition. To this end, it can be assumed that each a_i is homogeneous of degree δ_i such that $d_i + \delta_i = \mu$ for all i; then $\sum_i a_i\phi(x_i) = 0$; taking the homogeneous component of degree $\lambda + \mu$ on the left-hand sider, we obtain $\sum_i a_i z_{i,\lambda} = 0$, whence the existence of the homomorphism ϕ_λ; clearly ϕ_λ is graded of degree λ. Finally, $\phi_\lambda = 0$ except for a finite number of values of λ, and $\phi = \sum_\lambda \phi_\lambda$. by definition, which proves our assertion. □

In particular, $\mathrm{Homgr}_A(A,M) = \mathrm{Hom}_A(A,M)$ for every graded A-module M; moreover $\mathrm{Hom}_A(A,M)$ has a graded A-module structure, and it is immediate that with this structure the canonical mapping of M into $\mathrm{Hom}_A(A,M)$ is a graded A-module isomorphism.

Similarly, $\mathrm{Homgr}_A(M,A)$ has a graded A-module structure; it is called the **graded dual** of the graded A-module M and is denoted by $M^{*\mathrm{gr}}$, or simply M^* when no confusion results. If $\phi : M \to N$ is a graded homomorphism of degree δ, it follows from the above that the restriction to $N^{*\mathrm{gr}}$ of ϕ^* is a graded homomorphism of the graded dual $N^{*\mathrm{gr}}$ into the graded dual $M^{*\mathrm{gr}}$, of degree δ, called the graded dual of ϕ.

Let M, N, P, Q be graded A-modules of type Δ. Then there are canonical graded homomorphisms of degree 0:

$$\mathrm{Homgr}_A(M, \mathrm{Homgr}_A(N, P)) \to \mathrm{Homgr}_A(M \otimes_A N, P)$$

$$\mathrm{Homgr}_A(M, N) \otimes_A P \to \mathrm{Homgr}_A(M, N \otimes_A P)$$

$$\mathrm{Homgr}_A(M, P) \otimes \mathrm{Homgr}_A(N, Q) \to \mathrm{Homgr}_A(M \otimes_A N, P \otimes_A Q)$$

(the tensor products being given the graduations defined above) obtained by restricting the canonical homomorphisms for Hom sets; for, if $\phi : M \to \mathrm{Homgr}_A(N, P)$ is graded of degree δ, then, for all $x \in M_\lambda$, $\phi(x)$ is a graded homomorphism $N \to P$ of degree $\delta + \lambda$ and hence, for $y \in N_\mu$, $\phi(x)(y) \in P_{\delta+\lambda+\mu}$; if $\psi : M \otimes_A N \to P$ corresponds canonically to ϕ, it is then seen that ψ is a graded homomorphisms of degree δ, whence our assertion concerning the first map; moreover it is seen that this homomorphism is bijective. The argument is similar for the other maps.

11.1.3 Graduation by an ordered group

An order structure (denoted by $\leq$) on a commutative group Δ written additively is said to be compatible with the group structure if, for all $\lambda, \mu, \rho \in \Delta$, the relation $\lambda \leq \mu$ implies $\lambda + \rho \leq \mu + \rho$. The group Δ with this order structure is then called an ordered group.

Let Δ be an ordered commutative group, A a graded ring of type Δ and (A_λ) its graduation. We say A is a **graded ring with positive degrees** if $A_\lambda = \{0\}$ for $\lambda < 0$. In this case, it follows from definition that $A_+ = \bigoplus_{\lambda>0} A_\lambda$ is a graded ideal of A.

Proposition 11.1.28. *Let Δ be an ordered group, A a graded ring of type Δ with positive degrees, (A_λ) its gradualion, M a graded A-module of type Δ and (M_λ) its graduation. Suppose that there exists λ_0 such that $M_{\lambda_0} \neq \{0\}$ and $M_\lambda = \{0\}$ for $\lambda < \lambda_0$. Then $A_+M \neq M$.*

Proof. Let x be a non-zero element of M_{λ_0}; suppose that $x \in A_+M$. Then $x = \sum_i a_i x_i$ where the a_i are nonzero homogeneous elements of A_+ and the x_i nonzero homogeneous elements of M with $\deg(x) = \deg(a_i) + \deg(x_i)$ for all i. But, as $\deg(a_i) > 0$, $\lambda_0 = \deg(a_i) + \deg(x_i) > \deg(x_i)$, which contradicts the hypothesis. □

Corollary 11.1.29. *Let Δ be an ordered group, A a graded ring of type Δ with positive degrees. If M is a finitely generated graded A-module such that $A_+M = M$, then $M = \{0\}$.*

Proof. Suppose $M \neq \{0\}$. Let λ_0 be a minimal element of the set of degrees of a finite generating system of M consisting of nonzero homogeneous elements; then the hypotheses of Proposition 11.1.28 would be fulfilled, which implies a contradiction. □

Corollary 11.1.30. *Let Δ be an ordered group, A a graded ring of type Δ with positive degrees. If M is a finitely generated graded A-module and N is a graded submodule of M such that $N + A_+M = M$, then $N = M$.*

Proof. The quotient module M/N is a finitely generated graded A-module and the hypothesis implies that $A_+(M/N) = M/N$, henee $M/N = 0$. □

Corollary 11.1.31. *Let Δ be an ordered group, A a graded ring of type Δ with positive degrees. Let $\phi : M \to N$ be a graded homomorphism of graded A-modules, where N is assumed to be finitely generated. If the homomorphism*

$$\phi \otimes \mathrm{id} : M \otimes_A (A/A_+) \to N \otimes_A (A/A_+)$$

is surjective, then ϕ is surjective.

Proof. Note that $\phi(M)$ is a graded submodule of N and we have

$$(M/\phi(M)) \otimes_A (A/A_+) \cong (N \otimes_A (A/A_+))/\mathrm{im}(\phi \otimes \mathrm{id})$$

as (A/A_+)-modules. The hypothesis therefore implies $(N/\phi(M)) \otimes_A (A/A_+) = \{0\}$ and henee $N = \phi(M)$ by Corollary 11.1.29. □

Remark 11.1.4. It follows from the proof of Corollary 11.1.29 that Corollaries 11.1.29 and 11.1.30 (resp. Corollary 11.1.31) are still valid when, instead of assuming that M (resp. N) is finitely generated, the following hypothesis is made: there exists a subset Δ^+ of Δ satisfying the following conditions:

(a) $M_\lambda = \{0\}$ for all $\lambda \notin \Delta^+$.

(b) every non-empty subset of Δ^+ has a least element.

This will be the case if $\Delta = \mathbb{Z}$ and M (resp. N) is a graded module with positive degrees.

Proposition 11.1.32. *Suppose that $\Delta = \mathbb{Z}$. With the hypothesis of Proposition 11.1.28, consider the graded A_0-module $N = M/A_+M$ and suppose the following conditions hold:*

(a) each of the N_λ considered as an A_0-module admits a basis $(y_{i\lambda})_{i\in I_\lambda}$.

(b) the canonical homomorphism $A_+ \otimes_A M \to M$ is injective.

Then M is a graded free A-module and, to be precise, if $x_{i\lambda}$ is an element of M_λ whose image in N_λ is $y_{i\lambda}$, the family $(x_{i\lambda})_{(i,\lambda)\in I}$ (where I is the disjoint union of the I_λ) is a basis of M.

Proof. We know that there is a graded free A-module L (of graduation (L_λ)) and a surjective homomorphism $p : L \to M$ of degree 0 such that $p(e_{i\lambda}) = x_{i\lambda}$ for all $(i, \lambda) \in I$, where $(e_{i\lambda})_{(i,\lambda)\in I}$ is a basis of L consisting of homogeneous elements $e_{i\lambda} \in L_\lambda$. It follows from the above Remark that p is surjective. Consider the graded A-module $R = \ker p$ and note that $R_\lambda = \{0\}$ for $\lambda < \lambda_0$ by definition; we need to prove that $R = \{0\}$ and by Proposition 11.1.28 it suffices to show that $A_+R = R$. Consider the following commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & A_+ \otimes R \arrow[r] \arrow[d, "\phi"] & A_+ \otimes L \arrow[r, "1\otimes p"] \arrow[d, "\psi"] & A_+ \otimes M \arrow[r] \arrow[d, "\eta"] & 0 \\
0 \arrow[r] & R \arrow[r] & L \arrow[r, "p"] & M \arrow[r] & 0
\end{tikzcd}$$

where the vertical maps are induced from the canonical injection $A_+ \to A$. We need to show that ϕ is surjective. Note that, as L is free (hence flat), ψ is injective. Also, η is injective by hypothesis. Then by the snake lemma, we have an exact sequence

$$R/A_+R \longrightarrow L/A_+L \xrightarrow{\bar{p}} M/A_+M \longrightarrow 0$$

By hypothesis we see $\bar{p}$ is a bijection, hence the claim follows. □

11.1.4 Graded rings of type $\mathbb{Z}$

In this paragraph, all the graduations considered are assumed to be of type $\mathbb{Z}$. If A (resp. M) is a graded ring (resp. graded module), A_i (resp. M_i) will denote the set of homogeneous elements of degree i in A (resp. M). Recall that if $A_i = \{0\}$ (resp. $M_i = \{0\}$) for $i < 0$, A (resp. M) will, to abbreviate, be called a graded ring (resp. module) with positive degrees.

Proposition 11.1.33. *Let $A = \bigoplus_{i\geq 0} A_i$ be a graded ring with positive degrees and (x_λ) a family of homogeneous elements of A_+. The following conditions are equivalent:*

(i) The ideal of A generated by the family (x_λ) is equal to A_+.

(ii) The family (x_λ) is a system of generators of the A_0-algebra A.

(iii) For all $i \geq 0$, the A_0-module A_i is generated by the elements of the form $\prod_\lambda x_\lambda^{n_\lambda}$ which are of degree i in A.

Proof. Clearly conditions (ii) and (iii) are equivalent. If they hold, every element of A_+ is of the form $f(x_\lambda)$ where f is a polynomial of $A_0[X_\lambda]$ with no constant term; then $A_+ = \sum_\lambda Ax_\lambda$, which proves that (iii) implies (i). Conversely, suppose that condition (i) holds. Let $A' = A_0[x_\lambda]$ be the sub-A_0-algebra of A generated by the family (x_λ) and let us show that $A' = A$. For this, it is sufficicnt to show that $A_i \subseteq B$ for all $i \geq 0$. We proceed by induction on i, the property being obvious for $i = 0$. Then let $y \in A_i$ with $i \geq 1$. Sincey $y \in A_+$, which is the ideal generated by (x_λ), there exists a family (a_λ) of elements of A of finite support such that $y = \sum a_\lambda x_\lambda$ and we may assume that each of the a_λ is homogeneous of degree $i - \deg(x_\lambda)$ (by replacing it if need be by its homogeneous component of that degree); as $\deg(x_\lambda) > 0$, the induction hypothesis shows that $a_\lambda \in A'$ for all α, whence $y \in A'$ and $A_i \subseteq A'$, which proves that (i) implies (ii). □

Proof. Part (a) follows from Proposition 11.1.33. As for (b), the condition in (b) is sufficient by Hilbert's basis theorem. If A is Noetherian, $A_0 = A/A_+$ is Noetherian and A_+ is finitely generated as an ideal. Thus A is an A_0-algebra of finite type by (a). □

Corollary 11.1.34. *Let $A = \bigoplus_{i\geq 0} A_i$ be a graded ring with positive degrees.*

(a) The ideal A_+ is finitely generated if and only if A is an A_0-algebra of finite type.

(b) The ring A is Noetherian if and only if A_0 is Noetherian and A is an A_0-algebra of finite type.

(c) Suppose that the conditions in (a) hold and let $M = \bigoplus_{i\in\mathbb{Z}} M_i$ be a finitely generated graded A-module. Then, for all $i \in \mathbb{Z}$, M_i is a finitely generated A_0-module and there exists i_0 such that $M_i = \{0\}$ for $i < i_0$.

Proof. Part (a) follows from Proposition 11.1.33. As for (b), the condition in (b) is sufficient by Hilbert's basis theorem. If A is Noetherian, $A_0 = A/A_+$ is Noetherian and A_+ is finitely generated as an ideal. Thus A is an A_0-algebra of finite type by (a).

We prove (c). We may suppose that A is generated (as an A_0-algebra) by homogeneous elements $a_1, \ldots, a_r$ of degree $i \geq 1$ and M is generated (as an A-module) by homogeneous

elements $x_1, \dots, x_n$; let $h_i = \deg(a_i)$ and $k_j = \deg(x_j)$. Clearly M_n consists of the linear combinations with coefficients in A_0 of the elements $a_1^{\alpha_1} \cdots a_r^{\alpha_r} x_j$ such that the α_i are positive integers satisfying the relation $k_j + \sum_{i=1}^r h_i \alpha_i = n$; for each n there is only a finite number of families $(\alpha_i)_{i=1}^r$ satisfying these conditions, since $h_i \geq 0$ for all i; we conclude that M_n is a finitely generated A_0-module and moreover clearly $M_n = \{0\}$ when $n < \inf(k_i)$. □

Let $A = \bigoplus_{i \in \mathbb{Z}} A_i$ be a graded ring and $M = \bigoplus_{i \in \mathbb{Z}} M_i$ a graded A-module; for each ordered pair (d, r) with $d \geq 1$ and $0 \leq r \leq d-1$, set

$$A^{(d)} = \bigoplus_{i \in \mathbb{Z}} A_{id}, \quad M^{(d,r)} = \bigoplus_{i \in \mathbb{Z}} M_{id+r}.$$

Clearly $A^{(d)}$ is a graded subring of A and $M^{(d,r)}$ a graded $A^{(d)}$-module; moreover, if N is a graded submodule of M, $N^{(d,r)}$ is a graded sub-$A^{(d)}$-module of $M^{(d,r)}$. We shall write $M^{(d)}$ instead of $M^{(d,0)}$; for each $d \geq 1$, M is the direct sum of the $A^{(d)}$-modules $M^{(d,r)}$ for $0 \leq r \leq d-1$.

Proposition 11.1.35. *Let A be a graded ring with positive degrees and $M = \bigoplus_{i \in \mathbb{Z}} M_i$ be a graded A-module. Suppose that A is an A_0-algebra of finite type and M a finitely generated A-module. Then*

(a) For every ordered pair (d, r) of integers such that $d \geq 1$ and $0 \leq r \leq d-1$, $M^{(d,r)}$ is a finitely generated $A^{(d)}$-module.

(b) $A_+^{(d)}$ is a finitely generated $A^{(d)}$-module and therefore $A^{(d)}$ is an A_0-algebra of finite type.

Proof. Let us show that A is a finitely generated $A^{(d)}$-module. Let $a_1, \dots, a_s$ be a system of generators of the A_0-algebra A consisting of homogeneous elements. The elements of A (finite in number) of the form $a_1^{\alpha_1} \cdots a_s^{\alpha_s}$ such that $0 \leq a_i \leq d$ for $1 \leq i \leq s$ constitute a system of generators of the $A^{(d)}$-module A; for every system of integers $n_i \geq 0$, $1 \leq i \leq s$, there are positive integers q_i and r_i such that $n_i = q_i d + r_i$, where $0 \leq r_i < d$ for $1 \leq i \leq s$; then

$$a_1^{n_1} \cdots a_s^{n_s} = (a_1^{q_1} \cdots a_s^{q_s})(a_1^{r_1} \cdots a_s^{r_s}).$$

which proves our assertion. Then, if M is a finitely generated A-module, it is also a finitely generated $A^{(d)}$-module; as M is the direct sum of the $M^{(d,r)}$ for $0 \leq r \leq d-1$, each of the $M^{(d,r)}$ is a finitely generated $A^{(d)}$-module, which proves (a).

Now by Corollary 11.1.34, A_+ is a finitely generated A-module, so (a) implies $A_+^{(d)}$ is a finitely-generated A_0-module, which again by Corollary 11.1.34 implies $A^{(d)}$ is a finite A_0-algebra. □

Proposition 11.1.36. *Let $A = \bigoplus_{i \geq 0} A_i$ be a graded ring with positive degrees which is a finitely generated A_0-algebra and $M = \bigoplus_{i \in \mathbb{Z}} M_i$ a graded A-module. Let $(x_\lambda)_{\lambda \in I}$ be a system of homogeneous generators of M such that $\sup_\lambda \deg(x_\lambda) < +\infty$. Then there exists $n_0 > 0$ and $d > 0$ such that, for any $n \geq n_0$ we have $M_{n+d} = A_d M_n$.*

Proof. Let A be generated as an A_0-algebra by homogeneous elements $a_1, \dots, a_s$, and set $d_i = \deg(a_i)$. Let d be a common multiple of all the d_i and set $b_i = a_i^{d/d_i}$ for $1 \leq i \leq s$, so that $\deg(b_i) = d$ for all i. Consider the set Z of elements of the form $a_1^{\alpha_1} \cdots a_s^{\alpha_s} x_\lambda$ with $0 \leq \alpha_i \leq d/d_i$ for $1 \leq i \leq s$ and $\lambda \in I$. Then by the hypothesis on (x_λ), we can choose $n_0 > 0$ be larger than the degree of every element of Z. If $n \geq n_0$ then any element of M_{n+d} can be written as an

A_0-linear combination of elements $a_1^{n_1} \cdots a_s^{n_s} x_j$ as above. If $n_i = (d/d_i)\beta_i + \gamma_i$ with $\gamma_i < d/d_i$, then we can write

$$a_1^{n_1} \cdots a_s^{n_s} x_j = b_1^{\beta_1} \cdots b_s^{\beta_s} (a_1^{\gamma_1} \cdots a_s^{\gamma_s} x_j) = b_1^{\beta_1} \cdots b_s^{\beta_s} z$$

where every b_i is homogenous of degree d and $z \in Z$ is homogeneous of some degree t. Note that $n + d > n_0 \geq t$, so the last expression makes sense. Now it is clear that $b_1^{\beta_1} \cdots b_s^{\beta_s} z$ belongs to $A_d M_n$, so $M_{n+d} = A_d M_n$. □

Corollary 11.1.37. *Let A be a graded ring such that $A = A_0[A_1]$, M a graded A-module and $(x_\lambda)_{\lambda \in I}$ a system of homogeneous generators of M such that $\deg(x_\lambda) \leq n_0$ for all $\lambda \in I$. Then for all $n \geq n_0$ and all $d > 0$, $M_{n+d} = A_d M_n$.*

Proof. In this case the integer d in Proposition 11.1.36 can be chosen to be 1, and the set Z has elements of degree smaller than n_0. Thus we have $M_{n+d} = A_1 M_n$ for $n \geq n_0$, and by induction $M_{n+d} = A_d M_n$ for $n \geq n_0$ and $d > 0$. □

Corollary 11.1.38. *Let A be a graded ring such that $A = A_0[A_1]$ and let $S = \bigoplus_{i \geq 0} S_i$ be a graded A-algebra with positive degrees which is a finitely generated A-module. Then there exists an integer $n_0 > 0$ such that:*

(a) For $n \geq n_0$ and $d > 0$, $S_{n+d} = S_d S_n$.

(b) For $d \geq n_0$, $S^{(d)} = S_0[S_d]$.

Proof. By Corollary 11.1.37 there exists an integer $n_0 \geq 0$ such that, for $n \geq n_0$ and $d > 0$, $S_{n+d} = A_d S_n$, whence a fortiori $S_{n+d} = S_d S_n$, which establishes (a). Then, for $d \geq n_0$ and $i > 0$, $S_{id} = (S_d)^i$ as follows by induction on i applying (a); this establishes (b). □

Corollary 11.1.39. *Let $A = \bigoplus_{i \geq 0} A_i$ be a graded ring with positive degrees which is a finitely generated A_0-algebra. There exists an integer $d > 0$ such that $A^{(md)} = A_0[A_{md}]$ for all $m \geq 1$.*

Proof. In Proposition 11.1.36 we can assume that $d \geq n_0$ (since the proof works with d any common multiple of the d_i). And therefore with $A = M$ we have $A_{d+d} = (A_d)^2$ and inductively $A_{id} = (A_d)^i$ for all $i > 0$. This shows the claim. □

Proposition 11.1.40. *Let Δ be an ordered group and A a graded ring of type Δ. If the product in A of two homogeneous nonzero elements is nonzero, then the ring A is integral.*

Proof. Let $x = \sum_\lambda x_\lambda$ and $y = \sum_\lambda y_\lambda$ be two non-zero elements of A, with x_λ, y_λ being homogeneous of degree λ for all $\lambda \in \Delta$. Let α (resp. β) be the greatest of the elements $\lambda \in \Delta$ such that $x_\lambda \neq 0$ (resp. $y_\lambda \neq 0$); it is immediate that if $\lambda \neq \alpha$ or $\mu \neq \beta$, either $x_\lambda y_\mu = 0$ or $\deg(x_\lambda y_\mu) < \lambda + \alpha$; the homogeneous component of xy of degree $\alpha + \beta$ is therefore $x_\lambda y_\beta$, which is non-zero by hypothesis; whence $xy \neq 0$. □

Proposition 11.1.41. *Let $\mathfrak{p} = \bigoplus_{i \geq 0} \mathfrak{p}_i$ be a graded ideal of A; for $\mathfrak{p}$ to be prime, it is necessary and sufficient that for homogeneous elements $x, y \in A$, $xy \notin \mathfrak{p}$ if and only if $x \notin \mathfrak{p}$ and $y \notin \mathfrak{p}$.*

Proof. The condition is obviously necessary. Conversely, if it is fulfilled, then in the graded ring $A/\mathfrak{p} = \bigoplus_{i \geq 0} A_i/\mathfrak{p}_i$ the product of two homogeneous nonzero elements is nonzero and hence $A/\mathfrak{p}$ is an integral domain. □

Let $\mathfrak{a}$ be an arbitrary ideal of A. We can associate to it a homogeneous ideal $\mathfrak{a}^h = \bigoplus_{i\geq 0}(\mathfrak{a} \cap A_i)$. It follows from the definition that $\mathfrak{a}^h \subseteq \mathfrak{a}$ and $\mathfrak{a}$ is homogeneous if and only if $\mathfrak{a} = \mathfrak{a}^h$.

Proposition 11.1.42. *Let A be a graded ring with positive degrees and $\mathfrak{p} \subseteq A$ be a prime ideal. Let $\mathfrak{p}^h$ be the homogeneous ideal generated by the homogeneous elements of $\mathfrak{p}$. Then $\mathfrak{p}^h$ is a prime ideal of A.*

Proof. For any homogeneous element $f, g \in A$ such that $fg \in \mathfrak{p}^h \subseteq \mathfrak{p}$, we have $f \in \mathfrak{p}$ or $g \in \mathfrak{p}$. Then by the definition of $\mathfrak{p}^h$, this implies $f \in \mathfrak{p}^h$ or $g \in \mathfrak{p}^h$. Thus $\mathfrak{p}^h$ is prime by Proposition 11.1.41. □

Corollary 11.1.43. *Let $A = \bigoplus_{i\geq 0} A_i$ be a graded ring with positive degrees.*

(a) Any minimal prime of A is a homogeneous ideal.

(b) Given a homogeneous ideal $\mathfrak{a} \subseteq A$ any minimal prime over $\mathfrak{a}$ is homogeneous.

Proof. The first claim is a direct application of Proposition 11.1.42, since the ideal $\mathfrak{p}^h$ is contained in $\mathfrak{p}$. The second follows by applying the result on $A/\mathfrak{a}$. □

Let A be a graded ring with positive degrees. Two graded ideals $\mathfrak{a} = \bigoplus_{i\geq 0} \mathfrak{a}_i$ and $\mathfrak{b} = \bigoplus_{i\geq 0} \mathfrak{b}_i$ of A are said to be **equivalent** if there exists an integer n_0 such that $\mathfrak{a}_n = \mathfrak{b}_n$ for $n \geq n_0$ (clearly it is an equivalence relation). A graded ideal is called **essential** if it is not equivalent to A_+. As we will see, this notation plays an important role when we study graded prime ideals.

Proposition 11.1.44. *Let A be a graded ring with positive degrees, $\mathfrak{a}$ a graded ideal, and $\mathfrak{p}$ a graded prime ideal of A with $\mathfrak{p} \not\supseteq A_+$. Then $\mathfrak{a} \subseteq \mathfrak{p}$ if and only if there exists an integer $n_0 \geq 0$ such that $\mathfrak{a}_n \subseteq \mathfrak{p}_n$ for all $n \geq n_0$.*

Proof. One implication is clear. Conversely, assume that $a_n \subseteq \mathfrak{p}_n$ for $n \geq n_0$. We now show that $a_{n_0-1} \subseteq \mathfrak{p}_{n_0-1}$. Since $\mathfrak{p} \not\supseteq A_+$, there exist $e > 0$ and $a \in A_e$ with $a \notin \mathfrak{p}$. If $b \in \mathfrak{a}_{n_0-1}$ then $ab \in \mathfrak{a}_{n_0-1+e} \subseteq \mathfrak{p}_{n_0-1+e}$, so $b \in \mathfrak{p}$ by primeness. This proves the claim. □

Corollary 11.1.45. *Let A be a graded ring with positive degrees and $\mathfrak{p}$, $\mathfrak{q}$ be graded prime ideals and $\mathfrak{p}$ with $\mathfrak{p} \not\supseteq A_+$ and $\mathfrak{q} \not\supseteq A_+$. Then $\mathfrak{p} = \mathfrak{q}$ if and only if they are equivalent.*

Proposition 11.1.46. *Let $\mathfrak{a}$ be a graded ideal of A and $n_0 > 0$ an integer. For there to exist a graded prime ideal $\mathfrak{p}$ such that $\mathfrak{p}_n = \mathfrak{a}_n$ for $n \geq n_0$, it is necessary and sufficient that, for any homogeneous elements x, y of degrees $\geq n_0$, the relation $xy \in \mathfrak{a}$ implies $x \in \mathfrak{a}$ or $y \in \mathfrak{a}$. If there exists $n \geq n_0$ such that $\mathfrak{a}_n \neq A_n$, then the prime ideal satisfying the above condition is unique.*

Proof. The condition of the statement is obviously necessary. If $\mathfrak{a}_n = A_n$ for all $n \geq n_0$, clearly every prime ideal containing A_+ is a solution to the problem; there may therefore be several prime ideals which solve the problem; however, any two of these ideals are obviously equivalent.

Now suppose that there exists a homogeneous element $a \in A_d$ with $d \geq n_0$ not belonging to $\mathfrak{a}_d$. Now we define

$$\mathfrak{p} = \{x \in A : ax \in \mathfrak{a}\}.$$

Clearly $\mathfrak{p}$ is an ideal of A; as the homogeneous components of ax are the products by a of those of x and a is a graded ideal, $\mathfrak{p}$ is a graded ideal; moreover, $1 \notin \mathfrak{p}$ and hence $\mathfrak{p} \neq A$. To prove that $\mathfrak{p}$ is prime, let $x \in A_m$ and $y \in A_n$ satisfy $x \notin \mathfrak{p}$ and $y \notin \mathfrak{p}$. Then $ax \notin \mathfrak{a}_{m+d}$ and $ay \notin \mathfrak{a}_{n+d}$,

hence $a^2xy \notin \mathfrak{a}_{m+n+2d}$ by hypothesis. Since $\mathfrak{a}$ is an ideal, we then get $axy \notin \mathfrak{a}_{m+n+d}$, so $xy \in \mathfrak{p}$. Now if $n \geq n_0$ and $a \in A$, the conditions $x \in \mathfrak{a}_n$ and $ax \in \mathfrak{a}_{n+d}$ are equivalent by hypothesis and hence $\mathfrak{p} \cap A_n = \mathfrak{a}_n$, which completes the proof of the existence of the graded prime ideal $\mathfrak{p}$ which solves the problem. The uniqueness part now follows from Corollary 11.1.45. □

Proposition 11.1.47. *Let $A = \bigoplus_{i\geq 0} A_i$ be a graded ring with positive degrees and $d > 0$ an integer.*

(a) For every essential graded prime ideal $\mathfrak{p}$ of A, $\mathfrak{p} \cap A^{(d)}$ is an essential graded prime ideal of $A^{(d)}$.

(b) Conversely, for every essential graded prime ideal $\mathfrak{p}'$ of $A^{(d)}$, there exists a unique (necessarily essential) graded prime ideal $\mathfrak{p}$ of A such that $\mathfrak{p} \cap A^{(d)} = \mathfrak{p}'$.

Proof. If $a \in A_i$ does not belong to $\mathfrak{p}_i$, then a^d does not belong to $\mathfrak{p}_{id}$, and hence $\mathfrak{p} \cap A^{(d)}$ is essential. This proves (a). Now let $\mathfrak{p}'$ be an essential graded prime ideal of $A^{(d)}$. If $\mathfrak{p}$ is a graded prime ideal of A such that $\mathfrak{p} \cap A^{(d)} = \mathfrak{p}'$, then for all $n \geq 0$, the set $\mathfrak{p} \cap A_n$ must be equal to the set $\mathfrak{a}_n$ of $x \in A_n$ such that $x^d \in \mathfrak{p}'$. Let us show that $\mathfrak{a} = \bigoplus_{n\geq 0} \mathfrak{a}_n$ is a graded prime ideal, which will proves (b). As $\mathfrak{p}'$ is prime, $\mathfrak{a}_n = \mathfrak{p}_n$ when n is a multiple of d. Now if $x \in \mathfrak{a}_n$, $y \in \mathfrak{a}_n$, then $(x-y)^{2d}$ is the sum of terms each of which is a product of x^d or y^d by a homogeneous element of degree nd and hence $(x-y)^{2d} \in \mathfrak{p}'$ and, since $\mathfrak{p}'$ is prime, $(x-y)^d \in \mathfrak{p}'$ and therefore $\mathfrak{a}_n$ is a subgroup of A. As $\mathfrak{p}'$ is an ideal of $A^{(d)}$, $\mathfrak{a}$ is a graded ideal of A; finally, the relation $(xy)^d \in \mathfrak{p}'$ implies $x^d \in \mathfrak{p}'$ or $y^d \in \mathfrak{p}'$, which completes the proof. □

Let A be a graded ring with positive degrees and $\mathfrak{p}$ an essential graded prime ideal of A. The set S of homogeneous elements of A not belonging to $\mathfrak{p}$ is multiplicative and the ring of fractions $S^{-1}A$ is therefore graded canonically (note that there will in general be homogeneous nonzero elements of negative degree in this graduation). We shall denote by $A_{\mathfrak{p}}$ the subring of $S^{-1}A$ consisting of the homogeneous elements of degree 0, in other words the set of fractions x/s, where x and s are homogeneous of the same degree in A and $s \notin \mathfrak{p}$. Similarly, for every graded A-module M, $S^{-1}M$ is graded canonically (loc. cit.) and we shall denote by $M_{\mathfrak{p}}$ the subgroup of homogeneous elements of degree 0, which is obviously an $A_{\mathfrak{p}}$-module.

Proposition 11.1.48. *Let $\mathfrak{p}$ be a graded prime ideal of A, $d > 0$ an integer, and $\mathfrak{p}'$ be the graded prime ideal $\mathfrak{p} \cap A^{(d)}$ of $A^{(d)}$. For every graded A-module M, the homomorphism $(M^{(d)})_{\mathfrak{p}'} \to M_{\mathfrak{p}}$ induced from the canonical injection $M^{(d)} \to M$ is bijective.*

Proof. If S is the set of homogeneous elements of A not belonging to $\mathfrak{p}$ and $S^{(d)} = S \cap A^{(d)}$, the canonical homomorphism $\phi : (S^{(d)})^{-1}M^{(d)} \to S^{-1}M$ is a homogeneous homomorphism of degree 0 and it is injective, for, if $x \in M_{nd}$ satisfies $sx = 0$ for $s \in A_m$, $s \notin \mathfrak{p}$, then also $s^d x = 0$ and $s^d \in A_{md}$, $s^d \notin \mathfrak{p}'$. It remains to show that the image under ϕ of $(M^{(d)})_{\mathfrak{p}'}$ is the whole of $M_{\mathfrak{p}}$; but if $x \in M_n$, $s \in A_n$ and $s \notin \mathfrak{p}$, then also $x/s = (xs^{d-1})/s^d$ where $xs^{d-1} \in A_{nd}$, $s^d \in A_{md}$ and $s^d \notin \mathfrak{p}'$, whence our assertion. □

Proposition 11.1.49. *Suppose A is a graded ring with positive degrees, $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ homogeneous prime ideals and $\mathfrak{a}$ a homogeneous ideal. Assume that $\mathfrak{a} \cap A_+ \not\subseteq \mathfrak{p}_i$ for all i, then there exists a homogeneous element $x \in \mathfrak{a} \cap A_+$ of positive degree such that $x \notin \mathfrak{p}_i$ for $1 \leq i \leq r$.*

Proof. We may assume that $\mathfrak{a} \subseteq A_+$ and there are no inclusions among the $\mathfrak{p}_i$. The result is true for $r = 1$. Suppose the result holds for $r-1$. Pick $x \in \mathfrak{a}$ homogeneous of positive degree such that $x \notin \mathfrak{p}_i$ for all $i = 1, \ldots, r-1$. If $x \notin \mathfrak{p}_r$ we are done, so assume that $x \in \mathfrak{p}_r$. Since

$\mathfrak{a}\mathfrak{p}_1 \cdots \mathfrak{p}_{r-1}$ is a homogeneous ideal that is not contained in $\mathfrak{p}_r$, there is a homogeneous element $y \in \mathfrak{a}\mathfrak{p}_1 \cdots \mathfrak{p}_{r-1}$ of positive degree such that $y \notin \mathfrak{p}_r$. Then $x^{\deg(y)} + y^{\deg(x)}$ works. □

11.2 Filtration and topologies

11.2.1 Filtrated rings and modules

Definition 11.2.1. *An increasing (resp. decreasing) sequence $(G_n)_{n\in\mathbb{Z}}$ of subgroups of a commutative group G is called an* ***increasing (resp. decreasing) filtration*** *on G. A commutative group with a filtration is called a filtered group.*

If $(G_n)_{n\in\mathbb{Z}}$ is an increasing (resp. decreasing) filtration on a commutative group G and we write $G'_n = G_{-n}$, clearly $(G'_n)_{n\in\mathbb{Z}}$ is a decreasing (resp. increasing) filtration on G. We may therefore restrict our study to decreasing filtrations and hence forth when we speak of a filtration, we shall mean a decreasing filtration, unless otherwise stated.

Given a decreasing filtration $(G_n)_{n\in\mathbb{Z}}$ on a commutative group G, clearly $\bigcap_{n\in\mathbb{Z}} G_n$ and $\bigcup_{n\in\mathbb{Z}} G_n$ are subgroups of G; the filtration is called **separated** if $\bigcap_{n\in\mathbb{Z}} G_n$ is reduced to the identity element and **exhaustive** if $\bigcup_{n\in\mathbb{Z}} G_n = G$.

Definition 11.2.2. *Given a ring A, a filtration $(A_n)_{n\in\mathbb{Z}}$ over the additive group A is called compatible with the ring structure on A if*

(a) $A_m A_n \subseteq A_{m+n}$ *for all* $m, n \in \mathbb{Z}$.

(b) $1 \in A_0$.

The ring A with this filtration is then called a ***filtered ring****.*

Conditions (a) and (b) show that A_0 is a subring of A and the A_n's are A_0-modules. The set $B = \bigcup_{n\in\mathbb{Z}} A_n$ is a subring of A and the set $\mathfrak{n} = \bigcap_{n\in\mathbb{Z}} A_n$ is an ideal of B; for if $x \in \mathfrak{n}$ and $a \in A_p$, then for all $k \in \mathbb{Z}$ we have $x \in A_{k-p}$, whence $ax \in A_k$ by (a); therefore $ax \in \mathfrak{n}$. An important particular case is that $A_0 = A$; then $A_n = A$ for all $n \leq 0$ and all the A_n are ideals of A.

Definition 11.2.3. *Let A be a filtered ring, $(A_n)_{n\in\mathbb{Z}}$ its filtration and M an A-module. A filtration $(M_n)_{n\in\mathbb{Z}}$ on M is called compatible with its module structure over the filtered ring A if*

$$A_m M_n \subseteq M_{m+n} \quad \textit{for all } m, n \in \mathbb{Z}. \tag{2.1.1}$$

The A-module M with this filtration is called a ***filtered module****.*

If M is a filtered module with filtration $(M_n)_{n\in\mathbb{Z}}$, then the M_n are all A_0-modules; if $B = \bigcup_{n\in\mathbb{Z}} A_n$, clearly $\bigcup_{n\in\mathbb{Z}} M_n$ is a B-module and so is $\bigcap_{n\in\mathbb{Z}} M_n$ by the same argument as above for $\mathfrak{n}$. If $A_0 = A$, all the M_n's are submodules of M.

Example 11.2.4. On a ring A the sets A_n such that $A_n = 0$ for $n > 0$, $A_n = A$ for $n \leq 0$ form what is called a **trivial filtration** associated with the trivial graduation on A; on an A-module M, every filtration (M_n) consisting of sub-A-modules is then compatible with the module structure on M over the filtered ring A. Then it is possible to say that every filtered commutative group G is a filtered $\mathbb{Z}$-module, if $\mathbb{Z}$ is given the trivial filtration.

Example 11.2.5. Let A be a graded ring of type $\mathbb{Z}$; for all $i \in \mathbb{Z}$, let A^n be the subgroup of homogeneous elements of degree n in A and set $A_n = \bigoplus_{i \geq n} A^i$. Then it is immediate that (A_n) is an exhaustive and separated decreasing filtration which is compatible with the ring structure on A; this filtration is said to be associated with the graduation (A^n) and the filtered ring A is said to be associated with the given graded ring A.

Now let M be a graded module of type $\mathbb{Z}$ over the graded ring A and for all $i \in \mathbb{Z}$ let M^n be the subgroup of homogeneous elements of degree n of M. If $M_n = \bigoplus_{i \geq n} M^i$, then (M_n) is an exhaustive and separated decreasing filtration which is compatible with the module structure on M over the filtered ring A; this filtration is said to be **associated** with the graduation (M^n) and the filtered module M is said to be **associated** with the given graded module M.

Example 11.2.6. Let A be a filtered ring, $(A_n)_{n \in \mathbb{Z}}$ its filtration and M an A-module. Let us write $M_n = A_n M$; it follows that

$$A_m M_n = A_m A_n M \subseteq A_{m+n} M = M_{m+n}$$

and that $M_0 = M$; therefore (M_n) is an exhaustive filtration which is compatible with the A-module structure on M. This filtration is said to be **derived** from the given filtration (A_n) on A; note that it is not necessarily separated, even if (A_n) is separated.

Example 11.2.7 (The $\mathfrak{a}$-adic filtration). Let A be a ring and $\mathfrak{a}$ an ideal of A. Let us write $A_n = \mathfrak{a}^n$ for $n > 0$ and $A_n = A$ for $n \leq 0$. It is immediate that (A_n) is an exhaustive filtration on A, called the **$\mathfrak{a}$-adic filtration**. Let M be an A-module; the filtration (M_n) derived from the $\mathfrak{a}$-adic filtration on A is called the $\mathfrak{a}$-adic filtration on M. If B is an A-algebra, then $\mathfrak{b} = \mathfrak{a}^e$ is an ideal of B and for every B-module N and $n \in \mathbb{Z}$ we have $\mathfrak{b}^n N = \mathfrak{a}^n N$, therefore the $\mathfrak{b}$-adic filtration on N coincides with the $\mathfrak{a}$-adic filtration (if N is considered as an A-module).

Let G be a filtered group and $(G_n)_{n \in \mathbb{Z}}$ its filtration; clearly, for every subgroup H of G, $(H \cap G_n)_{n \in \mathbb{Z}}$ is a filtration said to be **induced** by that on G. Similarly, if H is a normal subgroup of G, the family $((H + G_n)/H)_{n \in \mathbb{Z}}$ is a filtration on the group G/H, called the **quotient** under H of the filtration on G.

If G and G' are filtered groups and (G_n), (G'_n) are their filtrations. Then $(G_n \times G'_n)_{n \in \mathbb{Z}}$ is a filtration on $G \times G'$ called the **product** of the filtrations on G and G', which is exhaustive (resp. separated) if (G_n) and (G'_n) are.

Now let A be a filtered ring and (A_n) its filtration; on every subring B of A, clearly the filtration induced by that on A is compatible with the ring structure on B. If $\mathfrak{a}$ is an ideal of A, the quotient filtration on $A/\mathfrak{a}$ of that on A is compatible with the structure of this ring, for

$$(A_m + \mathfrak{a})(A_n + \mathfrak{a}) \subseteq A_m A_n + \mathfrak{a} \subseteq A_{m+n} + \mathfrak{a}.$$

If A' is another filtered ring, the product filtration on $A \times A'$ is compatible with the structure of this ring.

Simialrly, let M be a filtered A-module and (M_n) its filtration; on every submodule N of M, the filtration induced by that on M is compatible with the A-module structure on N and, on the quotient module M/N, the quotient filtration of that on M is compatible with the A-module structure, as

$$A_m(N + M_n) \subseteq N + A_m M_n \subseteq N + M_{m+n}.$$

Note that if the filtration on M is derived from that on A, so is the quotient filtration on M/N because we have $(N + A_n M)/N = A_n(M/N)$. However, this is not true in general for the filtration induced on N.

Let A be a filtered ring, M a filtered A-module and (M_n) the filtration of M. For all $x \in M$ let $v(x)$ denote the least upper bound in $\overline{\mathbb{R}}$ of the set on integers $n \in \mathbb{Z}$ such that $x \in M_n$. Then the following equivalences hold:

$$\begin{cases} v(x) = +\infty & x \in \bigcap_{n\in\mathbb{Z}} M_n \\ v(x) = p & x \in M_p \setminus M_{p+1} \\ v(x) = -\infty & x \notin \bigcup_{n\in\mathbb{Z}} M_n \end{cases}$$

Thé mapping $v : M \to \overline{\mathbb{R}}$ is called the **order function** of the filtered module M. If v is known then so are the M_n, for M_n is the set of $x \in M$ such that $v(x) \geq n$; the fact that the M_n are additive subgroups of M implies the relation

$$v(x + y) \geq \min\{v(x), v(y)\} \tag{2.1.2}$$

The above definition applies in particular to the filtered A-module A. If v_A is the order function of A and v_M the order function on M, it follows from (2.1.1) that for $a \in A$, and $x \in M$,

$$v_M(ax) \geq v_A(a) + v_M(x)$$

whenever the right-hand side is defined. In particular, for $a \in A$ and $b \in A$, we have $v_A(ab) \geq v_A(a) + v_A(b)$.

11.2.2 The associated graded module

Let G be a commutative group (written additively) and (G_n) a filtration on G. Let us write

$$\mathrm{gr}_n(G) = G_n/G_{n+1}, \quad \mathrm{gr}(G) = \bigoplus_{n\in\mathbb{Z}} \mathrm{gr}_n(G).$$

The commutative group $\mathrm{gr}(G)$ is then a graded group of type $\mathbb{Z}$, called the graded group associated with the filtered group G, the homogeneous elements of degree n of $\mathrm{gr}(G)$ being those of $\mathrm{gr}_n(G)$.

Now let A be a filtered ring, (A_n) its filtration, M a filtered A-module and (M_n) its filtration. For all $p \in \mathbb{Z}$, $q \in \mathbb{Z}$, we can define a map

$$\mathrm{gr}_p(A) \times \mathrm{gr}_q(M) \to \mathrm{gr}_{p+q}(M), \quad (\bar{a}, \bar{x}) \mapsto \overline{ax}. \tag{2.2.1}$$

This is well-defined in view of the equality $ax - by = (a - b)x + b(x - y)$ and the relations $A_{p+1}M_q \subseteq M_{p+q+1}$, $A_p M_{q+1} \subseteq M_{p+q+1}$. It is immediate that the map defined is $\mathbb{Z}$-bilinear; by linearity, we derive a $\mathbb{Z}$-bilinear mapping

$$\mathrm{gr}(A) \times \mathrm{gr}(M) \to \mathrm{gr}(M).$$

If this definition is first applied to the case $M = A$, the map (2.2.1) is an internal law of com-

position on $\mathrm{gr}(A)$, which it is immediately verified is associative and has an identity element which is the canonical image in $\mathrm{gr}_0(A)$ of the unit element of A; it therefore defines on $\mathrm{gr}(A)$ a ring structure and the graduation $(\mathrm{gr}_n(A))_{n\in\mathbb{Z}}$ is by definition compatible with this structure. The graded ring $\mathrm{gr}(A)$ (of type $\mathbb{Z}$) thus defined is called the **graded ring associated with the filtered ring** A. The mapping (2.2.1) is on the other hand a $\mathrm{gr}(A)$-module external law on $\mathrm{gr}(M)$, the module axioms being trivially satisfied, and the graduation $(\mathrm{gr}_n(M))_{n\in\mathbb{Z}}$ on $\mathrm{gr}(M)$ is obviously compatible with this module structure. The graded $\mathrm{gr}(A)$-module $\mathrm{gr}(M)$ (of type $\mathbb{Z}$) thus defined is called the graded module associated with the filtered A-module M.

Example 11.2.8. Let A be a ring and t an element of A which is not a divisor of 0. Let us give A the (t)-adic filtration. Then the associated graded ring $\mathrm{gr}(A)$ is canonically isomorphic to the polynomial ring $(A/(t))[X]$. For $\mathrm{gr}_n(A) = 0$ for $n < 0$ and by definition the ring $\mathrm{gr}_0(A)$ is the ring $A/(t)$. We now note that by virtue of the hypothesis on t the relation $at^n \equiv 0 \bmod (t^{n+1})$ is equivalent to $a \equiv 0 \bmod t$; if τ is the canonical image of t in $\mathrm{gr}_1(A)$, every element of $\mathrm{gr}_n(A)$ may then be written uniquely in the form $\alpha\tau^n$, where $\alpha \in \mathrm{gr}_0(A)$; whence our assertion.

Example 11.2.9. Let K be a ring and A the ring of formal power series

$$A = K[\![X_1, \dots, X_r]\!].$$

Let $\mathfrak{m}$ be the ideal of A whose elements are the formal power series with no constant term. Let us give A the $\mathfrak{m}$-adic filtration; if $M_1, \dots, M_s$ are the distinct monomials in $X_1, \dots, X_r$ of total degree $n-1$, clearly every formal power series u of total order $\deg(u) \geq n$ may be written as $\sum_{k=1}^{s} u_k M_k$, where the u_k belong to $\mathfrak{m}$; it is seen that $\mathfrak{m}^n$ is the set of formal power series u such that $\deg(u) \geq n$, which shows that deg is the order function for the $\mathfrak{m}$-adic filtration. Then clearly, for every formal power series $u \in \mathfrak{m}^n$, there exists a unique homogeneous polynomial of degree n in the X_i's which is congruent to $u \bmod \mathfrak{m}^{n+1}$, namely the sum of terms of degree n of u; we conclude that $\mathrm{gr}(A)$ is canonically isomorphic to the polynomial ring $K[X_1, \dots, X_r]$.

Example 11.2.10. More generally, let A be a ring and $\mathfrak{a}$ an ideal of A and A be given the $\mathfrak{a}$-adic filtration. Then the identity mapping of the $A/\mathfrak{a}$-module $\mathfrak{a}/\mathfrak{a}^2$ onto itself can be extended uniquely to a homomorphism ϕ from the symmetric algebra $S(\mathfrak{a}/\mathfrak{a}^2)$ to the $A/\mathfrak{a}$-algebra $\mathrm{gr}(A)$; it follows from the definition of $\mathrm{gr}(A)$ that ϕ is a surjeelive homomorphism of graded algebras; for $n \geq 1$, every element of $\mathrm{gr}_n(A)$ is a sum of classes mod $\mathfrak{a}^{n+1}$ of elements of the form $y = x_1 \cdots x_n$, where $x_i \in \mathfrak{a}$ for $1 \leq i \leq n$; if ξ_i is the class of x_i mod $\mathfrak{a}^2$, clearly the class of y mod $\mathfrak{a}^{n+1}$ is the element $\phi(\xi_1)\cdots\phi(\xi_n)$, whence our assertion. In particular, every system of generators of the $A/\mathfrak{a}$-module $\mathfrak{a}/\mathfrak{a}^2$ is a system of generators of the $A/\mathfrak{a}$-algebra $\mathrm{gr}(A)$.

If now M is an A-module and M is given the $\mathfrak{a}$-adic filtration, it is seen similarly that the graded $\mathrm{gr}(A)$-module $\mathrm{gr}(M)$ is generated by $\mathrm{gr}_0(M) = M/\mathfrak{a}M$. To be precise, the restriction Γ to $\mathrm{gr}(A) \times \mathrm{gr}_0(M)$ of the external law on the $\mathrm{gr}(A)$-module $\mathrm{gr}(M)$ is a $\mathbb{Z}$-bilinear mapping of $\mathrm{gr}(A) \times \mathrm{gr}_0(M)$ to $\mathrm{gr}(M)$. Moreover, it is immediately verified that, for $\alpha \in \mathrm{gr}(A)$, $\beta \in \mathrm{gr}_0(A)$, $\xi \in \mathrm{gr}_0(M)$, we have $\Gamma(\alpha\beta, \xi) = \Gamma(\alpha, \beta\xi)$ and hence Γ defines a canonical surjective $\mathrm{gr}_0(A)$-linear mapping

$$\gamma_M : \mathrm{gr}(A) \otimes_{\mathrm{gr}_0(A)} \mathrm{gr}_0(M) \to \mathrm{gr}(M) \tag{2.2.2}$$

Example 11.2.11. Let A be a graded ring of type $\mathbb{Z}$ and M a graded A-module of type $\mathbb{Z}$; let A^i, (resp. M^i) be the subgroup of homogeneous elements of degree i A (resp. M). Let A and M be

given the filtrations associated with their graduations. Then it is immediate that the $\mathbb{Z}$-linear mapping $A \to \mathrm{gr}(A)$ which maps an element of A^n to its canonical image in

$$\mathrm{gr}_n(A) = \bigoplus_{i \geq n} A^i / \bigoplus_{i \geq n+1} A^i$$

is a graded ring isomorphism. A canonical graded A-module isomorphism $E \to \mathrm{gr}(E)$ is defined similarly.

Proposition 11.2.12. *Let A be a filtered ring, $(A_n)_{n\in\mathbb{Z}}$ its filtration and v its order function. Suppose that $\mathrm{gr}(A)$ is an integral domain. Then, for every elements a, b of the ring $B = \bigcup_n A_n$, we have $v(ab) = v(a) + v(b)$.*

Proof. As $\mathfrak{n} = \bigcap_{n\in\mathbb{Z}} A_n$ is an ideal of the ring B, the formula holds if $v(a)$ or $v(b)$ is equal to $+\infty$. If not, $v(a) = r$ and $v(b) = s$ are integers. The classes $\bar{a}$ of a mod A_{r+1} and $\bar{b}$ of b mod A^{s+1} are nonzero by definition, whence by hypothesis $\bar{a}\bar{b} \neq 0$ in $\mathrm{gr}(A)$ and therefore $ab \notin A_{r+s+1}$; as $ab \in A_{r+s}$, we see $v(ab) = r + s$. □

Corollary 11.2.13. *Let A be a filtered ring and $(A_n)_{n\in\mathbb{Z}}$ its filtration. Define $B = \bigcup_{n\in\mathbb{Z}} A_n$ and $\mathfrak{n} = \bigcap_{n\in\mathbb{Z}} A_n$. If the ring $\mathrm{gr}(A)$ is integral, so is $B/\mathfrak{n}$.*

Proof. If a and b are elements of B not belonging to $\mathfrak{n}$, then $v(a) \neq +\infty$ and $v(b) \neq +\infty$, whence $v(ab) \neq +\infty$ and therefore $ab \notin \mathfrak{n}$. □

11.2.3 Homomorphism compatible with filtrations

Let G, G' be two commutative groups (written additively), (G_n) a filtration on G and (G'_n) a filtration on G'. A homomorphism $\phi : G \to G'$ is called **compatible** with the filtrations on G and G' if $\phi(G_n) \subseteq G'_n$ for all $n \in \mathbb{Z}$. If this holds, then by taking quotients we get a homomorphism $\mathrm{gr}_n(\phi) : G_n/G_{n+1} \to G'_n/G'_{n+1}$ there is therefore a unique additive group homomorphism $\mathrm{gr}(\phi) : \mathrm{gr}(G) \to \mathrm{gr}(G')$ such that, for all $n \in \mathbb{Z}$, $\mathrm{gr}(\phi)$ coincides with $\mathrm{gr}_n(\phi)$ on $\mathrm{gr}_n(G)$. The map $\mathrm{gr}(\phi)$ is called the **graded group homomorphism associated with ϕ**. If G'' is a third filtered group and $\psi : G' \to G''$ is a homomorphism which is compatible with the filtrations, then $\psi \circ \phi$ is a homomorphism which is compatible with the filtrations and we have

$$\mathrm{gr}(\psi \circ \phi) = \mathrm{gr}(\psi) \circ \mathrm{gr}(\phi)$$

Proposition 11.2.14. *Let G be a filtered group and H a subgroup of G; let H be given the induced filtration and G/H the quotient filtration. If $\iota : H \to G$ is the canonical injection and $\pi : G \to G/H$ the canonical surjection, then ι and π are compatible with the filtrations and the sequence*

$$0 \longrightarrow \mathrm{gr}(H) \xrightarrow{\mathrm{gr}(\iota)} \mathrm{gr}(G) \xrightarrow{\mathrm{gr}(\pi)} \mathrm{gr}(G/H) \longrightarrow 0$$

is exact.

Proof. The first assertion is obvious: if (G_n) is the filtration on G, then

$$(H \cap G_n) \cap G_{n+1} = H \cap G_{n+1}.$$

and hence $\mathrm{gr}(\iota)$ is injective; moreover the canonical mapping $G_n \to (H + G_n)/H$ is surjective, hence so is $\mathrm{gr}(\pi)$ and $\mathrm{gr}(\pi) \circ \mathrm{gr}(\iota) = \mathrm{gr}(\pi \circ \iota) = 0$. Finally, let $\xi \in \mathrm{gr}_n(G)$ belong to the kernel of $\mathrm{gr}(\pi)$; then there exists $x \in \xi$ such that $x \in H + G_{n+1}$; but as $G_{n+1} \subseteq G_n$,

$$G_n \cap (H + G_{n+1}) = (H \cap G_n) + G_{n+1}$$

and hence $x = y + z$ where $y \in H \cap G_n$ and $z \in G_{n+1}$; this proves that ξ is the class mod G_{n+1} of $\iota(y)$, in other words it belongs to the image of $\mathrm{gr}(H)$ under $\mathrm{gr}(\iota)$. □

Example 11.2.15. Note that the functor $\mathrm{gr}(\cdot)$ is not exact. Let $A = A' = k[X]$ where k is a field and give A the trivial filtration while A' the (X)-adic filtration. Then the identity map η from A to A' is compatible with the filtrations and we get a sequence

$$0 \longrightarrow \mathrm{gr}(A) \xrightarrow{\mathrm{gr}(\eta)} \mathrm{gr}(A') \longrightarrow 0$$

It is easy to see the map $\mathrm{gr}(\eta)$ is neither injective nor surjective. The point is that the filtration on A differs from the filtration induced by A' via the map η.

If now A and B are two filtered rings and $\rho : A \to B$ a ring homomorphism which is compatible with the filtrations, it is immediately verified that the graded group homomorphism $\mathrm{gr}(\rho) : \mathrm{gr}(A) \to \mathrm{gr}(B)$ is also a ring homomorphism. In particular, if A' is a subring of A with the induced filtration, $\mathrm{gr}(A')$ is canonically identified with a graded subring of $\mathrm{gr}(A)$ (Proposition 11.2.14). If $\mathfrak{a}$ is an ideal of A and $A/\mathfrak{a}$ is given the quotient filtration, $\mathrm{gr}(A/\mathfrak{a})$ is canonically identified with the quotient graded ring $\mathrm{gr}(A)/gr(\mathfrak{a})$ (Proposition 11.2.14).

Finally, let A be a filtered ring, M, N two filtered A-modules and $\phi : M \to N$ an homomorphism compatible with the filtrations. Then it is immediate that $\mathrm{gr}(\phi) : \mathrm{gr}(M) \to \mathrm{gr}(N)$ is a $\mathrm{gr}(A)$-linear mapping and hence a graded homomorphism of degree 0 of graded $\mathrm{gr}(A)$-modules. Moreover, if $\psi : M \to N$ is another A-homomorphism compatible with the filtrations, so is $\phi + \psi$ and we gave $\mathrm{gr}(\phi + \psi) = \mathrm{gr}(\phi) + \mathrm{gr}(\psi)$.

11.3 Filtrations and completions

Let G be a commutative group filtered by a family $(G_n)_{n\in\mathbb{Z}}$ of subgroups of G. There exists a unique topology on G which is compatible with the group structure and for which the G_n constitute a fundamental system of neighbourhoods of the identity element 0 of G (Example 3.1.7); it is called the topology on G defined by the filtration (G_n). When we use topological notions concerning a filtered group, we shall mean, unless otherwise stated, with the topology defined by the filtration. Note that the G_n, being subgroups of G, are both open and closed (Proposition 3.1.17). As G is commutative, we deduce that G admits a Hausdorff completion group $\widehat{G}$ (Theorem 3.2.12). For evcry subset E of G, the closure of E in G is equal to

$$\overline{E} = \bigcap_{n\in\mathbb{Z}} (E + G_n) = \bigcap_{n\in\mathbb{Z}} (G_n + E).$$

In particular $\bigcap_{n\in\mathbb{Z}} G_n$ is the closure of $\{0\}$; thus it is seen that for the topology on G to be Hausdorff it is necessary and suflicient that the filtration (G_n) be separated. On the other hand,

for the topology on G to be discrete, it is necessary and sufficient that there exist $n \in \mathbb{Z}$ such that $G_n = \{0\}$; in this case the filtration (G_n) is called **discrete**.

Not let G' be another filtered group and $\phi : G \to G'$ a homomorphism compatible with the filtrations; the definition of the topologies on G and G' shows immediately that ϕ is continuous. If H is a subgroup of G, the topology induced on H by that on G (resp. the quotient topology with respect to H of that on G) is the topology on H (resp. G/H) defined by the filtration induced by that on G (resp. quotient topology of that on G). The product topology of those on G and G' is the topology defined by the product of filtrations on G and G'.

Proposition 11.3.1. *Let A be a filtered ring, (A_n) its filtration and $B = \bigcup_{n\in\mathbb{Z}} A_n$. If M is a filtered B-module, (M_n) its filtration and $N = \bigcup_{n\in\mathbb{Z}} M_n$ of M, then the mapping $(a, x) \mapsto ax$ from $B \times N$ to N is continuous.*

Proof. Let $a_0 \in B$, $x_0 \in N$; there exists by hypothesis integers r, s such that $a_0 \in A_r$ and $x_0 \in M_s$. The equality

$$ax - a_0x_0 = (a - a_0)x_0 + a_0(x - x_0) + (a - a_0)(x - x_0)$$

shows that if $a - a_0 \in A_i$ and $x - x_0 \in M_j$, then $ax - a_0x_0$ belongs to $M_{i+s} + M_{j+r} + M_{i+j}$. Then, given an integer n, $ax - a_0x_0 \in M_n$ provided $i \geq n - s$, $j \geq n - r$ and $i + j \geq n$; that is so long as i and j are sufficiently large. □

Corollary 11.3.2. *The ring B is a topological ring and the B-module N is a topological B-module.*

It is seen in particular that a filtered ring A whose filtration is exhaustive is a topological ring; if this is so every filtered A-module whose filtration is exhaustive is a topological A-module.

Example 11.3.3. Let A be a ring and $\mathfrak{a}$ an ideal of A; the topology defined on A by the $\mathfrak{a}$-adic filtration is called the $\mathfrak{a}$-adic topology; as the $\mathfrak{a}$-adic filtration is exhaustive, A is a topological ring with this topology. Similarly, for every A-module M, the topology defined by the $\mathfrak{a}$-adic filtration is called the $\mathfrak{a}$-adic topology on M; M is a topological A-module under this topology.

Proposition 11.3.4. *Let A be a ring filtered by an exhaustive filtration (A_n) and $\mathfrak{p}$ an ideal of A. Suppose that the ideal $\mathrm{gr}(\mathfrak{p})$ of the ring $\mathrm{gr}(A)$ is prime. Then the closure of $\mathfrak{p}$ in A is a prime ideal.*

Proof. We know that $\mathrm{gr}(A/\mathfrak{p})$ is isomorphic to $\mathrm{gr}(A)/\mathrm{gr}(\mathfrak{p})$ (Proposition 11.2.14) and hence an integral domain; we conclude that $A/\bigcap_{n\in\mathbb{Z}}(\mathfrak{p} + A_n)$ is an integral domain by Corollary 11.2.13. Thus the closure $\overline{\mathfrak{p}} = \bigcap_{n\in\mathbb{Z}}(\mathfrak{p} + A_n)$ is a prime ideal. □

11.3.1 Complete filtered groups

Proposition 11.3.5. *Let G be a filtered group with filtration (G_n). The following conditions are equivalent:*

(i) G is a complete topological group.

(ii) The associated Hausdorff group $G' = G/(\bigcap_n G_n)$ is complete.

(iii) Every Cauchy sequence in G is convergent.

(iv) Every family $(x_\lambda)_{\lambda\in I}$ of elements of G' which converges to 0 with respect to the filter $\mathfrak{F}$ complements of finite subsets of I is summable in G'.

Proof. For a filter on G to be a Cauchy filter (resp. a convergent filter), it is necessary and sufficient that its image under the canonical mapping $G \to G'$ be a Cauchy (resp. convergent) filter (Proposition 2.2.6); whence first of all the equivalence of (i) and (ii); on the other hand, as G' is first countable, the equivalence of (i) and (iii) follows.

Suppose that G' is complete and let $(x_\lambda)_{\lambda\in I}$ be a family of elements of G' which converge to 0 with respect to G'. For every neighbourhood V' of 0 in G' which is a subgroup of G', there exists a finite subset J of I such that $x_\lambda \in V'$ whenever $\lambda \in I \setminus J$; then $\sum_{\lambda\in K} x_\lambda \in V'$ for every finite subset K of I not meeting J, which shows that the family $(x_\lambda)_{\lambda\in I}$ is summable. Conversely, suppose that condition (iv) holds and let (x_n) be a Cauchy sequence on G',the family $(x_{n+1}-x_n)$ is then summable and in particular the series with general term $x_{n+1} - x_n$ is convergent and hence the sequence (x_n) is convergent. □

Let G be a filtered group whose filtration (G_n); the quotient groups G/G_n are discrete and hence complete, since the G_n's are open in G. For each $n \in \mathbb{Z}$, we have a canonical map $\pi_n : G \to G/G_n$, and for $m < n$ there is a canonical map $\tau_{mn} : G/G_n \to G/G_m$ such that $(G/G_n, \pi_{mn})$ is an inverse system of discrete groups which is compatible with the maps (π_n). By the universal property of inductive limits, we then get a map $\pi : G \to \varprojlim G/G_n$. If $\iota : G \to \widehat{G}$ is the canonical mapping of G to its Hausdorff completion $\widehat{G}$, then as the G/G_n are complete, there exists a unique topological group isomorphism $\psi : \widehat{G} \to \varprojlim G/G_n$ such that $\pi = \psi \circ \iota$ (Corollary 3.3.29), we shall call it the **canonical isomorphism** of $\widehat{G}$ onto $\varprojlim G/G_n$.

$$\begin{tikzcd}
G/G_n \arrow[rr, "\tau_{mn}"] & & G/G_m \\
& \varprojlim G/G_n \arrow[ul, "\tau_n"] \arrow[ur, "\tau_m"'] & \\
& G \arrow[u, "\pi"] \arrow[uul, bend left, "\pi_n"] \arrow[uur, bend right, "\pi_m"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
\widehat{G} \arrow[r, "\psi"] & \varprojlim G/G_n \\
G \arrow[u, "\iota"] \arrow[ur, "\pi"'] &
\end{tikzcd}$$

With the result above, we can apply the prperties of inverse limit to completion. First let us observe that the inverse system $\{G/G_n\}$ has the special property that the transition maps $\tau_{mn} : G/G_n \to G/G_m$ are always surjective. Any inverse system with this property we shall call a **surjective system**. For such a system, we have the following result:

Proposition 11.3.6. *If $0 \to \{A_n\} \to \{B_n\} \to \{C_n\} \to 0$ is an exact sequence of inverse systems then we have an exact sequence*

$$0 \to \varprojlim A_n \to \varprojlim B_n \to \varprojlim C_n \to \varprojlim{}^1 A_n \to \varprojlim{}^1 B_n \to \varprojlim{}^1 C_n \to 0$$

Moreover, $\varprojlim^1 A_n = 0$ if $\{A_n\}$ is a surjective system.

Proof. For an inverse system $\{A_n\}$ let $A = \prod_n A_n$ and define $d_A : A \to A$ by

$$d_A((a_n)) = (a_n - \tau_{n,n+1}(a_{n+1}))$$

so that $\ker d_A = \varprojlim A_n$ and we set $\varprojlim^1 A_n := \operatorname{coker} d_A$. The exact sequence of inverse systems then defines a commutative diagram of exact sequences

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r] \arrow[d, "d_A"] & B \arrow[r] \arrow[d, "d_B"] & C \arrow[r] \arrow[d, "d_C"] & 0 \\ 0 \arrow[r] & A \arrow[r] & B \arrow[r] & C \arrow[r] & 0 \end{tikzcd}$$

and hence by snake lemma an exact sequence

$$0 \longrightarrow \ker d_A \longrightarrow \ker d_B \longrightarrow \ker d_C \longrightarrow \operatorname{coker} d_A \longrightarrow \operatorname{coker} d_B \longrightarrow \operatorname{coker} d_C \longrightarrow 0$$

To complete the proof we have only to prove that d_A is surjective if $\{A_n\}$ is a surjective system. But this is clear because to show d_A surjective we have only to solve inductively the equations $x_n - \tau_{n,n+1}(x_{n+1}) = a_n$ for $x_n \in A_n$, given $a_n \in A_n$. □

Corollary 11.3.7. *Let G be a filtered group and H a subgroup of G; let H be given the induced filtration and G/H the quotient filtration. If $\iota : H \to G$ is the canonical injection and $\pi : G \to G/H$ the canonical surjection, then the sequence*

$$0 \longrightarrow \widehat{H} \longrightarrow \widehat{G} \longrightarrow \widehat{G/H} \longrightarrow 0$$

is exact.

Proof. We have an exact sequence of the correspond inverse systems so Proposition 11.3.6 gives the claim immediately. □

Corollary 11.3.8. *Let G be a filtered group with filtration (G_n). Then $\widehat{G}_n$ is a subgroup of $\widehat{G}$ and $\widehat{G}/\widehat{G}_n \cong G/G_n$. Therefore, we have $\operatorname{gr}(G) \cong \operatorname{gr}(\widehat{G})$.*

Proof. Just apply Corollary 11.3.7 with $H = G_n$, in which case G/G_n has the discrete topology so that $\widehat{G/G_n} = G/G_n$. □

Example 11.3.9. Let G be a complete filtered group. Every closed subgroup of G with the induced filtration is complete. Every quotient group of G with the quotient filtration is complete.

Example 11.3.10. Let A be a ring and $\mathfrak{a}$ an ideal. The completion $\widehat{A}$ of A under the $\mathfrak{a}$-adic topology is called the $\mathfrak{a}$-adic completion of A. The canonical map $\iota : A \to \widehat{A}$ is a continuous ring homomorphism, whose kernel is $\bigcap_n \mathfrak{a}^n$.

Let M be an A-module, the completion $\widehat{M}$ of M under the $\mathfrak{a}$-adic topology is a topological $\widehat{A}$-module. If $\phi : M \to N$ is any A-module homomorphism, then $\phi(\mathfrak{a}^n M) = \mathfrak{a}^n \phi(M) \subseteq \mathfrak{a}^n N$, and therefore ϕ is continuous (with respect to the $\mathfrak{a}$-topologies on M and N) and so defines $\widehat{\phi} : \widehat{M} \to \widehat{N}$.

Example 11.3.11. Let A be a filtered ring whose filtration we denote by $(A_n)_{n\in\mathbb{Z}}$; let $B = A[\![X_1, \dots, X_r]\!]$. For all $\alpha = (\alpha_1, \dots, \alpha_s) \in \mathbb{N}^s$, we write $|\alpha| = \sum_{i=1}^s e_i$ and $X^\alpha = X_1^{\alpha_1} \cdots X_s^{\alpha_s}$ so that every element $P \in B$ can be written uniquely $P = \sum_{\alpha\in\mathbb{N}^s} c_{\alpha,P} X^\alpha$, where $c_{\alpha,P} \in A$. For all $n \in \mathbb{Z}$, define

$$B_n = \{P = \sum_\alpha c_{\alpha,P} X^\alpha : c_{\alpha,P} \in A_{n-|\alpha|} \text{ for all } \alpha \in \mathbb{N}^s\}.$$

Clearly B_n is an additive subgroup of B; on the other hand, if $P \in B_n$ and $Q \in B$, then, for all $\alpha \in \mathbb{N}^s$, $c_{\gamma,PQ} = \sum_{\alpha+\beta=\gamma} c_{\alpha,P} c_{\beta,Q}$; as the relation $\alpha + \beta = \gamma$ implies $|\alpha| \leq |\gamma|$, we have $PQ \in B_n$, so B_n is an ideal of B. Moreover, if $Q \in B_m$, then for $\alpha + \beta = \gamma$,

$$c_{\alpha,P} c_{\beta,Q} \in A_{n-|\alpha|} A_{n-|\beta|} \subseteq A_{m+n-|\gamma|},$$

which proves that $(B_n)_{n\in\mathbb{Z}}$ is a filtration compatible with the ring structure on B (for obviously $1 \in B_0$). When in future we speak of B as a filtered ring, we shall mean, unless otherwise stated, with the filtration (B_n). Clearly $\bigcap_{n\in\mathbb{Z}} B_n$ is the set of formal power series all of whose coefficients belong to $\bigcap_{n\in\mathbb{Z}} A_n$; then, if A is Hausdorff, so is B. If $A_0 = A$, then $B_0 = B$.

Proposition 11.3.12. *With the above notation, suppose that $A_0 = A$ and let h denote the mapping $P \mapsto (c_{\alpha,P})_{\alpha\in\mathbb{N}^s}$. Then h is an isomorphism of the additive topological group B onto the additive topological group $A^{\mathbb{N}^s}$. The polynomial ring $A[X_1, \ldots, X_s]$ is dense in B; if A is complete, so is B.*

Proof. Clearly h is bijective; $V_n = h(B_n)$ is the set of $(c_\alpha)_{\alpha\in\mathbb{N}^s}$ such that $c_\alpha \in A_{n-|\alpha|}$ for all $\alpha \in \mathbb{N}^s$ such that $|\alpha| \leq n$; as these elements α are finite in number, V_n is a neighbourhood of 0 in $A^{\mathbb{N}^s}$. Conversely, if V is a neighbourhood of 0 in $A^{\mathbb{N}^s}$, there is a finite subset E of $\mathbb{N}^s$ and an integer ν such that the conditions $c_\alpha \in A_\nu$ for all $\alpha \in E$ imply $(c_\alpha) \in V$; if then n is the greatest of the integers $\nu + |\alpha|$ for $\alpha \in E$, then $h(A_n) \subseteq V$, which proves the first assertion. Moreover, with n and E defined as above, $h(P - \sum_{\alpha\in E} c_{\alpha,P} X^\alpha) \in V$ for all $P \in B$, which shows that $A[X_1, \ldots, X_s]$ is dense in B. The last assertion follows from the first and the fact that a product of complete spaces is complete. □

Let $\mathfrak{a}$ be an ideal of A and suppose that (A_n) is the $\mathfrak{a}$-adic filtration; then, if $\mathfrak{b}$ is the ideal of B generated by $\mathfrak{a}$ and $X_1, \ldots, X_s$, the filtration (B_n) is the $\mathfrak{b}$-adic filtration. For clearly, for all $n \geq 0$, $\mathfrak{b}^n$ is generated by the elements cX^α such that $c \in \mathfrak{b}^{n-|\alpha|}$ for all $\alpha \in \mathbb{N}^s$ such that $|\alpha| \leq n$, whence $\mathfrak{b}^n \subseteq B_n$. Conversely, for all $P \in B_n$, $P = P_1 + P_2$, where

$$P_1 = \sum_{|\alpha|<n} c_{\alpha,P} X^\alpha, \quad P_2 = \sum_{|\alpha|\geq n} c_{\alpha,P} X^\alpha$$

Clearly it is possible to write $P_2 = \sum_{|\alpha|=n} Q_\alpha X^\alpha$, where the Q_α are elements of B, whence $P_2 \in \mathfrak{b}^n$; on the other hand, since $P \in B_n$, we have $c_{\alpha,P} X^\alpha \in \mathfrak{b}^n$ for all $|\alpha| \leq n$, whence $P_1 \in \mathfrak{b}^n$.

Corollary 11.3.13. *Let A be a ring and $B = A[\![X_1, \ldots, X_r]\!]$ the ring of formal power series in s indeterminates over A and $\mathfrak{n}$ the ideal of B consisting of the formal power series with no constant term. The ring B is Hausdorff and complete with the $\mathfrak{n}$-adic topology and the polynomial ring $A[X_1, \ldots, X_r]$ is everywhere dense in B.*

Proof. It is sufficient to apply what has just been said to the case $\mathfrak{m} = \{0\}$, so that the $\mathfrak{m}$-adic topology on A is trivial and A is thus complete. □

11.3.2 Completion of filtered rings and modules

Let A be a filtered ring, M a filtered A-module and (A_n) and (M_n) the respective filtrations of A and M; we shall assume that these filtrations are exhaustive so that for the corresponding topologies A is a topological ring and M a topological A-module (Proposition 11.3.1). Then we have defined $\widehat{A}$ as a topological ring and $\widehat{M}$ as a topological $\widehat{A}$-module. If $\iota : A \to \widehat{A}$

is the canonical homomorphism, then $\iota(A_m)\iota(A_n) \subseteq \iota(A_{m+n})$, whence by the continuity of multiplication in $\widehat{A}$,

$$\widehat{A}_n\widehat{A}_m \subseteq \widehat{A}_{m+n}$$

where $\widehat{A}_n$ is the closure of $\iota(A_n)$ in A. It can be similarly shown that $\widehat{A}_n\widehat{M}_m \subseteq \widehat{M}_{m+n}$, in other words,

Proposition 11.3.14. *Let A be a filtered ring and M a filtered A-module, the respective filtrations (A_n), (E_n) of A and M being exhaustive. Then $(\widehat{A}_n)$ is a filtration compatible with the ring structure on $\widehat{A}$ and $(\widehat{M}_n)$ is a filtration compatible with the module structure on $\widehat{A}$ over the filtered ring $\widehat{A}$. Moreover, these filtrations are exhaustive and define respectively the topologies on $\widehat{A}$ and $\widehat{M}$. Finally, the canonical mappings $\mathrm{gr}(A) \to \mathrm{gr}(\widehat{A})$ and $\mathrm{gr}(M) \to \mathrm{gr}(\widehat{M})$ of graded $\mathbb{Z}$-modules are respectively a graded ring isomorphism and a graded $\mathrm{gr}(A)$ -module isomorphism.*

In what follows, for every uniform space X, ι_X will denote the canonical mapping from X to its Hausdorff completion $\widehat{X}$ and $X_0 = \iota_X(X)$ the uniform subspace of X, which is the Hausdorff space associated with X. Recall that the topology on X is the inverse image under ι_X of that on X_0. Recall also that, for every uniformly continuous mapping $f : X \to Y$, $\hat{f}$ denotes the uniformly continuous mapping from $\widehat{X}$ to $\widehat{Y}$ such that $\hat{f} \circ \iota_X = \iota_Y \circ f$. If X is a uniform subspace of Y and i is the canonical injection, then $\widehat{X}$ is identified with a uniform subspace of $\widehat{Y}$ and $\hat{i}$ is the canonical injection of $\widehat{X}$ into $\widehat{Y}$ (Proposition 2.2.40).

Lemma 11.3.15. *Let $0 \to X \to Y \to Z \to 0$ be an exact sequence of strict morphism of topological groups. Suppose that X, Y, Z admit Hausdorff completion groups and that the identity elements of X, Y, Z admit countable fundamental systems of neighbourhoods. Then*

$$0 \longrightarrow \widehat{X} \longrightarrow \widehat{Y} \longrightarrow \widehat{Z} \longrightarrow 0$$

is an exact sequence of strict morphisms.

Proof. Let $f : X \to Y$ and $g : Y \to Z$ be the given maps. We have already seen that the completion of a strict injection is strict injective, so it remains to show the following: if $Y = X/N$ (where N is a subgroup of X) and $f : X \to Y$ is the canonical mapping, then $\hat{f}$ is a surjective strict morphism with kernel $\widehat{N}$.

Let $X_0 = \iota_X(X)$ and $Y_0 = \iota_Y(Y)$; let $f_0 : X_0 \to Y_0$ be the map which coincides with $\hat{f}$ on X_0; as ι_X (resp. ι_Y) is a surjective strict morphism of X onto X_0 (resp. Y onto Y_0), f_0 is a surjective strict morphism by Example 3.1.42. Now X_0 and Y_0 are metrizable, so it follows from **??** that $\hat{f}_0 = \hat{f}$ is a surjective strict morphism and has kernel the closure $\widehat{N}'_0$ in $\widehat{X}$ of the kernel N'_0 of f_0. Then it will be sufficient for us to prove that $\widehat{N}'_0 = \widehat{N}$. Now N'_0 obviously contains $N_0 = \iota_X(N)$, so $\widehat{N}'_0 \supseteq \widehat{N}$; it will be sufficient to show that N'_0 is contained in the closure $\overline{N}_0$ of N_0 in X_0. Now,

$$U = \iota_X^{-1}(X_0 \setminus \overline{N}_0) = X \setminus \iota_X^{-1}(\overline{N}_0)$$

is an open set in X which does not meet N; as f is a surjective strict morphism, $V = f(U)$ is an open set in Y not containing the identity element 0 of Y and hence not meeting the closure of $\{0\}$; then $\iota_Y(V)$ does not contain the identity element of Y_0. But $\iota_Y(V) = f_0(X_0 \setminus N_0)$ and hence $N'_0 \subseteq \overline{N}_0$, which complete the proof. □

Proposition 11.3.16. *Let A be a filtered ring, (A_n) its filtration, M an A-module and (M_n) the filtration on M derived from that on A. Suppose that the filtration (A_n) is exhaustive and the module M is finitely generated. If $\iota_M : M \to \widehat{M}$ is the canonical mapping, then, for all $n \in \mathbb{Z}$,*

$$\widehat{M}_n = \widehat{A}_n\widehat{M} = \widehat{A}_n\iota_M(M), \quad \widehat{M} = \widehat{A}\widehat{M} = \widehat{A}\iota_M(M).$$

In particular $\widehat{M}$ is a finitely generated $\widehat{A}$-module.

Proof. By hypothesis there exists a surjective homomorphism $\phi : L \to M$, where $L = A^I$, I being a finite set; let L be given the product filtration, consisting of the $L_n = A_n^I$; then $\widehat{L} = \widehat{A}^I$ and $\widehat{L}_n = \widehat{A}_n^I$. Let $\iota_L : L \to \widehat{L}$ be the canonical mapping and $(e_i)_{i\in I}$ the canonical basis of L; for an element $\sum_i a_i\iota_L(e_i)$ of $\widehat{L}_n$ to belong to $\widehat{L}_n$, it is necessary and sufficient that $a_i \in \widehat{A}_n$ for all i, thus we see $\widehat{L}_n = \widehat{A}_n\widehat{L} = \widehat{A}_n\iota_L(L)$.

Now note that by definition $\phi(L_n) = M_n$ and hence ϕ is a strict morphism of L onto M. Lemma 11.3.15 then shows that $\hat{\phi} : \widehat{L} \to \widehat{M}$ is a surjective strict morphism. As L_n is an open subgroup of $\widehat{L}$, $\hat{\phi}(\widehat{L}_n)$ is an open (and therefore closed) subgroup of M; but by what we have just proved,

$$\hat{\phi}(\widehat{L}_n) = \hat{\phi}(\widehat{A}_n\iota_L(L)) = \widehat{A}_n\iota_M(M).$$

As $\iota_M(M_n) \subseteq \widehat{A}_n\iota_M(M)$, this then implies

$$\widehat{M}_n \subseteq \widehat{A}_n\iota_M(M) \subseteq \widehat{A}_n\widehat{M} \subseteq \widehat{M}_n$$

and therefore $\widehat{M}_n = \widehat{A}_n\widehat{M} = \widehat{A}_n\iota_M(M)$. Take the union of all $n \in \mathbb{Z}$, we obtain the second formula. □

Corollary 11.3.17. *Under the conditions of Proposition 11.3.16, if A is complete, so is M.*

Proof. As the canonical mapping $A \to \widehat{A}$ is then surjective, $M = \iota_M(M)$ by Proposition 11.3.5 and the conclusion follows from Proposition 11.3.5. □

Corollary 11.3.18. *Let A be a ring, $\mathfrak{a}$ a finitely generated ideal of A and $\widehat{A}$ the Hausdorff ompletion of A with respect to the $\mathfrak{a}$-adic topology. Then $\widehat{\mathfrak{a}^n} = (\hat{\mathfrak{a}})^n = \widehat{A}\mathfrak{a}^n$ for every integer $n > 0$ and the topology on $\widehat{A}$ is the $\hat{\mathfrak{a}}$-adic topology.*

Proof. Let us write $A_n = \mathfrak{a}^n$, which is a finitely generated ideal of A. The formula $\mathfrak{a}^pA_n = \mathfrak{a}^{n+p}$ shows that the topology induced on A_n by the $\mathfrak{a}$-adic topology coincides with the $\mathfrak{a}$-adic topology on the A-module A_n. By Proposition 11.3.16 applied to $M = A_n$, $\widehat{A}_n = \widehat{A}A_n$, in other words $\widehat{\mathfrak{a}^n} = \widehat{A}\mathfrak{a}^n$. In particular $\hat{\mathfrak{a}} = \widehat{A}\mathfrak{a}$, whence $(\hat{\mathfrak{a}})^n = \widehat{A}\mathfrak{a}^n$. □

Example 11.3.19. Let A be a graded ring of type $\mathbb{N}$ and let $(A^n)_{n\geq 0}$ be its graduation; let it be given the associated filtration which is separated and exhaustive. The additive group A is canonically identified with the subspace $\bigoplus_{n\in\mathbb{N}} A^n$ in $B = \prod_{n\in\mathbb{N}} A^n$. If B is given the topology the product of the discrete topologies, the topology induced on A is the topology defined by the filtration on A; also B is a complete topological group and A is dense in B. The additive topological group B is then identified with the completion $\widehat{A}$ of the Hausdorff additive group A and it has a unique ring structure which makes it the completion of the topological ring A. To define multiplication in this ring, note that, if we write $A_n = \bigoplus_{i\geq n} A^i$, the closure in B of the ideal A_n is the set B_n of $x = (x_n)$ such that $x_n = 0$ for $i < n$. Let $x = (x_n)$, $y = (y_n)$ be two

elements of B and $z = (z_n)$ their product. Then, for all $n > 0$, $x \equiv x^{(n)} \bmod B_{n+1}$ and $y \equiv y^{(n)} \bmod B_{n+1}$. But $x^{(n)}$ and $y^{(n)}$ belong to A and it is therefore seen that, for all $n \in \mathbb{N}$,

$$z_n = \sum_{i+j=n} x_i y_j.$$

In particular, we again obtain that, if A is a ring, the completion of the polynomial ring $A[X_1, \dots, X_r]$ with the filtration associated with its usual graduation (by total degree) is canonically identified with the ring of formal power series $A[\![X_1, \dots, X_r]\!]$.

Example 11.3.20. Let α be a non-zero non-invertible element of a principal ideal domain; the (α)-adic topology on A is also called the α-adic topology; it is Hausdorff for the intersection of the ideals (α^n) reduces to 0. Note that the completion of A with respect to this topology is not necessarily an integral domain. The associated graded ring $\mathrm{gr}(A) = \mathrm{gr}(\widehat{A})$ is canonically isomorphic to $(A/\alpha)[X]$. If $A = \mathbb{Z}$, the completion of $\mathbb{Z}$ with respect to the α-adic topology $(n > 1)$ is denoted by $\mathbb{Z}_\alpha$, and its elements are called α-adic integers.

Example 11.3.21. Let k be a field, $A = k[(X_n)_{n\in\mathbb{N}}]$, and $\mathfrak{m} = (X_1, X_2, \dots)$. We will think of an element $f \in \widehat{A}$ as a (possibly) infinite sum

$$f(X) = \sum_I a_I X^I$$

(using multi-index notation) such that for each $d \geq 0$ there are only finitely many nonzero a_I for $|I| = d$. The maximal ideal $\hat{\mathfrak{m}}$ in $\widehat{A}$ is the collection of f with zero constant term. In particular, the element

$$f = X_1 + X_2^2 + X_3^2 + \cdots$$

is in $\hat{\mathfrak{m}}$ but not in $\mathfrak{m}\widehat{A}$. This shows the inclusion $\mathfrak{m}\widehat{A} \subseteq \hat{\mathfrak{m}}$ is proper.

Proposition 11.3.22. *Let A be a ring and $(\mathfrak{a}_\lambda)_{\lambda\in I}$ a family of ideals of A, distinct from A, such that $\mathfrak{a}_\lambda$ and $\mathfrak{a}_\mu$ are relatively prime for $\alpha, \mu \in I$. For every family $s = (s_\lambda)_{\lambda\in I}$ of positive integers of finite support, set $\mathfrak{a}_s = \bigcap_{\lambda\in I} \mathfrak{a}_\lambda^{s_\lambda}$, and let $\mathcal{T}$ be the topology compatible with the ring structure on A such that the $\mathfrak{a}_s$'s form a fundamental system of neighbourhoods of 0. Let $\widehat{A}$ be the Hausdorff completion of A with respect to this topology. On the other hand, for all $\lambda \in I$, let A_λ be the ring A with the $\mathfrak{a}_\lambda$-adic topology and let $\widehat{A}_\lambda$ be its Hausdorff completion. If $\phi : A \to \prod_{\lambda\in I} A_\lambda$ denotes the diagonal homomorphism, then ϕ is continuous and the corresponding homomorphism*

$$\hat{\phi} : \widehat{A} \to \prod_{\lambda\in I} \widehat{A}_\lambda$$

is a topological ring isomorphism.

Proof. Note that $\mathcal{T}$ is the least upper bound of all $\mathfrak{a}_\lambda$-adic topologies. The first assertion follows from Example 3.3.8. Let us set $B = \prod_{\lambda\in I} A_\lambda$; as the topology on A is finer than each of the $\mathfrak{a}_\lambda$-adic topologies, the mappings $\pi_\lambda \circ \phi$ are continuous and hence ϕ is continuous. Also, $\phi(\mathfrak{a}_s)$ is the intersection of the diagonal Δ of B and the open set $\bigcap_{\lambda\in I} \pi_\lambda^{-1}(\mathfrak{a}_\lambda^{s_\lambda})$, it follows that ϕ is a strict morphism from the additive group A to B with image A. Now A is dense in B. For let $b = (a_\lambda)$ be an element of B; every neighbourhood of b in B contains a set of the form $b + V$, where $V = \bigcap_{\lambda\in I} \pi_\lambda^{-1}(\mathfrak{a}_\lambda^{s_\lambda})$ for a family $s = (s_\lambda)$ of positive integers with finite support. As the $\mathfrak{a}_\lambda$'s are

relatively prime in pairs, there exists $x \in A$ such that $x \equiv a_\lambda \bmod \mathfrak{a}_\lambda^{s_\lambda}$ for all $\lambda \in I$ (by CRT, note that (s_λ) has finite support) and hence $(b+V) \cap \Delta \neq \varnothing$. The Hausdorff completion of the group B/Δ is then $\{0\}$; applying Lemma 11.3.15 to the exact sequences $0 \to A \to B \to B/\Delta \to 0$, we see $\hat{\phi}$ is an isomorphism of $\widehat{A}$ onto $\widehat{B}$. □

Corollary 11.3.23. *Let A be a PID and P a representative system of elements of A such that the ideals πA with $\pi \in P$ run though all the maximal ideals of A. The topology on A with respect to which the nonzero ideals of A form a fundamental system of neighbourhoods of 0, which is compatible with the ring structure on A, is Hausdorff and the completion of A with this topology is canonically isomorphic to the product of the completions of A with respect to the π-adic topologies, where π runs through P.*

Proof. The principal ideals πA where $\pi \in P$ are maximal and distinct and hence relatively prime, we have already seen that the π-adic topologies are Hausdorff and hence so is the topology defined in the statement of Proposition 11.3.22, which is finer than each of the π-adic topologies. □

If Corollary 11.3.23 is applied when $A = \mathbb{Z}$, we denote by $\widehat{Z}$ the completion of $\mathbb{Z}$ with respect to the topology for which all the nonzero ideals of $\mathbb{Z}$ form a fundamental system of neighbourhoods of 0, the ring isomorphic to the product $\prod_{p \in P} \mathbb{Z}_p$ of the rings of $\mathfrak{p}$-adic integers (P being the set of prime numbers), and is usually denoted by $\widehat{\mathbb{Z}}$.

Proposition 11.3.24. *Let A be a ring, $(\mathfrak{m}_i)_{1 \le i \le r}$ a finite family of distinct maximal ideals of A and set*

$$\mathfrak{t} = \prod_{i=1}^{r} \mathfrak{m}_i = \bigcap_{i=1}^{n} \mathfrak{m}_i, \quad S = \bigcap_{i=1}^{r} (A - \mathfrak{m}_i).$$

Endow A with the $\mathfrak{t}$-adic topology, $S^{-1}A$ the $S^{-1}\mathfrak{t}$-adic topology and each of the local ring $A_{\mathfrak{m}_i}$ the $(\mathfrak{m}_i A_{\mathfrak{m}_i})$-adic topology. Let $\phi : A \to S^{-1}A$ and $\psi : S^{-1}A \to \prod_{i=1}^{r} A_{\mathfrak{m}_i}$ be the canonical homomorphisms. Then ϕ and ψ are continuous and the corresponding homomorphisms $\hat{\phi}$ and $\hat{\psi}$ are topological ring isomorphism.

Proof. Since $\mathfrak{m}_i \cap S = \varnothing$ for each $i \in I$, the ideal $\mathfrak{m}'_i = \mathfrak{m}_i B$ of B is maximal and we have $S^{-1}\mathfrak{t} = \bigcap_{i=1}^{r} \mathfrak{m}'_i$. Also, $B_{\mathfrak{m}'_i} = A_{\mathfrak{m}_i}$ up to a canonical isomorphism. As $\phi^{-1}(\mathfrak{t}B) = \mathfrak{t}$ and $\psi_i^{-1}(\mathfrak{m}_i A_{\mathfrak{m}_i}) \supseteq \mathfrak{t}B$, ϕ and ψ are continuous. Then it is sufficient to prove that, if

$$\omega = \psi \circ \phi : A \to \prod_{i=1}^{r} A_{\mathfrak{m}_i}$$

then $\hat{\omega}$ is an isomorphism of $\widehat{A}$ onto $\prod_{i=1}^{r} \widehat{A}_{\mathfrak{m}_i}$, for this result applied to B and the $\mathfrak{m}'_i$ will show that $\hat{\psi}$ is an isomorphism and therefore also $\hat{\phi}$. Note that every product of powers of the $\mathfrak{m}_i$ contains a power of $\mathfrak{t}$ and hence the $\mathfrak{t}$-adic topology is the least upper bound of the $\mathfrak{m}_i$-adic topologies; moreover, if A_i denotes the ring A with the $\mathfrak{m}_i$-adic topology and $\gamma : A \to \prod_{i=1}^{r} A_i$ is the diagonal mapping, then $\hat{\gamma} : \widehat{A} \to \prod_{i=1}^{r} \widehat{A}_i$ is an isomorphism (Proposition 11.3.22). Then it all amounts to proving that, if $v_i : A_i \to A_{\mathfrak{m}_i}$ is the canonical mapping, then $\hat{v}_i : \widehat{A}_i \to \widehat{A}_{\mathfrak{m}_i}$ is an isomorphism. Now, for all n, the mapping

$$v_{i,n} : A/\mathfrak{m}_i^n \to A_{\mathfrak{m}_i}/\mathfrak{m}_i^n A_{\mathfrak{m}_i}$$

derived from v_i by taking quotients is an isomorphism; our assertion follows from the fact that $\widehat{A}_i$ (resp. $\widehat{A}_{\mathfrak{m}_i}$) is the inverse limit of the discrete rings $A/\mathfrak{m}_i^n$ (resp. $A_{\mathfrak{m}_i}/\mathfrak{m}_i A_{\mathfrak{m}_i}$). □

Now we want to consider the $\mathfrak{m}$-adic completion of a maximal ideal $\mathfrak{m}$ of A. Before this, let us prove the following useful lemma.

Lemma 11.3.25. *Let A be a complete Hausdorff topological ring, in which there exists a fundamental system of neighbourhoods of* 0 *consisting of additive subgroups of A.*

(a) For all $x \in A$ such that $\lim_n x^n = 0$, then $1 - x$ is invertible in A and its inverse is equal to $\sum_n x^n$.

(b) Let $\mathfrak{a}$ be an ideal of A such that $\lim_n x^n = 0$ for all $x \in \mathfrak{a}$. For an element y of A to be invertible, it is necessary and suflicient that its class mod $\mathfrak{a}$ be invertible in $A/\mathfrak{a}$; in particular $\mathfrak{a}$ is contained in the Jacobson radical of A.

Proof. Note that

$$(1 - x)(1 + x + x^2 + \cdots + x^n) = 1 - x^{n+1}$$

so for (a) it all amounts to proving that the series with general term x^n is convergent in A when $\lim_n x^n = 0$; now, by hypothesis, for every symmetric neighbourhood V of 0 in A, there exists an integer $p > 0$ such that $x^n \in V$ for all $n \geq p$. We conclude that

$$x^p + \cdots + x^q \in V$$

for all $q \geq p$ and our assertion then follows from Cauchy's criterion, since A is complete.

Suppose that there exists $y \in A$ such that $yz \equiv 1 \bmod \mathfrak{a}$. The hypothesis on $\mathfrak{a}$ implies, by (a), that yz is invertible in A and hence y is invertible in A. In particular, every $x \in \mathfrak{a}$ is such that $1 - x$ is invertible in A and, as $\mathfrak{a}$ is an ideal of A, it is contained in the Jacobson radical of A. □

Proposition 11.3.26. *Let A be a ring and $\mathfrak{m}$ a maximal ideal of A. The Hausdorff completion A of A with respect to the $\mathfrak{m}$-adic topology is a local ring whose maximal ideal is $\widehat{\mathfrak{m}}$.*

Proof. If $\mathfrak{n} = \bigcap_{n \geq 1} \mathfrak{m}^n$, then $\widehat{A}$ is the completion of the Hausdorff ring $A/\mathfrak{n}$ associated with A and, as $\mathfrak{m}/\mathfrak{n}$ is maximal in $A/\mathfrak{n}$, we may assume that A is Hausdorff with respect to the $\mathfrak{m}$-adic topology. As $A/\mathfrak{m}$ and $\widehat{A}/\widehat{\mathfrak{m}}$ are isomorphic rings, $\widehat{\mathfrak{m}}$ is maximal in $\widehat{A}$. As the topology on A is defined by the filtration $(\mathfrak{m}^n)$, the proposition will be a consequence of Lemma 11.3.25: apply it to the topological ring $\widehat{A}$ and the ideal $\widehat{\mathfrak{m}}$, as, for all $x \in \widehat{\mathfrak{m}}$, $x^n \in (\widehat{\mathfrak{m}})^n \subseteq \widehat{\mathfrak{m}^n}$ and the sequence (x^n) therefore tends to 0. □

Example 11.3.27. If we take $A = \mathbb{Z}$, every maximal ideal of $\mathbb{Z}$ is of the form $p\mathbb{Z}$ where p is prime. The ring of p-adic numbers $\mathbb{Z}_p$ is then a local ring of which $\mathfrak{p}\mathbb{Z}_p$ is the maximal ideal and whose residue field is isomorphic to $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$, and $\mathbb{Z}_{(p)}$ with the $p\mathbb{Z}_{(p)}$-adic topology is identified with a topological subring of $\mathbb{Z}_p$ containing $\mathbb{Z}$.

Corollary 11.3.28. *Let A be a semi-local ring, $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ its distinct maximal ideals and*

$$\mathfrak{t} = \bigcap_{i=1}^{r} \mathfrak{m}_i = \prod_{i=1}^{r} \mathfrak{m}_i$$

its Jacobson radical. Then the Hausdorff completion $\widehat{A}$ of A with respect to the $\mathfrak{t}$*-adic topology is a semi-local ring, canonically isomorphic to the product $\prod_{i=1}^{r} \widehat{A}_{\mathfrak{m}_i}$, where $\widehat{A}_{\mathfrak{m}_i}$ is the Hausdorff completion ring of the local ring $A_{\mathfrak{m}_i}$ with respect to the $(\mathfrak{m}_i A_{\mathfrak{m}_i})$-adic topology.*

11.3.3 Lifting properties of the associated graduation

Theorem 11.3.29. *Let X, Y be two filtered groups with filtrations (X_n), (Y_n); let $\phi : X \to Y$ be a homomorphism compatible with the filtrations.*

(a) Suppose that the filtration (X_n) is exhaustive. For $\mathrm{gr}(\phi)$ to be injective, it is necessary and sufiicient that $\phi^{-1}(Y_n) = X_n$ for all $n \in \mathbb{Z}$.

(b) Suppose that one of the following hypotheses holds:

(α) X is complete and Y Hausdorff.

(β) Y is discrete.

Then, for $\mathrm{gr}(\phi)$ to be surjective, it is necessary and suficient that $Y_n = \phi(X_n)$ for all $n \in \mathbb{Z}$.

Proof. To say that the mapping $\mathrm{gr}_n(\phi)$ is injective means that

$$X_n \cap \phi^{-1}(Y_{n+1}) \subseteq X_{n+1}.$$

This is obviously the case if $\phi^{-1}(Y_{n+1}) = X_{n+1}$. Conversely, if this holds for all n, we deduce by induction on k that

$$X_m \cap \phi^{-1}(Y_{n+1}) \subseteq X_{n+1} \quad \text{for all } m, n \in \mathbb{Z} \text{ with } m < n+1.$$

As the filtration (X_n) is exhaustive, we see $\bigcup_{m<n} X_m = X$, hence $\phi^{-1}(Y_{n+1}) \subseteq X_{n+1}$ for all $n \in \mathbb{Z}$ and therefore $\phi^{-1}(Y_{n+1}) = X_{n+1}$, which completes the proof of (a).

To say that the mapping $\mathrm{gr}_n(\phi)$ is surjective means that

$$Y_n = \phi(X_n) + Y_{n+1}.$$

This is obviously the case if $Y_n = \phi(X_n)$. Conversely, suppose that $Y_n = \phi(X_n) + Y_{n+1}$ for all $n \in \mathbb{Z}$. Let n be an integer and y an element of Y_n; we now define a sequence (x_k) of elements of X_n such that for all $k \geq 0$,

$$x_{k+1} \equiv x_k \mod X_{n+k} \quad \text{and} \quad \phi(x_k) \equiv y \mod Y_{n+k}.$$

First we take x_0 equal to the identity element of X, which certainly gives $\phi(x_0) \equiv y \bmod Y_n$. Suppose that $x_k \in X_n$ has been constructed such that $\phi(x_k) \equiv y \bmod Y_{n+k}$; then $y - \phi(x_k) \in Y_{n+k} = \phi(X_{n+k}) + Y_{n+k+1}$ so there exists $t \in X_{n+k}$ such that $y - \phi(x_k) \equiv \phi(t) \bmod Y_{n+k+1}$ and hence $\phi(x_k + t) \equiv y \bmod Y_{n+k+1}$; it then sufficies to take $x_{k+1} = x_k + t$ to carry out the induction.

This being done, if Y is discrete, there exists $k \geq 0$ such that $Y_{n+k} = \{0\}$, whence $\phi(x_k) = y$ and hence in this case it has been proved that $\phi(X_n) = Y_n$ for all n. Suppose now that X is complete and Y Hausdorff. As $x_k - x_j \in X_{n+k}$ for $j \geq k$, (x_k) is a Cauchy sequence in X; as X_n is closed in X and hence complete, this sequence has at least one limit x in X_n. By virtue of the continuity of ϕ, $\phi(x)$ is the unique limit of the sequence $(\phi(x_k))$ in Y, Y being Hausdorff.

But the relations $\phi(x_k) \equiv y \bmod Y_{n+k+1}$ show that y is also a limit of this sequence, whence $\phi(x) = y$ and it has also been proved that $\phi(X_n) = Y_n$. □

Corollary 11.3.30. *Suppose that X is Hausdorff and its filtration exhaustive. Then, if $\mathrm{gr}(\phi)$ is injective, ϕ is injective.*

Proof. Since $\phi^{-1}(Y_n) = X_n$, we have $\ker \phi \subseteq \bigcap_n \phi^{-1}(Y_n) = \bigcap_n X_n$, whence the corollary. □

Corollary 11.3.31. *Suppose that one of the following hypotheses holds:*

(α) X is complete, Y is Hausdorff and its filtration is exhaustive;

(β) Y is discrete and its filtration is exhaustive.

Then, if $\mathrm{gr}(\phi)$ is surjective, ϕ is surjective.

Proof. In this case $Y = \bigcup_n Y_n = \bigcup_n \phi(X_n) \subseteq \phi(X)$ by Theorem 11.3.29. □

Corollary 11.3.32. *Suppose that X and Y are Hausdorff, the filtrations of X and Y exhaustive and X complete. Then, if $\mathrm{gr}(\phi)$ is bijective, ϕ is bijective.*

Proposition 11.3.33. *Let A be a filtered ring, M a filtered A-module and (A_n) and (M_n) the respective filtrations on A and M. Suppose that A is complete and the filtration (M_n) is exhaustive and separated. Let $(x_i)_{i\in I}$ be a finite family of elements of M and for $i \in I$ let n_i be an integer such that $x_i \in M_{n_i}$. Finally let ξ_i be the class of x_i in $\mathrm{gr}_{n_i}(M)$. Then, if (ξ_i) is a system of generators of the $\mathrm{gr}(A)$-module $\mathrm{gr}(M)$, then (x_i) is a system of generators of the A-module M.*

Proof. In the A-module $L = A^I$ let L_n denote the set (a_i) such that $a_i \in A_{n-n_i}$ for all $i \in I$; if p and q are the least and greatest of the n_i, then $A^I_{n-p} \subseteq L_n \subseteq A^I_{n-q}$, so the topology defined on L by the definition (L_n) is the same as the product topology; hence L is a complete filtered A-module. As L is free, there exists an A-linear mapping $\phi : L \to M$ such that $\phi((a_i)) = \sum_i a_i x_i$ and it is obviously compatible with the filtrations; we must prove that ϕ is surjective and for this it is sufficient, by virtue of Corollary 11.3.31, to show that $\mathrm{gr}(\phi)$ is surjective or also that, for all $x \in M_n$, there exist a family (a_i) such that $a_i \in A_{n-n_i}$ for all $i \in I$ and $x \equiv \sum_i a_i x_i \bmod M_{n+1}$. Let ξ be the class of x in $\mathrm{gr}_n(M)$; since the ξ_i generate the $\mathrm{gr}(A)$-module $\mathrm{gr}(M)$, there exist $\alpha_i \in \mathrm{gr}(A)$ such that $\xi = \sum_i a_i \xi_i$, and we may assume that $\alpha_i \in \mathrm{gr}_{n-n_i}(A)$ by replacing if need be α_i by its homogeneous component of degree $n - n_i$. Then α_i the image of an element $a_i \in A_{n-n_i}$ and the family (a_i) has the required property. □

Corollary 11.3.34. *Let A be a complete filtered ring and M a filtered A-module whose filtration is exhaustive and separated. If $\mathrm{gr}(M)$ is a finitely generated (resp. Noetherian) $\mathrm{gr}(A)$-module, then M is a finitely generated (resp. Noetherian) A-module.*

Proof. If $\mathrm{gr}(M)$ is finitely generated, there is a finite system of homogeneous generators and Proposition 11.3.33 shows that M is finitely generated. Suppose now that $\mathrm{gr}(M)$ is Noetherian and let N be a submodule of M; the filtration induced on N by that on M is exhaustive and separated and $\mathrm{gr}(N)$ is identified with a sub-$\mathrm{gr}(A)$-module of $\mathrm{gr}(M)$ by Proposition 11.2.14 and hence is finitely generated by hypothesis; we conclude that N is a finitely generated A-module and hence M is Noetherian. □

Corollary 11.3.35. *Let A be a complete Hausdorff filtered ring whose filtration is exhaustive. If* $\mathrm{gr}(A)$ *is Noetherian, so is A.*

Corollary 11.3.36. *Let A be a complete filtered ring, (A_n) its filtration, M a Hausdorff filtered A-module, (E_n) its filtration and N a finitely generated submodule of M; suppose that $A_0 = A$ and $M_0 = M$.*

(a) If for all $n \in \mathbb{Z}$ we have $M_n = M_{n+1} + A_n N$, then $M = N$.

(b) If the filtration on M is derived from that on A, the relation $M = M_1 + N$ implies $M = N$.

Proof. Let $\xi_1, \dots, \xi_s$ be the classes mod M_1 of a finite system of generators of N. It follows from the given hypothesis that for all $n \geq 0$ every element of $\mathrm{gr}_n(M)$ can be expressed in the form $\sum_{i=1}^{s} \alpha_i \xi_i$, where $\alpha_i \in \mathrm{gr}(A)$; the ξ_i therefore generate the $\mathrm{gr}(A)$-module $\mathrm{gr}(M)$, which proves (a) by virtue of Proposition 11.3.33. If the filtration on M is derived from that on A, the relation $M = M_1 + N$ implies

$$M_n = A_n M = A_n M_1 + A_n N = A_n A_1 M + A_n N \subseteq A_{n+1} M + A_n N = M_{n+1} + A_n N \subseteq M_n$$

whence (b). □

Proposition 11.3.37. *Let A be a filtered ring and (A_n) its filtration. Suppose that there exist a subring C of A_0 such that $C \cap A_1 = \{0\}$ and C is identified with a subring of* $\mathrm{gr}_0(A)$. *Let $(x_1, \dots, x_r)$ be a family of element of A with $x_i \in A_{n_i}$ and let ξ_i be the class of x_i in* $\mathrm{gr}_{n_i}(A)$.

(a) If the family (ξ_i) of elements of $\mathrm{gr}(A)$ *is algebraically independent over C, then the family (x_i) is algebraically independent over C.*

(b) If the filtration on A is exhaustive and discrete and (ξ_i) is a system of generators of the C-algebra $\mathrm{gr}(A)$, *then (x_i) is a system of generators of the C-algebra A.*

Proof. Let B be the polynomial algebra $C[X_1, \dots, X_r]$ over C and give B the graduation (B_n) of type $\mathbb{Z}$ where B_n is the set of C-linear combinations of the monomials $X_1^{s_1}, \dots, X_r^{s_r}$ such that $\sum_i n_i s_i = n$. Let ϕ be the homomorphism $f \mapsto f(x_1, \dots, x_r)$ from the C-algebra B to the C-algebra A. By definition, $\phi(B_n) \subseteq A_n$ for all $n \in \mathbb{Z}$ and hence ϕ is compatible with the filtrations. The hypothesis of (a) means that $\mathrm{gr}(\phi)$ is injective. As the filtration on B is exhaustive and separated, Corollary 11.3.30 may be applied and ϕ is injective, which proves the conclusion of (a). Similarly, the hypothesis (b) on the (ξ_i) means that $\mathrm{gr}(\phi)$ is surjective. As A is discrete and its filtration is exhaustive, Theorem 11.3.29 may be applied and ϕ is surjective, which proves the conclusion of (b). □

Proposition 11.3.38. *Let A be a complete Hausdorff filtered ring and (A_n) its filtration. Suppose that there exist a subring C of A_0 such that $C \cap A_1 = \{0\}$ and C is identified with a subring of* $\mathrm{gr}_0(A)$. *Let $(x_1, \dots, x_r)$ be a family of element of A with $x_i \in A_{n_i}$ and let ξ_i be the class of x_i in* $\mathrm{gr}_{n_i}(A)$.

(a) There exists a unique C-homomorphism ρ from $B = C[\![X_1, \dots, X_r]\!]$ to A such that $\rho(X_i) = x_i$.

(b) If the family (x_i) is algebraically independent over C, the homomorphism ρ is injective.

(c) If the filtration on A is exhaustive and (ξ_i) is a system of generators of the C-algebra $\mathrm{gr}(A)$, *then ρ is surjective.*

Proof. As $n_i \geq 1$ for all i, we have $\sum_i n_i s_i \geq \sum_i s_i$ for every monomial $X_1^{s_1}, \dots, X_r^{s_r}$ and on the other hand $\sum_i n_i s_i \leq N$ if N is the greatest of the n_i. If B_n denotes the set of formal power series whose non-zero terms $a_s X^s$ satisfy $\sum_i n_i s_i \leq n$, it follows from Corollary 11.3.13 that B is Hausdorff and complete with the exhaustive filtration (B_n) and that $B' = C[X_1, \dots, X_r]$ is dense in B. Moreover the homomorphism ϕ defined in the proof of Proposition 11.3.37 is continuum on B' and can be extended uniquely to a continuous homomorphism $\rho : B \to A$, since A is Hausdorff and complete, which proves (a). Also, $\mathrm{gr}(B) = \mathrm{gr}(B')$ and $\mathrm{gr}(v) = \mathrm{gr}(\phi)$, so (b) and (c) follow respectively from Corollary 11.3.30 and Theorem 11.3.29 in view Of the hypotheses on A. □

Let A be a local ring, $\mathfrak{m}$ its maximal ideal and M an A-module; let A and M be given the $\mathfrak{m}$-adic filtrations and let $\mathrm{gr}(A)$ and $\mathrm{gr}(M)$ be the graded ring and the graded $\mathrm{gr}(A)$-module associated with A and M. We have seen (Example 11.2.10) that the canonical mapping (2.2.2) is always surjective; we are going to consider the following property of M:

(GR) The canonical map $\gamma_M : \mathrm{gr}(A) \otimes_{\mathrm{gr}_0(A)} \mathrm{gr}_0(M) \to \mathrm{gr}(M)$ is bijective.

Proposition 11.3.39. *Let A be a local ring, $\mathfrak{m}$ its maximal ideal, M, N two A-modules and $\phi : N \to M$ an A-homomorphism. Suppose that M and N are given the $\mathfrak{m}$-adic filtrations and*

(a) M satisfies property (GR);

(b) $\mathrm{gr}_0(\phi) : \mathrm{gr}_0(N) \to \mathrm{gr}_0(M)$ is injective.

Then $\mathrm{gr}(\phi) : \mathrm{gr}(N) \to \mathrm{gr}(M)$ is injective and N and $P = \operatorname{coker} \phi$ satisfy property (GR).

Proof. It is immediately verified that the diagram

$$\begin{tikzcd}
\mathrm{gr}(A) \otimes_{\mathrm{gr}_0(A)} \mathrm{gr}_0(N) \arrow[r, "1\otimes \mathrm{gr}_0(\phi)"] \arrow[d, "\gamma_N"] & \mathrm{gr}(A) \otimes_{\mathrm{gr}_0(A)} \mathrm{gr}_0(M) \arrow[d, "\gamma_M"] \\
\mathrm{gr}(N) \arrow[r, "\mathrm{gr}(\phi)"] & \mathrm{gr}(M)
\end{tikzcd}$$

is commutative. As $\mathrm{gr}_0(A) = A/\mathfrak{m}$ is a field, the hypothesis implies that $1 \otimes \mathrm{gr}_0(\phi)$ is injective; as by hypothesis γ_M is injective, so is $\gamma_M \circ (1 \otimes \mathrm{gr}_0(\phi))$. This implies first that γ_N is injective and hence bijective and therefore that $\mathrm{gr}(\phi)$ is injective. The formula $\phi^{-1}(\mathfrak{m}^n M) = \mathfrak{m}^n N$ is then a consequence of Theorem 11.3.29(a).

Also, let us write $N' = \phi(N)$ and let $\iota : N' \to M$ be the canonical injection. If $\pi : M \to P = M/N'$ is the canonical homomorphism, then in the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{gr}(A) \otimes_{\mathrm{gr}_0(A)} \mathrm{gr}_0(N') \arrow[r] \arrow[d, "\gamma_{N'}"] & \mathrm{gr}(A) \otimes_{\mathrm{gr}_0(A)} \mathrm{gr}_0(M) \arrow[r] \arrow[d, "\gamma_M"] & \mathrm{gr}(A) \otimes_{\mathrm{gr}_0(A)} \mathrm{gr}(P) \arrow[r] \arrow[d, "\gamma_P"] & 0 \\
0 \arrow[r] & \mathrm{gr}(N) \arrow[r, "\mathrm{gr}(\iota)"] & \mathrm{gr}(M) \arrow[r, "\mathrm{gr}(\pi)"] & \mathrm{gr}(P) \arrow[r] & 0
\end{tikzcd}$$

the lower row is exact by Proposition 11.2.14 and so is the upper row by virtue of Proposition 11.2.14 and the fact that $\mathrm{gr}_0(A)$ is a field. The first part of the argument applied to ι shows that $\gamma_{N'}$ is bijective; as γ_M is also bijective by hypothesis, we conclude that γ_P is bijective by the snake lemma. □

Corollary 11.3.40. *Under the hypotheses of Proposition 11.3.39, if we assume also that N is Hausdorff with the $\mathfrak{m}$-adic filtration, then ϕ is injective.*

Proposition 11.3.41. *Let A be a ring, $\mathfrak{m}$ an ideal of A contained in the Jacobson radical of A and M an A-module. Let A and M be given the $\mathfrak{m}$-adic filtrations. Suppose that one of the following conditions holds:*

(a) M is a finitely generated A-module and A is Hausdorff.

(b) $\mathfrak{m}$ is nilpotent.

Then for M to be a free A-module, it is necessary and suffcient that $M/\mathfrak{m}M$ be a free $(A/\mathfrak{m})$-module and that M satisfies property (GR).

Proof. If M is a free A-module and (x_λ) a basis of M, $\mathfrak{m}^n M$ is the direct sum of the submodules $\mathfrak{m}^n x_\lambda$ of M for all $n \geq 0$; then $\mathfrak{m}^n M/\mathfrak{m}^{n+1}M$ is identified with the direct sum of the $\mathfrak{m}^n x_\lambda/\mathfrak{m}^{n+1}x_\lambda$. We deduce first (for $n = 0$) that the classes $1 \otimes x_\lambda$ of the x_λ in $M/\mathfrak{m}M = (A/\mathfrak{m}) \otimes_A M$ form a basis of the $(A/\mathfrak{m})$-module $M/\mathfrak{m}E$, since the canonical mapping

$$(\mathfrak{m}^n/\mathfrak{m}^{n+1}) \otimes_A (M/\mathfrak{m}M) \longrightarrow \mathfrak{m}^n M/\mathfrak{m}^{n+1}M$$

is bijective for all $n \geq 0$; hence γ_M is bijective. Note that this part of the proof uses neither condition (a) nor condition (b).

Suppose conversely that the conditions of the statement hold and let $(x_\lambda)_{\lambda \in I}$ be a family of elements of M whose classes mod $\mathfrak{m}M$ form a basis of the $(A/\mathfrak{m})$-module $M/\mathfrak{m}M$; let L be the free A-module $A^{\oplus I}$ and (e_λ) a basis of L; let $\phi : L \longrightarrow M$ the A-linear mapping such that $\phi(e_\lambda) = x_\lambda$ for all $\lambda \in I$. Now, each of the hypotheses (a) and (b) implies that A is Hausdorff and hence so is L with the $\mathfrak{m}$-adic filtration, since $\mathfrak{m}^n L = (\mathfrak{m}^n)^{\oplus I}$. Also, since $\mathrm{gr}(L)$ is identified with $\mathrm{gr}(A) \otimes_{A/\mathfrak{m}} (L/\mathfrak{m}L)$ from the first part of the proof, it is possible to write $\mathrm{gr}(\phi)$ as

$$\mathrm{gr}(L) \xrightarrow{\cong} \mathrm{gr}(A) \otimes_{A/\mathfrak{m}} (L/\mathfrak{m}L) \xrightarrow{\eta} \mathrm{gr}(A) \otimes_{A/\mathfrak{m}} (M/\mathfrak{m}M) \xrightarrow{\gamma_M} \mathrm{gr}(M)$$

where η is the bijection mapping the class $1 \otimes \bar{e}_\lambda$ onto $1 \otimes \bar{x}_\lambda$. The hypothesis then implies that $\mathrm{gr}(\phi)$ is bijective and the conclusion follows with the aid of Corollary 11.3.30, Proposition 7.1.5 and Corollary 11.3.31. □

Recall that we have already seen that if A is a ring and $\mathfrak{a}$ is an ideal of A such that A is Hausdorff and complete with the $\mathfrak{a}$-adic topology, then the topological ring A is cannically identified with the inverse limit of the discrete rings $A_i = A/\mathfrak{a}^{i+1}$ $(i \in \mathbb{N})$ with respect to the canonical homomorphisms

$$\pi_{ij} : A/\mathfrak{a}^{j+1} \longrightarrow A/\mathfrak{a}^{i+1}$$

for $i \leq j$; note that π_{ij} is surjective and if $\mathfrak{n}_{ij}$ is its kernel, then

$$\mathfrak{n}_{ij} = \mathfrak{a}^{i+1}/\mathfrak{a}^{j+1} = (\mathfrak{a}/\mathfrak{a}^{j+1})^{i+1} = (\mathfrak{n}_{0,j})^{i+1};$$

in particular $(\mathfrak{n}_{0,j})^{j+1} = 0$. Conversely, we have the following result:

Proposition 11.3.42. *Let (A_i, π_{ij}) be an inverse system of discrete rings with index set $\mathbb{N}$ and let (M_i, u_{ij}) be an inverse system of modules over the inverse system of rings (A_i, π_{ij}). Let $\mathfrak{n}_j$ be the kernel of $\pi_{0,j} : A_j \longrightarrow A_0$ and set $A = \varprojlim A_i$, $M = \varprojlim M_i$. Suppose that*

(a) for all $i \in \mathbb{N}$, π_{ii} is the identity on A_i and for $i \leq j$, π_{ij} and u_{ij} are surjective;

(b) for $i \leq j$, the kernel of π_{ij} and u_{ij} are $\mathfrak{n}_j^{i+1}$ and $\mathfrak{n}_j^{i+1}M_j$, respectively.

Then the following assertions hold:

(i) A is a complete Hausdorff topological ring, M is a complete topological A-module and the cannical homomorphisms $\pi : A \to A_i$, $u_i : M \to M_i$ are surjective.

(ii) If M_0 is a finitely generated A_0-module, then M is a finitely generated A-module; to be precise, every finite subset E of M such that $u_0(E)$ generates M_0 is a system of generators of M.

Proof. The first assertion (i) follows from Corollary 2.2.21 and Corollary 2.2.24. For each $i \in \mathbb{N}$, let $\mathfrak{m}_{i+1} = \ker \pi_i$, $N_{i+1} = \ker u_i$; then by hypothesis (b),

$$\mathfrak{m}_{i+1} = \varprojlim_k \pi_{i,i+k}^{-1}(0) = \varprojlim_k \mathfrak{n}_{i+1}^{i+k}, \quad N_{i+1} = \varprojlim_k u_{i,i+k}^{-1}(0) = \varprojlim_k \mathfrak{n}_{i+k}^{i+1}M_{i+k};$$

and as π_{i+k} and u_{i+k} are surjective, we also have

$$\pi_{i+k}(\mathfrak{m}_{i+1}) = \mathfrak{n}_{i+k}^{i+1}, \quad u_{i+k}(N_{i+1}) = \mathfrak{n}_{i+k}^{i+1}M_{i+k}. \tag{3.3.1}$$

We prove that $\mathfrak{m}_i N_j \subseteq N_{i+j}$ for $i, j \geq 1$, which amounts to showing that $u_{i+j-1}(\mathfrak{m}_i N_j) = 0$. For this, note that $\mathfrak{n}_k^{k+1} = 0$ for $k \geq 0$ as it is the kernel of $\pi_{kk} = \mathrm{id}$, so

$$u_{i+j-1}(\mathfrak{m}_i N_j) = \pi_{i+j-1}(\mathfrak{m}_i)u_{i+j-1}(N_j) = \mathfrak{n}_{i+j-1}^{i}(\mathfrak{n}_{i+j-1}^{j}M_{i+j-1}) = 0;$$

we see similarly that $\mathfrak{m}_i\mathfrak{m}_j \subseteq \mathfrak{m}_{i+j}$. If for $i \leq 0$ we set $\mathfrak{m}_i = A$ and $N_i = M$, then $(\mathfrak{m}_i)_{i\in\mathbb{Z}}$ is a filtration of A and $(N_i)_{i\in\mathbb{Z}}$ is a filtration of M compatible with that of A. The topology on A and M are obviously those defined by these filtrations. Now let $\mathfrak{a}$ be an ideal of A such that $\pi_1(\mathfrak{a}) = \mathfrak{n}_1$ and M' be the submodule of M generated by a subset E of M such that $u_0(E)$ generates M_0; we are going to show that

$$N_i = \mathfrak{a}^i M' + N_{i+1} \quad \text{for} \quad i \geq 0. \tag{3.3.2}$$

Let us write $\mathfrak{a}_i = \pi_i(\mathfrak{a})$ and $M'_i = u_i(M')$; from the definition of N_{i+1}, it then suffices to show that

$$u_i(N_i) = \mathfrak{a}_i^i M'_i.$$

This is true if $i = 0$, since $N_0 = M$ and $M'_0 = M_0$ by hypothesis. If $i \geq 1$, then $u_i(N_i) = \mathfrak{n}_i^i M_i$ by (3.3.1). As $\pi_{1,i}$ is surjective and $\pi_{0,i} = \pi_{0,1} \circ \pi_{1,i}$, $\pi_{1,i}$ maps the kernel $\mathfrak{n}_i$ of $h_{0,i}$ onto the kernel of $h_{0,1}$ and $\mathfrak{n}_i = \pi_{1,i}^{-1}(\mathfrak{n}_1)$, so

$$\pi_{1,i}(\mathfrak{a}_i) = \pi_1(\mathfrak{a}) = \mathfrak{n}_1 = \pi_{1,i}(\mathfrak{n}_i);$$

as the kernel of $\pi_{1,i}$ is $\mathfrak{n}_i^2$, we conclude that $\mathfrak{a}_i \subseteq \mathfrak{n}_i \subseteq \mathfrak{a}_i + \mathfrak{n}_i^2$, whence $\mathfrak{n}_i = \mathfrak{a}_i + \mathfrak{n}_i^2$. Moreover $u_{0,i}(M'_i) = u_0(M') = M_0 = u_{0,i}(M_i)$ and as $\ker u_{0,i} = \mathfrak{n}_i M_i$, $M_i = M'_i + \mathfrak{n}_i M_i$, so

$$\mathfrak{n}_i M_i = (\mathfrak{a}_i + \mathfrak{n}_i^2)^i (M'_i + \mathfrak{n}_i M_i).$$

Now $\mathfrak{a}_i^k \mathfrak{n}_i^{i+1-k} \subseteq \mathfrak{n}_i^{i+1} = 0$ for $0 \leq k \leq i$, so it follows that $u_i(N_i) = \mathfrak{n}_i M_i = \mathfrak{a}_i^i M'_i$, which proves (3.3.2). Moreover, $\mathfrak{m}_1 = \pi_1^{-1}(\mathfrak{n}_1)$, so $\mathfrak{a} \subseteq \mathfrak{m}_1$ and therefore $\mathfrak{a}^i \subseteq \mathfrak{m}_1^i \subseteq \mathfrak{m}_i$, whence

$N_i \subseteq \mathfrak{m}_i M' + N_{i+1}$. On the other hand, obviously $\mathfrak{m}_i M \subseteq N_i$ and so $N_i = \mathfrak{m}_i M' + N_{i+1}$ for $i \geq 0$; it then follows from Corollary 11.3.36 that $M' = M$, which completes the proof. □

11.4 The adic topology on Noetherian rings

Let A be a filtered ring, M a filtered A-module and (A_n) and (M_n) be the corresponding filtrations. Since we only consider the $\mathfrak{a}$-adic filtration, we may assume that all filtrations are exhaustive and consist of submodules. The **Rees ring** of A is then defined by

$$\mathrm{Rees}(A) = \bigoplus_{n \geq 0} A_n X^n \subseteq A[X]$$

and the **Rees mudule** of M is defined by

$$\mathrm{Rees}(M) = \bigoplus_{n \geq 0} M_n \otimes_A AX^n \subseteq M \otimes_A A[X].$$

Note that $\mathrm{Rees}(M)$ is a graded $\mathrm{Rees}(A)$-module of type $\mathbb{N}$, since we have

$$A_m X^m (M_n \otimes_A AX^n) \subseteq (A_m M_n \otimes_A AX^{m+n}) \subseteq M_{m+n} \otimes_A AX^{m+n}.$$

The most important case is that $\mathfrak{a}$ is an ideal of A and A, M are given the $\mathfrak{a}$-adic filtration. In this case we write $\mathrm{Rees}_{\mathfrak{a}}(A)$ for the Rees ring $\bigoplus_{n \geq 0} \mathfrak{a}^n X^n$ and $\mathrm{Rees}_{\mathfrak{a}}(M)$ for $\bigoplus_{n \geq 0} \mathfrak{a}^n M \otimes_A AX^n$.

11.4.1 Good filtrations

Let A be a ring, $\mathfrak{a}$ an ideal of A, M an A-module and (M_n) a filtration on the additive group M consisting of submodules of M. The filtrations (M_n) is called **$\mathfrak{a}$-good** if:

(a) $\mathfrak{a} M_n \subseteq M_{n+1}$ for all $n \in \mathbb{Z}$.

(b) There exists an integer n_0 such that $\mathfrak{a} M_n = M_{n+1}$ for all $n \geq n_0$.

If (M_n) is $\mathfrak{a}$-good, then by induction on we see $\mathfrak{a}^p M_n = M_{n+p}$ for all $n \geq n_0$ and $p > 0$. Note that condition (a) means that the filtration (M_n) is compatible with the A-module structure on M if A is given the $\mathfrak{a}$-adic filtration. Clearly, on every A-module M, the $\mathfrak{a}$-adic filtration is $\mathfrak{a}$-good.

Theorem 11.4.1. *Let A be a ring, $\mathfrak{a}$ an ideal of A, and give A the $\mathfrak{a}$-adic filtration. Let M be an A-module and (M_n) a filtration of M consisting of finitely generated submodules. Suppose that $\mathfrak{a} M_n \subseteq M_{n+1}$ for all n. Then the two following conditions are equivalent:*

(a) The filtration (M_n) is $\mathfrak{a}$-good.

(b) $\mathrm{Rees}_{\mathfrak{a}}(M)$ is a finitely generated $\mathrm{Rees}_{\mathfrak{a}}(A)$-module.

Proof. Suppose that $\mathfrak{a} M_n = M_{n+1}$ for $n \geq n_0 \geq 0$. For $i \leq n_0$, let $(e_{ij})_{1 \leq j \leq r_i}$ be a finite system of generators of the A-module M_i. As the A-module $M_n \otimes_A AX^n$ is generated by the elements $e_{nj} \otimes X^n$ for $0 \leq n \leq n_0$ and is equal to

$$\mathfrak{a}^{n-n_0} M_{n_0} \otimes_A AX^n$$

for $n > n_0$, the Rees(A)-module Rees(M) is generated by the elements $e_{nj} \otimes X^n$ for $0 \leq n \leq n_0$ and $1 \leq j \leq r_n$; then it is certainly finitely generated.

Conversely, if Rees(M) is a finitely generated Rees(A)-module, it is generated by a finite family of elements of the form $e_k \otimes X^{n_k}$, where $e_k \in M_{n_k}$. Let n_0 be the greatest of the integers n_k. Then for $n \geq n_0$ and $x \in M_n$,

$$x \otimes X^n = \sum_k t_k(e_k \otimes X^{n_k})$$

where $t_k \in$ Rees(A); replacing if need be to by its homogeneous component of degree $n - n_k$, we may assume that $t_k = a_k X^{n-n_k}$ where $a_k \in \mathfrak{a}^{n-n_k}$. As the unique element X^n forms a basis of the A-module AX^n, the equation $x \otimes X^n = (\sum_k a_k e_k) \otimes X^n$ implies $x = \sum_k a_k e_k$. Then $M_n \subseteq \mathfrak{a}^{n-n_0} M_{n_0}$; since the opposite inclusion is obvious by hypothesis, we see $M_n = \mathfrak{a}^{n-n_0} M_{n_0}$, whence $\mathfrak{a}M_n = M_{n+1}$ for $n \geq n_0$. □

Lemma 11.4.2. *Let A be a Noetherian ring and $\mathfrak{a}$ an ideal of A. Then the subring* $\mathrm{Rees}_{\mathfrak{a}}(A)$ *of $A[X]$ is Noetherian.*

Proof. Note that $\mathrm{Rees}_{\mathfrak{a}}(A)$ is an A-algebra generated by $\mathfrak{a}X$; as A is Noetherian, $\mathfrak{a}X$ is a finitely generated A-module, so the claim follows from Hilbert basis theorem. □

Proposition 11.4.3. *Let A be a filtered ring, $\mathfrak{a}$ an ideal of A, and M is an A-module with a $\mathfrak{a}$-good filtration. If N is a submodule of M then the quotient filtration on M/N is $\mathfrak{a}$-good. If further A is Noetherian, then the submodule filtration on N is $\mathfrak{a}$-good.*

Proof. If N and M/N have the submodule (resp. quotient) filtrations respectively, then $\mathrm{Rees}_{\mathfrak{a}}(N)$ is a $\mathrm{Rees}_{\mathfrak{a}}(A)$-submodule of $\mathrm{Rees}_{\mathfrak{a}}(M)$ and we have $\mathrm{Rees}_{\mathfrak{a}}(M/N) \cong \mathrm{Rees}_{\mathfrak{a}}(M)/\mathrm{Rees}_{\mathfrak{a}}(N)$ as $\mathrm{Rees}_{\mathfrak{a}}(A)$-modules. Since the filtration on M is $\mathfrak{a}$-good, $\mathrm{Rees}_{\mathfrak{a}}(M)$ is a finitely generated $\mathrm{Rees}_{\mathfrak{a}}(A)$-module and so $\mathrm{Rees}_{\mathfrak{a}}(M/N)$ is finitely generated, which implies the filtration on M/N is $\mathfrak{a}$-good. If further A is Noetherian then $\mathrm{Rees}_{\mathfrak{a}}(A)$ is Noetherian, and so $\mathrm{Rees}_{\mathfrak{a}}(N)$ is finitely generated. It then follows that the filtration on N is $\mathfrak{a}$-good. □

Corollary 11.4.4 (Artin-Rees Lemma). *Let A be a Noetherian ring, $\mathfrak{a}$ an ideal of A, M a finitely generated A-module and N a submodule of M. The filtration induced on N by the $\mathfrak{a}$-adic filtration on M is $\mathfrak{a}$-good. In other words, there exists an integer n_0 such that for $n \geq n_0$ we have*

$$\mathfrak{a}(\mathfrak{a}^n M \cap N) = \mathfrak{a}^{n+1} M \cap N.$$

Corollary 11.4.5. *Let A be a Noetherian ring and $\mathfrak{a}$, $\mathfrak{b}$ two ideals of A. Then there exists an integer $n > 0$ such that $\mathfrak{a}^n \cap \mathfrak{b} \subseteq \mathfrak{a}\mathfrak{b}$.*

Proof. By the Artin-Rees Lemma, there exist $n > 0$ such that $\mathfrak{a}^{n+1} \cap \mathfrak{b} = \mathfrak{a}(\mathfrak{a}^n \cap \mathfrak{b}) \subseteq \mathfrak{a}\mathfrak{b}$. □

Corollary 11.4.6. *Let A be a Noetherian ring, $\mathfrak{a}$ an ideal of A and x an element of A which is not a divisor of* 0*. There exists an integer $n_0 > 0$ such that, for all $n \geq n_0$, we have $(\mathfrak{a}^n : x) \subseteq \mathfrak{a}^{n-n_0}$.*

Proof. Corollary 1 applied to $M = A$, $N = Ax$ shows that there exists n_0 such that, for all $n \geq n_0$, $\mathfrak{a}^n \cap Ax = \mathfrak{a}^{n-n_0}(\mathfrak{a}^{n_0} \cap Ax)$. Then, if $xy \in \mathfrak{a}^n$,

$$xy \in \mathfrak{a}^n \cap Ax \subseteq \mathfrak{a}^{n-n_0} x$$

and, as x is not a divisor of 0, we deduce that $y \in \mathfrak{a}^{n-n_0}$. □

Corollary 11.4.7. *Let A be a Noetherian ring, $\mathfrak{a}$ an ideal of A, M a finitely generated A-module and (M_n) and (M'_n) two filtrations consisting of submodules of M. Suppose that the filtrations (M_n) and (M'_n) are compatible with the A-module structure on M when A is given the $\mathfrak{a}$-adic filtration. If the filtration (M_n) is $\mathfrak{a}$-good and $M'_n \subseteq M_n$ for all $n \in \mathbb{Z}$, then the filtration (M'_n) is $\mathfrak{a}$-good.*

Proof. This is a special case of Proposition 11.4.3. □

Lemma 11.4.8. *Let A, B be two Noetherian rings, $\rho : A \to B$ a ring homomorphism, M a finitely generated A-module and N a finitely generated B-module. Then $\mathrm{Hom}_A(M, N)$ is a finitely generated B-module.*

Proof. There exists by hypothesis a surjective A-homomorphism $\eta : A^n \to M$; the mapping $\phi \mapsto \phi \circ \eta$ of $\mathrm{Hom}_A(M, N)$ to $\mathrm{Hom}_A(A^n, N)$ is therefore injective and, as B is Noetherian, it is sufiicient to prove that $\mathrm{Hom}_A(A^n, N)$ is a finitely generated B-module; which 1s immediate since it is isomorphic to N^n. □

Proposition 11.4.9. *Let A be a Noetherian ring, $\mathfrak{a}$ an ideal of A and M, N two finitely generated A-modules. If (N_n) is an $\mathfrak{a}$-good filtration on N, the submodules $\mathrm{Hom}_A(E, N_n)$ form an $\mathfrak{a}$-good filtration on the A-module $\mathrm{Hom}_A(M, N)$.*

Proof. As $\mathfrak{a}^k N_n \subseteq N_{n+k}$ for $n \in \mathbb{Z}$ and $k \geq 0$, it is also true that

$$\mathfrak{a}^k \mathrm{Hom}_A(M, N_n) \subseteq \mathrm{Hom}_A(M, N_{n+k})$$

the family $(\mathrm{Hom}_A(M, N_n))$ is then a filtration on $\mathrm{Hom}_A(M, N)$ compatible with its module structure over the ring A filtered by the $\mathfrak{a}$-adic filtration. Since M is finitely generated, there exists an integer $r > 0$ and a surjective A-homomorphism $\eta : A^r \to M$ which defines an injective A-homomorphism

$$\eta^* : \mathrm{Hom}_A(M, N) \to \mathrm{Hom}_A(A^r, N)$$

clearly η^* is compatible with the filtrations $(\mathrm{Hom}_A(M, N))$ and $(\mathrm{Hom}_A(A^r, N))$. As the A-modules $\mathrm{Hom}_A(M, N)$ and $\mathrm{Hom}_A(A^r, N)$ are finitely generated (Lemma 11.4.8), it is sufficient by virtue of Proposition 11.4.3 to show that the filtration $(\mathrm{Hom}_A(A^r, N))$ is $\mathfrak{a}$-good; but this is immediate by virtue of the existence of the canonical isomorphism $\mathrm{Hom}_A(A^r, N) \to N^r$, and the fact that the relation $\mathfrak{a}N = N_{n+1}$ implies $\mathfrak{a}(N_n^r) = (\mathfrak{a}N_n)^r = N_{n+1}^r$. □

Proposition 11.4.10. *Let A be a Noetherian ring and $\mathfrak{a}$ an ideal of A such that A is Hausdorff and complete with respect to the $\mathfrak{a}$-adic topology. Let M be a filtered A-module over the filtered ring A, the filtration (M_n) of A being such that $M_0 = M$ and M is Hausdorff with respect to the topology defined by (M_n). Then the following conditions are equivalent:*

(i) *M is a finitely generated A-module and (M_n) is an $\mathfrak{a}$-good filtration.*

(ii) *$\mathrm{gr}(M)$ is a finitely generated $\mathrm{gr}(A)$-module.*

(iii) *$\mathrm{gr}_n(M)$ is a finitely generated A-module for all n and there exists n_0 such that for $n \geq n_0$ the canonical homomorphism $\mathrm{gr}_1(A) \otimes_A \mathrm{gr}_n(M) \to \mathrm{gr}_{n+1}(M)$ is surjective.*

Proof. It follows immediately from the definitions that (i) implies (iii). Also, (ii) is equivalent to (iii): the fact that (ii) implies (iii) is a consequence of Corollary 11.1.37; conversely, if (iii) holds, clearly $\mathrm{gr}(M)$ is generated as a $\mathrm{gr}(A)$-module by the sum of the $\mathrm{gr}_p(M)$ for $p \leq n_0$ and hence by hypothesis admits a finite system of generators. It remains to prove that (iii) implies (i).

Assume (iii), as the $\mathrm{gr}_n(M)$ are finitely generated and $M_0 = M$, clearly first, by induction on n, M/M_n is a finitely generated A-module for all n; it will therefore be sufficient to prove that, for $n > n_0$, M_n is a finitely generated A-module and that $\mathfrak{a}M_n = M_{n+1}$. Now, consider the A-module M_{n+1} with the exhaustive and separated filtration $(M_{n+k})_{k\geq 1}$. Now since $\mathrm{gr}_1(A) = \mathfrak{a}/\mathfrak{a}^2$, hypothesis (iii) implies that the image of $\mathfrak{a}M_n$ in $\mathrm{gr}_{n+1}(M)$ is equal to $\mathrm{gr}_{n+1}(M)$ and generates the graded $\mathrm{gr}(A)$-module $\mathrm{gr}(M_{n+1})$. As $\mathrm{gr}_{n+1}(M)$ is by hypothesis a finitely generated A-module, it follows from Proposition 11.3.33 that $\mathfrak{a}M_n = M_{n+1}$ and that M_{n+1} is a finitely generated A-module. □

Remark 11.4.1. Note that in the proof of Proposition 11.4.10, only the implication $(iii) \Rightarrow (i)$ uses the hypothesis A is $\mathfrak{a}$-adic complete and Hausdorff. In particular, we see if A is Noetherian and the filtration (M_n) is $\mathfrak{a}$-good then $\mathrm{gr}(M)$ is a finitely generated $\mathrm{gr}(A)$-module.

11.4.2 The adic topology on Noetherian rings

Proposition 11.4.11. *Let A be a Noetherian ring, $\mathfrak{a}$ an ideal of A and M a finitely generated A-module. All the $\mathfrak{a}$-good filtrations on M define the same topology on M, namely the $\mathfrak{a}$-adic topology.*

Proof. Let (M_n) be an $\mathfrak{a}$-good filtration on M. As this filtration is exhaustive, every element of M belongs to one of the M_n and, as M is finitely generated (hence Noetherian) and the M_n are A-modules, there exists an integer n_1 such that $M_{n_1} = M$. On the other hand let n_0 be such that $\mathfrak{a}M_n = M_{n+1}$ for $n \geq n_0$; then, for $n > n_0 - n_1$,

$$\mathfrak{a}^n M \subseteq M_{n+n_1} = \mathfrak{a}^{n+n_1-n_0} M_{n_0} \subseteq \mathfrak{a}^{n+n_1-n_0} M,$$

which proves the proposition. □

Theorem 11.4.12 (Krull). *Let A be a Noetherian ring, $\mathfrak{a}$ an ideal of A, M a finitely generated A-module and N a submodule of M. Then the $\mathfrak{a}$-adic topology on N is induced by the $\mathfrak{a}$-adic topology on M.*

Proof. It follows from Artin-Rees Lemma that the filtration induced on N by the $\mathfrak{a}$-adic filtration on M is $\mathfrak{a}$-good and the conclusion then follows from Proposition 11.4.11. □

Corollary 11.4.13. *Let A be a Noetherian ring, $\mathfrak{a}$ an ideal of A, M an A-module and N a finitely generated A-module. Then every homomorphism $\phi : M \to N$ is a strict morphism for the $\mathfrak{a}$-adic topologies.*

Proof. As $\phi(\mathfrak{a}^n M) = \mathfrak{a}^n \phi(M)$, ϕ is a strict morphism of M onto $\phi(M)$ for the $\mathfrak{a}$-adic topologies on these two modules and the $\mathfrak{a}$-adic topology on $\phi(M)$ is induced by the $\mathfrak{a}$-adic topology on N by Theorem 11.4.12, hence the claim. □

Corollary 11.4.14. *Let $0 \to M_1 \to M_2 \to M_3 \to 0$ be an exact sequence of finitely-generated modules over a Noetherian ring A. Let $\mathfrak{a}$ be an ideal of A, then the sequence of $\mathfrak{a}$-adic completions*

$$0 \longrightarrow \widehat{M}_1 \longrightarrow \widehat{M}_2 \longrightarrow \widehat{M}_3 \longrightarrow 0$$

is exact.

Proposition 11.4.15. *Let A be a Noetherian ring, $\mathfrak{a}$ an ideal of A and M a finitely generated A-module. The closure $\bigcap_{n=0}^{\infty} \mathfrak{a}^n M$ of $\{0\}$ in M with respect to the $\mathfrak{a}$-adic topology is the set of $x \in M$ for which there exists an element $a \in \mathfrak{a}$ such that $(1-a)x = 0$.*

Proof. If $x = ax \bmod \mathfrak{a}$ where $a \in \mathfrak{a}$, then $x = a^n x$ for every integer $n > 0$ and hence $x \in \bigcap_n \mathfrak{a}^n M$. Conversely, if $x \in \bigcap_n \mathfrak{a}^n M$, Ax is contained in the intersection of the neighbourhoods of 0 in M; it then follows from Theorem 11.4.12 that the $\mathfrak{a}$-adic topology on Ax, which is induced by that on M, is the trivial topology; as $\mathfrak{a}x$ is by definition a neighbourhood of 0 with this topology, $\mathfrak{a}x = Ax$ and hence there exists $a \in \mathfrak{a}$ such that $x = ax$. □

Corollary 11.4.16 (Krull's Intersection Theorem). *Let A be a Noetherian ring and $\mathfrak{a}$ an ideal of A. Then the ideal $\bigcap_n \mathfrak{a}^n$ is the set of elements $x \in A$ for which there exists $a \in \mathfrak{a}$ such that $(1-a)x = 0$. In particular, for $\bigcap_n \mathfrak{a}^n = \{0\}$, it is necessary and sufficient that no element of $1 + \mathfrak{a}$ is a divisor of 0 in A.*

Remark 11.4.2. The hypothesis that A is Noetherian is essential in this corollary. For example, let A be the ring of infinitely differentiable mappings from $\mathbb{R}$ to itself and let $\mathfrak{m}$ be the (maximal) ideal of A consisting of the functions f such that $f(0) = 0$. It is immediate that $\bigcap_n \mathfrak{m}^n$ is the set of functions f such that $f^{(n)}(0) = 0$ for all $n \geq 0$ and there exist such functions with $f(x) \neq 0$ for all $x \neq 0$, for example the function f defined by $f(x) = e^{-1/x^2}$ for $x \neq 0$ and $f(0) = 0$. Also, note that for such an f, the elment $1 + f$ is even invertible in A.

11.4.3 The adic completion of a Noetherian ring

Let A be a ring, $\mathfrak{a}$ an ideal of A and M an A-module; let $\widehat{A}$ and $\widehat{M}$ denote the respective Hausdorff completions of A and M with respect to the $\mathfrak{a}$-adic topology and $\iota_M : M \to \widehat{M}$ the canonical mapping. The A-bilinear mapping $(a, x) \mapsto a\iota_M(x)$ of $\widehat{A} \times M$ to $\widehat{M}$ defines a canonical A-linear mapping

$$\alpha_M : \widehat{A} \otimes_A M \to \widehat{M}.$$

Let $\phi : M \to N$ be an A-module homomorphism and let $\hat{\phi} : \widehat{M} \to \widehat{N}$ be the mapping obtained by passing to the Hausdorff completions; for $a \in \widehat{A}$ and $x \in M$,

$$\alpha_N(a \otimes \phi(x)) = a\iota_M(\phi(x)) = a\hat{\phi}(\iota_M(x)) = \hat{\phi}(\alpha_M(a \otimes x)).$$

In other words, the following diagram is commutative:

$$\begin{tikzcd}
\widehat{A} \otimes_A M \arrow[r, "1\otimes\phi"] \arrow[d, "\alpha_M"] & \widehat{A} \otimes N \arrow[d, "\alpha_N"] \\
\widehat{M} \arrow[r, "\hat{\phi}"] & \widehat{N}
\end{tikzcd}$$

Finally, recall that by Proposition 11.3.16, if M is finitely generated then the homomorphism α_M is surjective.

Theorem 11.4.17. *Let A be a Noetherian ring, $\mathfrak{a}$ an ideal of A and M, N, L three finitely generated A-modules. Then*

(a) If $0 \to M \to N \to L \to 0$ is an exact sequence of A-modules, then the sequence

$$0 \longrightarrow \widehat{M} \longrightarrow \widehat{N} \longrightarrow \widehat{L} \longrightarrow 0$$

obtained by passing to the Hausdorff completions (with respect to the $\mathfrak{a}$-adic topologies) is exact.

(b) The canonical $\widehat{A}$-linear mapping $\alpha_M : \widehat{A} \otimes M \to \widehat{M}$ is bijective.

(c) The A-module $\widehat{A}$ is flat.

Proof. We have seen that M and L carry the submodule filtration and quotient filtration, respectively, so claim (a) follows from Lemma 11.3.15. Assertion (b) is obvious when $M = A$ and the case where M is a free finitely generated A-module can be immediately reduced to that. In the general case, M admits a finite presentation

$$0 \longrightarrow N \longrightarrow A^n \longrightarrow M \longrightarrow 0$$

so we derive a commutative diagram

$$\begin{tikzcd}
 & \widehat{A} \otimes_A N \arrow[r] \arrow[d, "\alpha_N"] & \widehat{A} \otimes_A A^n \arrow[r] \arrow[d, "\alpha_{A^n}"] & \widehat{A} \otimes_A M \arrow[r] \arrow[d, "\alpha_M"] & 0 \\
0 \arrow[r] & \widehat{N} \arrow[r] & \widehat{A}^n \arrow[r] & \widehat{M} \arrow[r] & 0
\end{tikzcd}$$

The first row is exact and so is the second by (a). Since A is Noetherian we know that N is also finitely generated, so α_M and α_N are both surjective. Since α_{A^n} is bijective, we then deduce that α_M is injective by the snake lemma.

Then it follows from (a) and (b) that, if $\mathfrak{a}$ is an ideal of A (necessarily finitely generated), the canonical mapping $\widehat{A} \otimes_A \mathfrak{a} \to \widehat{A}$ is injective, being the composition of $\hat{\mathfrak{a}} \to \widehat{A}$ and $\alpha_{\mathfrak{a}}$, which proves that A is a flat A-module. □

Under the conditions of Theorem, $\widehat{A} \otimes_A M$ is often identified with M by means of the canonical mapping α_M. If $\phi : M \to N$ is a homomorphism of finitely generated A-modules, $\hat{\phi} : \widehat{M} \to \widehat{N}$ is then identified with $1 \otimes \phi$ by virtue of the commutativity of diagram.

Corollary 11.4.18. *Let A be a Noetherian ring, $\mathfrak{a}$ an ideal of A and $\widehat{A}$ the Hausdorff completion of A with respect to the $\mathfrak{a}$-adic topology. If an element $a \in A$ is not a divisor of zero in A, its canonical image $\hat{a}$ in A is not a divisor of zero in $\widehat{A}$.*

Proof. This follows from the fact that $\widehat{A}$ is a flat A-module. □

Corollary 11.4.19. *Let A be a Noetherian ring, $\mathfrak{a}$ an ideal of A, M a finitely generated A-module and N and P two submodules of M. With the $\mathfrak{a}$-adic topologies and let ι_M be the canonical mapping from M to $\widehat{M}$, then*

$$\widehat{N} = \widehat{A}\iota_M(N), \quad \widehat{(N+P)} = \widehat{N} + \widehat{P}, \quad \widehat{N \cap P} = \widehat{N} \cap \widehat{P}, \quad \widehat{(N:P)} = (\widehat{N} : \widehat{P}).$$

Moreover, if $\mathfrak{a}$ and $\mathfrak{b}$ are two ideals of A, then $\widehat{\mathfrak{a}\mathfrak{b}} = \hat{\mathfrak{a}}\hat{\mathfrak{b}}$.

Proof. By Theorem 11.4.17, $\widehat{M}, \widehat{N}, \widehat{P}$ are canonically identified with $\widehat{A}\otimes_A M$, $\widehat{A}\otimes_A N$, and $\widehat{A}\otimes_A P$, which establishes the formulas. Finally, as $\hat{\mathfrak{a}} = \widehat{A}\mathfrak{a}$, $\hat{\mathfrak{b}} = \widehat{A}\mathfrak{b}$, we see

$$\widehat{\mathfrak{a}\mathfrak{b}} = \widehat{A}\mathfrak{a}\mathfrak{b} = \widehat{A}\mathfrak{a}\widehat{A}\mathfrak{b} = \hat{\mathfrak{a}}\hat{\mathfrak{b}}$$

which finishes the proof. □

Corollary 11.4.20. *Let A be a Noetherian ring, $\mathfrak{a}$ an ideal of A and $\widehat{A}$ the Hausdorff completion of A with respect to the $\mathfrak{a}$-adic topology. Then the topology on $\widehat{A}$ is the $\hat{\mathfrak{a}}$-adic topology.*

Proof. By Corollary 11.4.19 we have $\widehat{(\mathfrak{a}^n)} = (\hat{\mathfrak{a}})^n$. Since $\widehat{(\mathfrak{a}^n)}$ is a fundamental system of neighbourhoods in $\widehat{A}$ by Proposition 2.1.26, the claim follows. □

Corollary 11.4.21. *If A is a Noetherian ring, the ring of normal power series $A[\![X_1, \dots, X_n]\!]$ is a flat A-module.*

Proof. The ring $A[\![X_1, \dots, X_n]\!]$ is the completion of $B = A[X_1, \dots, X_n]$ with respect to the $\mathfrak{m}$-adic topology, where $\mathfrak{m}$ is the set of polynomials with no constant terms. As B is Noetherian, $A[\![X_1, \dots, X_n]\!]$ is a flat B-module by Theorem 11.4.17 and, as B is free A-module, we deduce that $A[\![X_1, \dots, X_n]\!]$ is a flat A-module by Corollary 7.2.22. □

Proposition 11.4.22. *Let A be a Noetherian ring, $\mathfrak{a}$ an ideal of A, $\widehat{A}$ the Hausdorff completion of A with respect to the $\mathfrak{a}$-adic topology and ι the canonical mapping from A to $\widehat{A}$. Then*

(a) The mapping $\mathfrak{m} \mapsto \hat{\mathfrak{m}}$ is a bijection of the set of maximal ideals of A containing $\mathfrak{a}$ onto the set of maximal ideals of $\widehat{A}$ and $\mathfrak{n} \mapsto \iota^{-1}(\mathfrak{n})$ is the inverse bijection.

(b) Let $\mathfrak{m}$ be a maximal ideal of A containing $\mathfrak{a}$. Then the homomorphism $\iota_{\mathfrak{m}} : A_{\mathfrak{m}} \to \widehat{A}_{\hat{\mathfrak{m}}}$ derived from ι is an embedding with dense image if $A_{\mathfrak{m}}$ is given the $\mathfrak{m}A_{\mathfrak{m}}$-adic topology and $\widehat{A}_{\hat{\mathfrak{m}}}$ the $\hat{\mathfrak{m}}\widehat{A}_{\hat{\mathfrak{m}}}$-adic topology.

Proof. Assertion (a) follows immediately from the fact that the canonical homomorphism $A/\mathfrak{a} \to \widehat{A}/\hat{\mathfrak{a}}$ derived from ι is bijective and the fact that every maximal ideal of $\widehat{A}$ contains $\hat{\mathfrak{a}}$, since $\hat{\mathfrak{a}}$ is contained in the Jacobson radical of $\widehat{A}$ (Lemma 11.3.25).

Finally let us prove (b). As $\mathfrak{m} = \iota^{-1}(\hat{\mathfrak{m}})$, $\iota(A - \mathfrak{m}) \subseteq \widehat{A} - \hat{\mathfrak{m}}$ and ι certainly defines a homomorphism $\iota_{\mathfrak{m}} : A_{\mathfrak{m}} \to \widehat{A}_{\hat{\mathfrak{m}}}$. Let us show that $\iota_{\mathfrak{m}}$ is injective; let $a \in A$ and $s \in A - \mathfrak{m}$ be such that

$$\iota_{\mathfrak{m}}(a/s) = \iota(a)/\iota(s) = 0.$$

then there exists $t \in \widehat{A} - \hat{\mathfrak{m}}$ such that $t\iota(a) = 0$ and the annihilator of $\iota(a)$ in A is therefore not contained in $\hat{\mathfrak{m}}$. Now, if $\mathfrak{b}$ is the annihilator of a in A, then the annihilator of $\iota(a)$ in A is $\hat{\mathfrak{b}}$ (Corollary 11.4.18); hence $\mathfrak{b} \not\subseteq \mathfrak{m}$, which shows that $a/s = 0$.

Moreover, there is a commutative diagram

$$\begin{array}{ccc} A/\mathfrak{m}^k & \longrightarrow & A_{\mathfrak{m}}/(\mathfrak{m}A_{\mathfrak{m}})^k \\ \downarrow{\scriptstyle\tau} & & \downarrow{\scriptstyle\tau_{\mathfrak{m}}} \\ \widehat{A}/\hat{\mathfrak{m}}^k & \longrightarrow & \widehat{A}_{\hat{\mathfrak{m}}}/(\hat{\mathfrak{m}}\widehat{A}_{\hat{\mathfrak{m}}})^k \end{array}$$

where τ and $\tau_{\mathfrak{m}}$ are derived from ι and $\iota_{\mathfrak{m}}$ respectively and the horizontal arrows are the canonical isomorphisms. As $\mathfrak{m}^k$ is an open ideal of A (since it contains $\mathfrak{a}^k$), τ is bijective and hence so

is $\tau_{\mathfrak{m}}$. This shows first that $(\hat{\mathfrak{m}}\widehat{A}_{\hat{\mathfrak{m}}})^k = \iota_{\mathfrak{m}}((\mathfrak{m}A_{\mathfrak{m}})^k)$ and hence the topology on $A_{\mathfrak{m}}$ is induced by that on $\widehat{A}_{\hat{\mathfrak{m}}}$. Moreover, $\widehat{A}_{\hat{\mathfrak{m}}} = A_{\mathfrak{m}} + (\hat{\mathfrak{m}}\widehat{A}_{\hat{\mathfrak{m}}})^k$ for all $k > 0$ and hence $A_{\mathfrak{m}}$ is dense in $\widehat{A}_{\hat{\mathfrak{m}}}$. □

Corollary 11.4.23. *Let A be a Noetherian local (resp. semi-local) ring and $\mathfrak{r}$ its Jacobson radical. Then $\widehat{A}$ is a Noetherian local (resp. semi-local) ring whose Jacobson radical is $\hat{\mathfrak{r}}$.*

Proof. As $\widehat{A}/\hat{\mathfrak{m}}$ is isomorphic to $A/\mathfrak{m}$, it is a Noetherian ring and $\hat{\mathfrak{m}} = \iota(\mathfrak{m})$ is a finitely generated A-module and therefore $\widehat{A}$ is Noetherian. The rest part follows from Proposition 11.4.22 and the third formula in Corollary 11.4.19. □

Corollary 11.4.24. *Let A be a Noetherian ring and $\mathfrak{m}$ an maximal ideal of A. Then the $\mathfrak{m}$-adic completion $\widehat{A}$ of A is a Noetherian local ring and is isomomorphic to the $\mathfrak{m}A_{\mathfrak{m}}$-adic completion $\widehat{A_{\mathfrak{m}}}$ of $A_{\mathfrak{m}}$.*

Proof. Taking $\mathfrak{a}$ to be the maximal ideal $\mathfrak{m}$ in Proposition 11.4.22(a), we see the $\mathfrak{m}$-adic completion $\widehat{A}$ is Noetherian local with maximal ideal $\hat{\mathfrak{m}}$. Then by Proposition 11.4.22(b), since $\widehat{A}_{\hat{\mathfrak{m}}}$ is identified with $\widehat{A}$, we have an dense embedding $\iota_{\mathfrak{m}} : A_{\mathfrak{m}} \to \widehat{A}$, where $A_{\mathfrak{m}}$ is given the $\mathfrak{m}A_{\mathfrak{m}}$-adic topology and $\widehat{A}$ the $\hat{\mathfrak{m}}$-adic topology. Since $\widehat{A}$ is complete, this proves $\widehat{A} \cong \widehat{A_{\mathfrak{m}}}$. □

11.4.4 Zariski rings

For a topological ring A, if an ideal $\mathfrak{a}$ of A is such that the given topology on A is the $\mathfrak{a}$-adic topology, then $\mathfrak{a}$ is called a **defining ideal** of the topology on A. Let A be a Noetherian ring, $\mathfrak{a}$ an ideal of A. If $\mathfrak{b}$ is a defining ideal of the $\mathfrak{a}$-adic topology, then there exists an integer $n > 0$ such that $\mathfrak{b}^n \subseteq \mathfrak{a}$ and hence $\mathfrak{b} \subseteq \sqrt{\mathfrak{a}}$; conversely, since A is Noetherian, there exists an integer $k > 0$ such that $(\sqrt{\mathfrak{a}})^k \subseteq \mathfrak{a}$ (Proposition 6.2.3) and hence $\sqrt{\mathfrak{a}}$ is the largest defining ideal of the $\mathfrak{a}$-adic topology.

Proposition 11.4.25. *Let A be a Noetherian ring and $\mathfrak{a}$ an ideal of A. The following properties are equivalent:*

(i) $\mathfrak{a}$ is contained in the Jacobson radical of A.

(ii) Every finitely generated A-module is Hausdorff with the $\mathfrak{a}$-adic topology.

(iii) For every finitely generated A-module M, every submodule of M is closed with respect to the $\mathfrak{a}$-adic topology on M.

(iv) Every maximal ideal of A is closed with respect to the $\mathfrak{a}$-adic topology.

(v) The Hausdorff completion $\widehat{A}$ is a faithfully flat A-module.

Proof. Let us show that (i) implies (ii). Suppose that $\mathfrak{a}$ is contained in the Jacobson radical of A and let M be a finitely generated A-module. If $x \in M$ and $a \in \mathfrak{a}$ are such that $(1-a)x = 0$, then $x = 0$, for $1 - a$ is invertible in A. Then M is Hausdorff with the $\mathfrak{a}$-adic topology.

Next we show that (ii) implies (iii). Suppose (ii) holds. Let M be a finitely generated A-module and N a submodule of M. Then M/N is Hausdorff with the $\mathfrak{a}$-adic topology, which is the quotient topology of the $\mathfrak{a}$-adic topology on M; thus N is closed in M.

Clearly (iii) implies (iv). Now assume (iv), then for every maximal ideal $\mathfrak{m}$ of A, the A-module $A/\mathfrak{m}$ is Hausdorff with the $\mathfrak{a}$-adic topology. This implies $\mathfrak{a}(A/\mathfrak{m}) \neq A/\mathfrak{m}$, unless the $\mathfrak{a}$-adic topology on $A/\mathfrak{m}$ were the trivial topology and $A/\mathfrak{m}$ were reduced to 0, which is absurd

since $A/\mathfrak{m}$ is a field. The canonical image of $\mathfrak{a}$ in $A/\mathfrak{m}$ is therefore an ideal of $A/\mathfrak{m}$ distinct from $A/\mathfrak{m}$ and hence reduced to 0; then $\mathfrak{a} \subseteq \mathfrak{m}$, which proves that $\mathfrak{a}$ is contained in the Jacobson radical of A.

Finally, for every finitely generated A-module M, the canonical mapping $M \mapsto M \otimes_A \widehat{A}$ is identified with the canonical mapping $M \mapsto \widehat{M}$ from M to its Hausdorff completion with respect to the $\mathfrak{a}$-adic topology (by Theorem 11.4.17) and the kernel of this mapping is then the closure of $\{0\}$ in M with respect to this topology. As we already know that $\widehat{A}$ is a flat A-module, the equivalence of (v) and (ii) follows from the characterization of faithfully flat modules (Proposition 7.3.1). This finishes the proof. □

A topological ring A is called a **Zariski ring** if it is Noetherian and there exists a defining ideal $\mathfrak{a}$ for the topology on A satisfiyng the equivalent conditions of Proposition 11.4.25. A Zariski ring A is necessarily Hausdorff (Proposition 11.4.25) and every defining ideal of its topology is contained in the Jacobson radical of A.

Example 11.4.26 (Examples of Zariski rings).

(a) Let A be a Noetherian ring and $\mathfrak{a}$ an ideal of A. If A is Hausdorff and complete with the $\mathfrak{a}$-adic topology, then A is a Zariski ring with this topology. In particular, $\widehat{A}$ is a Zariski ring.

(b) Every quotient ring $A/\mathfrak{b}$ of a Zariski ring A is a Zariski ring, for it is Noetherian and, if $\mathfrak{a}$ is a defining ideal of A, then $\mathfrak{a}(A/\mathfrak{b}) = (\mathfrak{a} + \mathfrak{b})/\mathfrak{b}$ is contained in the Jacobson radical of $A/\mathfrak{b}$.

(c) Let A be a Noetherian semi-local ring and $\mathfrak{t}$ its Jacobson radical. Then A with the $\mathfrak{t}$-adic topology is a Zariski ring. This will always be the topology in question (unless otherwise stated) when we consider a Noetherian semi-local ring as a topological ring.

If A is a Zariski ring and M is a finitely generated A-module, then since M is Hausdorff, we may (by virtue of Proposition 11.4.25) identify M with a subset of $\widehat{M}$ by means of the canonical mapping ι_M. With this identification, by Proposition 11.4.25 we have

Corollary 11.4.27. *Let A be a Zariski ring, M a finitely generated A-module and N a submodule of M. Then $N = \widehat{N} \cap M$.*

Corollary 11.4.28. *Let A be a Zariski ring and M a finitely generated A-madule. If $\widehat{M}$ is a free $\widehat{A}$-module, then M is a free A-madule.*

Proof. Let $\mathfrak{a}$ be a defining ideal of A, which is therefore contained in the Jacobson radical of A. We apply the criterion of Proposition 10.3.9: the canonical mapping $\iota_M : M \to \widehat{M}$ defines a bijection $i_M : M/\mathfrak{a}M \to \widehat{M}/\widehat{\mathfrak{a}M}$. Similarly the canonical map $\iota_M : A \to \widehat{A}$ defines a bijection $i_A : A/\mathfrak{a} \to \widehat{A}/\hat{\mathfrak{a}}$, which is a ring isomorphism. Then $\widehat{M}/\widehat{\mathfrak{a}M}$ is given an $(\widehat{A}/\hat{\mathfrak{a}})$-module structure and hence (by means of i_A) an $(A/\mathfrak{a})$-module structure. It is immediate that i_M is $(A/\mathfrak{a})$-linear, so that it is an $(A/\mathfrak{a})$-module isomorphism. As $\widehat{M}/\widehat{\mathfrak{a}M}$ is a free $(\widehat{A}/\hat{\mathfrak{a}})$-module, $M/\mathfrak{a}M$ is a free $(A/\mathfrak{a})$-module.

On the other hand, let $\eta : \mathfrak{a} \otimes_A M \to M$ be the canonical homomorphism; as $(\mathfrak{a} \otimes_A M) \otimes_A \widehat{A}$ is canonically identified with $\hat{\mathfrak{a}} \otimes_A \widehat{M}$ and $M \otimes_A \widehat{A}$ with $\widehat{M}$, the hypothesis that M is a free A-module implies that the homomorphism $\eta \otimes 1 : \hat{\mathfrak{a}} \otimes_A \widehat{M} \to \widehat{M}$ is injective. As $\widehat{A}$ is a faithfully flat

A-module, we conclude that η is injective and the conditions for applying the above mentioned criterion are indeed fulfilled. □

Corollary 11.4.29. *Let A be a Zariski ring such that A is an integral domain and let $\mathfrak{a}$ be an ideal of A. If the ideal $\hat{\mathfrak{a}}$ of A is principal, then $\mathfrak{a}$ is principal.*

Corollary 11.4.30. *Let A be a Zariski ring such that $\widehat{A}$ is an integral domain, L the field of fractions of $\widehat{A}$ and $K \subseteq L$ the field of fractions of A. Then $\widehat{A} \cap K = A$.*

Proof. Clearly $A \subseteq \widehat{A} \cap K$; on the other hand, if $x \in \widehat{A} \cap K$, then $\widehat{A}x \subseteq \widehat{A}$ and hence, as $\widehat{A}x = \widehat{A} \otimes_A Ax$, we have

$$\widehat{A} \otimes_A ((Ax + A)/A) = (\widehat{A} \otimes_A Ax)/(\widehat{A} \otimes_A A) = 0.$$

As $\widehat{A}$ is a faithfully flat A-module, we deduce that $Ax \subseteq A$, whence $x \in A$. □

Corollary 11.4.31. *Let A be a Noetherian ring, M, N two finitely generated A-modules and $\phi : M \to N$ an A-homomorphism. For every maximal ideal $\mathfrak{m}$ of A, let $A(\mathfrak{m})$ (resp. $M(\mathfrak{m})$, $N(\mathfrak{m})$) denote the Hausdorff completion of A (resp. M, N) with respect to the $\mathfrak{m}$-adic topology and $\phi(\mathfrak{m}) : M(\mathfrak{m}) \to N(\mathfrak{m})$ the corresponding homomorphism to ϕ. For ϕ to be injective (resp. surjective, bijective, zero), it is necessary and sufiicient that $\phi(\mathfrak{m})$ be so for every maximal ideal $\mathfrak{a}$ of A.*

Proof. We know that for ϕ to be injective (resp. surjective, bijective, zero), it is necessary and sufficient that $\phi_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ be so for every maximal ideal $\mathfrak{m}$ of A. We now note that $A_{\mathfrak{m}}$ is a Noetherian local ring and hence a Zariski ring and there is a canonical A-algebra isomorphism $(A_{\mathfrak{m}})(\mathfrak{m}A_{\mathfrak{m}}) \to A(\mathfrak{m})$ (Corollary 11.3.28). On the other hand, there is a commutative diagram

$$\begin{array}{ccccc} M_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} A(\mathfrak{m}) & \longrightarrow & M \otimes_A A(\mathfrak{m}) & \longrightarrow & M(\mathfrak{m}) \\ \downarrow{\scriptstyle \phi_{\mathfrak{m}} \otimes 1} & & \downarrow{\scriptstyle \phi \otimes 1} & & \downarrow{\scriptstyle \phi(\mathfrak{m})} \\ N_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} A(\mathfrak{m}) & \longrightarrow & N \otimes_A A(\mathfrak{m}) & \longrightarrow & N(\mathfrak{m}) \end{array}$$

where the horizontal arrows on the left arise from the associativity of the tensor product and the isomorphisms $M_{\mathfrak{m}} \to M \otimes_A A_{\mathfrak{m}}$, $N_{\mathfrak{m}} \to N \otimes_A A_{\mathfrak{m}}$. As M and N are finitely generated A-modules, it follows from Theorem 11.4.17 that the rows of this diagram consist of isomorphisms; thus we are reduced to proving that $\phi_{\mathfrak{m}}$ being injective (resp. surjective, bijective, zero) is equivalent to $\phi_{\mathfrak{m}} \otimes 1$ being so. But this follows from the fact that $(A_{\mathfrak{m}})(\mathfrak{m}A_{\mathfrak{m}})$ (and hence also $A(\mathfrak{m})$) is a faithfully flat $A_{\mathfrak{m}}$-module. □

Proposition 11.4.32. *Let A, B be two rings and $\rho : A \to B$ be a ring homomorphism. Suppose that A is Noetherian and B is a finitely generated A-module (with the structure defined by f). Let $\mathfrak{a}$ be an ideal of A, then*

(a) For the $\mathfrak{a}^e$-adic topology on B to be Hausdorff, it is necessary and suficient that the elements of $1 + \rho(\mathfrak{a})$ be not divisors of 0 in B.

(b) If A with the $\mathfrak{a}$-adic topology is a Zariski ring, then B with the $\mathfrak{a}^e$-adic topology is a Zariski ring.

(c) If ρ is injectioe (thus identifying A with a subring of B), the $\mathfrak{a}^e$-adic topology on B induces on A the $\mathfrak{a}$-adic topology.

Proof. Recall that the $\mathfrak{a}^e$-adic filtration on B coincides with the $\mathfrak{a}$-adic filtration on the A-module B. Assertion (a) is thus a special case of Proposition 11.4.25 and assertion (c) a special case of Artin-Rees Lemma. Finally let us show (b). Suppose that A is a Zariski ring with the $\mathfrak{a}$-adic topology and let N be a finitely generated B-module; it is also a finitely generated A-module and the $\mathfrak{a}$-adic and $\mathfrak{a}^e$-adic filtrations on N coincide; then N is Hausdorff with the $\mathfrak{a}^e$-adic topology. Finally the A-module B is Noetherian and hence the ring B is Noetherian, which completes the proof that B is a Zariski ring. □

Proposition 11.4.33. *Let A, B be two Zariski rings, $\widehat{A}$, $\widehat{B}$ their completions, $\rho : A \to B$ a continuous ring homomorphism and $\hat{\rho} : \widehat{A} \to \widehat{B}$ the homomorphism obtained from f by passing to the completions. If $\hat{\rho}$ is bijective, then the A-module B is faithfully flat.*

Proof. As A and B are Hausdorff, the hypothesis that $\hat{\rho}$ is bijective implies first that ρ is injective. Identifying (algebraically) A with $\rho(A)$ by means of ρ and $\widehat{A}$ with $\widehat{B}$ by means of $\hat{\rho}$, we then obtain the inclusions $A \subseteq B \subseteq \widehat{A} = \widehat{B}$. Then we know that $\widehat{A}$ is a faithfully flat A-module and a faithfully flat B-module, hence B is a faithfully flat A-module. □

Proposition 11.4.34. *Let A be a Noetherian local ring, $\mathfrak{m}$ its maximal ideal, A its $\mathfrak{m}$-adic completion and B a ring such that $A \subseteq B \subseteq \widehat{A}$. Suppose that B is a Noetherian local ring whose maximal ideal $\mathfrak{n}$ satisfies the relation $\mathfrak{n} = \mathfrak{m}B$. Then*

$$\mathfrak{n}^k = \mathfrak{m}^k B = \hat{\mathfrak{m}}^k \cap B$$

for all $k \geq 0$, the $\mathfrak{n}$-adic topology on B is induced by the $\hat{\mathfrak{m}}$-adic topology on $\widehat{A}$, B is a faithfully flat A-module and there is an isomorphism of $\widehat{A}$ onto the $\mathfrak{n}$-adic completion $\widehat{B}$ of B, which extends the canonical injection $A \to B$.

Proof. It is sufficient to verify the relation $\mathfrak{n}^k = \hat{\mathfrak{m}}^k \cap B$, for, as B is dense in A and the $\mathfrak{n}$-adic topology is induced by the $\hat{\mathfrak{m}}$-adic topology, the last assertion will follow from Corollary 2.2.41 and the last but one from Proposition 11.4.33. The injections $A \to B \to \widehat{A} = \widehat{B}$ induce injective homomorphisms

$$A/(\hat{\mathfrak{m}} \cap A) \longrightarrow B/(\hat{\mathfrak{m}} \cap B) \longrightarrow \widehat{A}/\hat{\mathfrak{m}}$$

We know that $\hat{\mathfrak{m}} \cap A = \mathfrak{m}$ and that $A/\mathfrak{m} \cong \widehat{A}/\hat{\mathfrak{m}}$, hence $B/(\hat{\mathfrak{m}} \cap B) \cong \widehat{A}/\hat{\mathfrak{m}}$, which shows that $B/(\hat{\mathfrak{m}} \cap B)$ is a field, hence that $\hat{\mathfrak{m}} \cap B$ is a maximal ideal of B and therefore $\hat{\mathfrak{m}} \cap B = \mathfrak{n}$. As $A/\mathfrak{m} \cong \widehat{A}/\hat{\mathfrak{m}}$ we have $\widehat{A} = A + \hat{\mathfrak{m}}$, thus $B = A + \mathfrak{n} = A + \mathfrak{m}B$. By induction on k we deduce that

$$B = A + \mathfrak{m}^k B = A + \mathfrak{n}^k$$

for all $k > 1$. As $\mathfrak{n}^k \subseteq \hat{\mathfrak{m}}^k + B$, it is sufficient to show that $\hat{\mathfrak{m}}^k \cap B \subseteq \mathfrak{n}^k$. If $b \in \hat{\mathfrak{m}}^k \cap B$, we may write $b = a + z$ where $a \in A$, $z \in \mathfrak{n}^k$; whence

$$a = b - z \in \hat{\mathfrak{m}}^k \cap A = \mathfrak{m}^k \subseteq \mathfrak{n}^k$$

and $b \in \mathfrak{n}^k$. □

Example 11.4.35. An important case where this applies is the following: B is the ring of integral series in n variables over a complete valued field K, which converge in the neighbourhood of 0, A is the local ring $K[X_1, \ldots, X_n]_{\mathfrak{m}}$ where $\mathfrak{m}$ is the maximal ideal consisting of the polynomials with no constant term and $\widehat{A}$ is the ring of formal power series $K[\![X_1, \ldots, X_n]\!]$.

Proposition 11.4.36. *Let A be a Noetherian ring, $\mathfrak{a}$ an ideal of A, S the multiplicative subset $1+\mathfrak{a}$ of A and M a finitely generated A-module.*

(a) $S^{-1}A$ is a Zariski ring with the $(S^{-1}\mathfrak{a})$-adic topology.

(b) The canonical mapping $i : M \to S^{-1}M$ is continuous if M is given the $\mathfrak{a}$-adic topology and $S^{-1}M$ the $(S^{-1}\mathfrak{a})$-adic topology and $\hat{i} : \widehat{M} \to \widehat{S^{-1}M}$ is an isomorphism.

Proof. Every element of $1+S^{-1}\mathfrak{a}$ is of the form

$$1+(a/(1+b)) = (1+a+b)/(1+b)$$

where $a, b \in \mathfrak{a}$; it is therefore invertible in $S^{-1}A$, which proves that $S^{-1}\mathfrak{a}$ is contained in the Jacobson radical of $S^{-1}A$. As $S^{-1}A$ is Noetherian, it is then a Zariski ring with the $(S^{-1}\mathfrak{a})$-adic topology, which proves (a). Let us show (b). For all $n > 0$, we have

$$i^{-1}((S^{-1}\mathfrak{a})^n M) = i^{-1}(S^{-1}\mathfrak{a}^n M) = \mathfrak{a}^n M$$

since by Proposition 10.2.36, if $x \in i^{-1}(S^{-1}\mathfrak{a}^n M)$ then $(1-a)x = y$, where $a \in \mathfrak{a}$, $y \in \mathfrak{a}^n M$, whence

$$x = (1+a+a^2+\cdots+a^{n-1})y + a^n x \in \mathfrak{a}^n M.$$

This proves that i is continuous and a strict morphism (Proposition 10.2.36). Moreover, the kernel of i, which is the set of $x \in M$ for which there exists some $s \in S$ such that $sx = 0$, is identical with the kernel of the canonical mapping $\iota : M \to \widehat{M}$. Then there exists a topological isomorphism $\iota_0 : i(M) \to \iota(M)$ such that the following diagram is commutative:

$$\begin{tikzcd}
 & \iota(M) \arrow[r, hook] \arrow[dd, "\iota_0"] & \widehat{M} \arrow[dd, "\hat{i}"] \\
M \arrow[ur, "\iota"] \arrow[dr, "i"'] & & \\
 & i(M) \arrow[r, hook] & \widehat{S^{-1}M}
\end{tikzcd}$$

Therefore the problem reduces to verify that $i(M)$ is dense in $S^{-1}M$. Now every element of $S^{-1}M$ may be written as $x/(1-a)$, where $a \in \mathfrak{a}$, and it is immediately verified that

$$x/(1-a) \equiv (1+a+\cdots+a^{n-1})x \mod S^{-1}\mathfrak{a}^n M$$

which completes the proof. □

11.5 Lifting in complete rings

11.5.1 Strongly relatively prime polynomials

Let A be a ring. Two elements x, y of A are called **strongly relatively prime** if the principal ideals (x) and (y) are relatively prime, in other words if $Ax + Ay = A$; it amounts to the same to say that there exist two elements a, b of A such that $ax + by = 1$.

Lemma 11.5.1 (Euclid Lemma). *Let x, y be two strongly relatively prime elements of A; if $z \in A$ is such that x divides yz, then x divides z.*

Proof. If $1 = ax + by$, then $z = x(az) + (yz)b$, so x divides z. □

If x and y are strongly relatively prime in A, then $(xy) = (x) \cap (y)$. If A is an integral domain, two strongly relatively prime elements then have an lcm equal to their product and are therefore relatively prime in the sense that $\gcd(x, y) = 1$. Conversely, if A is a principal ideal domain, two relatively prime elements are also strongly relatively prime, as follows from Bezout's identity.

For polynomial rings there is the following result:

Proposition 11.5.2. *Let A be a ring and F, G two strongly relatively prime polynomials in $A[X]$. Suppose that F is monic and of degree s. Then every polynomial T in $A[X]$ may be written uniquely in the form*

$$T = PF + QG \tag{5.1.1}$$

where $P, Q \in A[X]$ and $\deg(Q) < s$. If further $\deg(T) \leq n$ and $\deg(G) \leq n - s$, then $\deg(P) \leq n - s$.

Proof. As F is monic, $FP \neq 0$ for every nonzero polynomial P of $A[X]$ and in this case $\deg(FP) = s + \deg(P)$. Let T be any polynomial in $A[X]$. As the ideal generated by F and G is the whole of $A[X]$, there exist polynomials P_1 and Q_1 such that

$$T = P_1F + Q_1G.$$

As F is monic of degree s, Euclidean division shows that there exist two polynomials Q' and Q'' such that $Q_1 = Q''F + Q'$ where $\deg(Q') < s$. Then we deduce that

$$T = P_1F + Q_1G = P_1F + Q''FG + Q'G = PF + Q'G$$

where $P = P_1 + Q''G$. To show the uniqueness of formula (5.1.1), it is sufficient to prove that the relations

$$0 = PF + QG, \quad \deg(Q) < s.$$

imply $P = Q = 0$. Now, if this holds, F divides QG and, as F and G are strongly relatively prime, F divides Q by Lemma 11.5.1, which is impossible unless $Q = 0$. This then implies $PF = 0$, and so $P = 0$ by the remark at the begining.

Finally, suppose that $\deg(T) \leq n$ and $\deg(G) \leq n - s$. With the polynomial T in the form (5.1.1),

$$\deg(QG) \leq \deg(Q) + \deg(G) < s + \deg(G) \leq n$$

and therefore

$$s + \deg(P) = \deg(PF) = \deg(T - QG) \leq n$$

whence $\deg(P) \leq n - s$. □

Example 11.5.3. For a polynomial $P \in A[X]$ to be strongly relatively prime to $X - a$ (where $a \in A$), it is necessary and sufiicient that $P(a)$ be invertible in A. For if P and $X - a$ are strongly relatively prime, it follows from Proposition 11.5.2 that there exist $c \in A$ and a polynomial $Q \in A[X]$ such that $1 = (X - a)Q + cP$, whence $cP(a) = 1$ and $P(a)$ is invertible. Conversely, by Euclidean division

$$P = (X - a)G + P(a)$$

and, if $P(a) = b^{-1}$ where $b \in A$, we deduce that $1 = bP - b(X - a)G$, which shows that P and $X - a$ are strongly relatively prime.

Let A and B be two rings and $\rho : A \to B$ a ring homomorphism. If $P = \sum_{n=0}^{\infty} a_n X^n$ is a formal power series in $A[\![X]\!]$, let $f(P)$ denote the formal power series $\sum_{n=0}^{\infty} \rho(a_n)X^n$ in $B[\![X]\!]$. If P is a polynomial, so is $\rho(P)$ and, if further P is monic, then $\rho(P)$ is monic of the same degree as P. Finally, $P \mapsto f(P)$ is clearly a homomorphism of $A[\![X]\!]$ to $B[\![X]\!]$ which extends f and maps X to X.

Proposition 11.5.4. *Let A and B be two rings, $\rho : A \to B$ a homomorphism and P, Q two polynomials in $A[X]$. If P and Q are strongly relatively prime in $A[X]$, then $\rho(P)$ and $\rho(Q)$ are strongly relatively prime in $B[X]$. The converse is true if ρ is surjective, if its kernel is contained in the Jacobson radical of A and if P is monic.*

Proof. Suppose that P and Q are strongly relatively prime; then there exist polynomials U, V in $A[X]$ such that $PU + QV = 1$; we deduce that

$$\rho(P)\rho(U) + \rho(Q)\rho(V) = 1$$

whence the first assertion. To show the second, let $\mathfrak{a}$ denote the kernel of ρ. Let $M = A[X]$ and N be the ideal of M generated by P and Q. As ρ is surjective and $\rho(P)$ is monic, Proposition 11.5.2 shows that for every polynomial $T \in A[X]$ there exist two polynomials U, V in $A[X]$ such that

$$\rho(T) = \rho(P)\rho(U) + \rho(Q)\rho(V)$$

whence the relation $M = N + \mathfrak{a}M$. Now, M/N is a finitely generated A-module, for every polynomial is congruent mod P to a polynomial of degree strictly smaller than $\deg(P)$, P being monic. As $\mathfrak{a}(M/N) = M/N$ and $\mathfrak{a}$ is contained in the Jacobson radical of A, Nakayama's Lemma shows that $M/N = 0$, which means that P and Q are strongly relatively prime. □

11.5.2 Restricted power series and Hensel's lemma

Definition 11.5.5. *A commutative topological ring A is said to be linearly topologized (and its topology is said to be **linear**) if there exists a fundamental system $\mathcal{B}$ of neighbourhoods of 0 consisting of ideals of A.*

Note that in such a ring, the ideals $\mathfrak{a} \in \mathcal{B}$ are open and closed. For all $\mathfrak{a} \in \mathcal{B}$, the quotient topological ring $A/\mathfrak{a}$ is then discrete. For $\mathfrak{a}, \mathfrak{b} \in \mathcal{B}$ and $\mathfrak{b} \subseteq \mathfrak{a}$, let

$$\pi_{\mathfrak{a}\mathfrak{b}} : A/\mathfrak{b} \to A/\mathfrak{a}$$

be the canonical mapping. We know that $(A/\mathfrak{a}, \pi_{\mathfrak{a}\mathfrak{b}})$ is an inverse system of discrete rings (relative to the indexing set $\mathcal{B}$ which is ordered by inclusion and directed), whose inverse limit is a complete Hausdorff linearly topologized ring $\widetilde{A}$. Further, a strict morphism $\iota : A \to \widetilde{A}$ is defined, whose kernel is the closure of $\{0\}$ in A and whose image is dense in $\widetilde{A}$, so that $\widetilde{A}$ is canonically identified with the Hausdorff completion of A.

Definition 11.5.6. *Given a commutative topological ring A, a formal power series*

$$P = \sum_{\alpha \in \mathbb{N}^p} c_\alpha X^\alpha$$

in the ring $A[\![X_1, \dots, X_p]\!]$ is called ***restricted*** *if, for every neighbourhood V of 0 in A, there is only a finite number of coefiicients c_α not belonging to V (in other words, the family (c_α) tends to 0 in A with respect to the filter of complements of finite subsets of $\mathbb{N}^p$.*

If A is linearly topologized, the restricted formal power series in $A[\![X_1, \dots, X_p]\!]$ form a subring of $A[\![X_1, \dots, Xp]\!]$, denoted by $A\{X_1, \dots, X_p\}$, for if $P = \sum a_\alpha X^\alpha$ and $Q = \sum b_\alpha X^\alpha$ are two restricted formal power series and $\mathfrak{a}$ a neighbourhood of 0 in A which is an ideal of A, there exists an integer m such that $a_\alpha \in \mathfrak{a}$ and $b_\alpha \in \mathfrak{a}$ for every $\alpha \in \mathbb{N}^p$ such that $|\alpha| \geq m$. Now, if

$$PQ = \sum c_\alpha X^\alpha \quad \text{where} \quad c_\alpha = \sum_{\beta+\gamma=\alpha} a_\beta b_\gamma.$$

We conclude that if $|\alpha| \geq 2m$, then $|\beta| \geq m$ or $|\gamma| \geq m$ and hence, since $\mathfrak{a}$ is an ideal, $c_\alpha \in \mathfrak{a}$ so long as $|\alpha| \geq 2m$, which establishes our assertion. Moreover, every derivative $\partial(PQ)/\partial X_i$ $(1 \leq i \leq p)$ of a restricted formal power series is restricted, as follows immediately from the definition and the fact that the neighbourhoods $\mathfrak{a} \in \mathcal{B}$ are additive subgroups of A.

Let us always assume that A is linearly topologized and let $\mathcal{B}$ be a fundamental system of neighbourhoods of 0 in A consisting of ideals of A; for all $\mathfrak{a} \in \mathcal{B}$, let $\pi_\mathfrak{a} : A \to A/\mathfrak{a}$ be the canonical homomorphism. By definition, for every restricted formal power series $T \in A\{X_1, \dots, X_n\}$,

$$\pi_\mathfrak{a}(T) \in (A/\mathfrak{a})[X_1, \dots, X_p]$$

Clearly $((A/\mathfrak{a})[X_1, \dots, X_p], \pi_{\mathfrak{a}\mathfrak{b}})$ is an inverse system of rings and $(\pi_\mathfrak{a})$ is an inverse system of homomorphisms $A\{X_1, \dots, X_p\} \to (A/\mathfrak{a})[X_1, \dots, X_p]$; as every polynomial is a restricted formal power series, $\pi_\mathfrak{a}$ is is surjective; its kernel $N_\mathfrak{a}$ is the ideal of $A\{X_1, \dots, X_p\}$ consisting of the restricted formal power series all of whose coefficients belong to $\mathfrak{a}$; we shall give $A\{X_1, \dots, X_p\}$ the (linear) topology for which the $N_\mathfrak{a}$ (for $\mathfrak{a} \in \mathcal{B}$) form a fundamental system of neighbourhoods of 0 (a topology which obviously depends only on that on A). Then it follows from Corollary 3.3.29 that

$$\pi = \varprojlim \pi_\mathfrak{a} : A\{X_1, \dots, X_p\} \to \varprojlim_\mathfrak{a} (A/\mathfrak{a})[X_1, \dots, X_p]$$

is a strict morphism whose kernel is the closure of $\{0\}$ in $A\{X_1, \dots, X_p\}$ and whose image is dense in $B = \varprojlim_\mathfrak{a} (A/\mathfrak{a})[X_1, \dots, X_p]$.

Proposition 11.5.7. *If the linearly topologized ring A is Hausdorff and complete, the canonical homomorphism π is a topological ring isomorphism.*

Proof. For all $\alpha \in \mathbb{N}^p$ and all $\mathfrak{a} \in \mathcal{B}$, let $\phi_\alpha^\mathfrak{a}$ be the mapping $(A/\mathfrak{a})[X_1, \dots, X_p] \to A/\mathfrak{a}$ which maps every polynomial to the coefficient of X^α in this polynomial; clearly the $(\phi_\alpha^\mathfrak{a})_\mathfrak{a}$ form an inverse system of $(A/\mathfrak{a})$-module homomorphisms (relative to the ordered set $\mathcal{B}$) and, as A is canonically identified with $\varprojlim_\mathfrak{a} (A/\mathfrak{a})$ by hypothesis $\phi_\alpha = \varprojlim_\mathfrak{a} \phi_\alpha^\mathfrak{a}$ is a continuous A-homomorphisms from B to A. For every element $S = (S_\mathfrak{a})_{\mathfrak{a}\in\mathcal{B}}$ of B, we consider the formal power series $T = \sum_\alpha \phi_\alpha(S) X^\alpha$. For each $\mathfrak{a} \in \mathcal{B}$, since $S_\mathfrak{a}$ is a polynomial, there exist $n > 0$ such that $\phi_\alpha^\mathfrak{a}(S_\mathfrak{a}) = 0$ for $|\alpha| \geq n$, which implies $\phi_\alpha^\mathfrak{b}(S_\mathfrak{b}) \in \mathfrak{a}/\mathfrak{b}$ for all $\mathfrak{b} \in \mathcal{B}$, $\mathfrak{b} \subseteq \mathfrak{a}$. Taking limits for these $\mathfrak{b}$'s, we then see $\phi_\alpha(S) \in \mathfrak{a}$ for $|\alpha| \geq n$, which proves T is restricted. Also, it is immediate that $\pi(T) = S$. As A is Hausdorff, the intersection of the $N_\mathfrak{a}$ reduces to 0 and hence π is bijective, which completes the proof, since π is a strict morphism. □

Proposition 11.5.8. *Let A, B be two linearly topologized rings, B being Hausdorff and complete, and $\rho : A \to B$ a continuous homomorphism. For every family $(b_i)_{1\leq i\leq p}$ of elements of B, there exists a unique continuous homomorphism*

$$\tilde{\rho} : A\{X_1, \dots, X_p\} \to B$$

such that $\tilde{\rho}(a) = f(a)$ for all $a \in A$ and $\tilde{\rho}(X_i) = b_i$ for $1 \leq i \leq p$.

Proof. There exists a unique homomorphism $v : A[X_1, \dots, X_p] \to B$ such that $v(a) = \rho(a)$ for $a \in A$ and $v(X_i) = b_i$, for $1 \leq i \leq p$. Moreover, if $\mathfrak{b}$ is a neighbourhood of 0 in B which is an ideal, $\rho^{-1}(\mathfrak{a})$ is an ideal of A which is a neighbourhood of 0 and, for every polynomial $P \in N_{\mathfrak{a}}$, clearly $v(P) \in \mathfrak{b}$ and hence v is continuous. As $A[X_1, \dots, X_p]$ is dense in $A\{X_1, \dots, X_p\}$, the existence and uniqueness of $\tilde{\rho}$ follow from Proposition 3.2.8 and the principle of extension of identities. □

Example 11.5.9. In the special case where $A = B$ and f is the identity mapping we shall write $P(b_1, \dots, b_p)$ for the value of $\tilde{f}(P)$ for every restricted formal power series $P \in A\{X_1, \dots, X_p\}$.

Now we turn to the most important application of restricted power series in this part. In a topological ring A, an element x is called **topologically nilpotent** if 0 is a limit of the sequence (x^n). If A is a linearly topologized ring, to say that x is topologically nilpotent means that for every open ideal $\mathfrak{a}$ of A the canonical image of x in $A/\mathfrak{a}$ is a nilpotent element of that ring. If $\mathfrak{r}_{\mathfrak{a}}$ is the nilradical of $A/\mathfrak{a}$, clearly $(\mathfrak{r}_{\mathfrak{a}})$ is an inverse system of subsets and the set $\mathfrak{t}$ of topological nilpotent elements of A is the inverse image of $\varprojlim_{\mathfrak{a}} \mathfrak{r}_{\mathfrak{a}}$ under the canonical homomorphism $A \to \varprojlim A/\mathfrak{a}$; it is therefore a closed ideal of A. If also A is Hausdorff and complete, this ideal is contained in the Jacobson radical of A and, for an element $x \in A$ to be invertible, it is necessary and sufficient that its class mod $\mathfrak{t}$ be invertible in $A/\mathfrak{t}$ (Lemma 11.3.25). Note that if A is a ring and $\mathfrak{a}$ an ideal of A, the elements of $\mathfrak{a}$ are topologically nilpotent with respect to the $\mathfrak{a}$-adic topology.

Theorem 11.5.10 (Hensel's Lemma). *Let A be a complete Hausdorff linearly topologized ring. Let $\mathfrak{m}$ be a closed ideal of A whose elements are topologically nilpotent. Let $A/\mathfrak{m}$ be the quotient topological ring and $\pi : A \to A/\mathfrak{m}$ the canonical mapping. Let T be a restricted formal power series in $A\{X\}$, $\bar{P}$ a monic polynomial in $(A/\mathfrak{m})[X]$ and $\bar{Q}$ a restricted formal power series in $(A/\mathfrak{m})\{X\}$. Suppose that $\pi(T) = \bar{P}\bar{Q}$ and that $\bar{P}$ and $\bar{Q}$ are strongly relatively prime in $(A/\mathfrak{m})\{X\}$. Then there exists a unique ordered pair (P, Q) consisting of a monic polynomial $P \in A[X]$ and a restricted formal power series $Q \in A\{X\}$ such that*

$$T = PQ, \quad \pi(P) = \bar{P}, \quad \pi(Q) = \bar{Q}. \tag{5.2.1}$$

Moreover, P and Q are strongly relatively prime in $A\{X\}$ and, if T is a polynomial, so is Q.

Proof. The proof is divided into several steps. In the first three we assume that A is discrete, in which case T and Q are *polynomials*. First assume that $\mathfrak{m}^2 = 0$. Let P_1, Q_1 be two polynomials of $A[X]$ such that P_1 is monic and $\pi(P_1) = \bar{P}$, $\pi(Q_1) = \bar{Q}$. Proposition 11.5.4 shows that P_1 and Q_1 are strongly relatively prime; hence (Proposition 11.5.2) there exists a unique ordered pair of polynomials (U, V) of $A[X]$ such that

$$T - P_1Q_1 = P_1U + Q_1V, \quad \deg(V) < \deg(P_1) = \deg(\bar{P}).$$

Applying π on this equation, we then see

$$\bar{P}\pi(U) + \bar{Q}\pi(V) = \pi(T) - \bar{P}\bar{Q} = 0.$$

As $\bar{P}$ is monic, $\bar{P}$ and $\bar{Q}$ strongly relatively prime and $\deg(\pi(V)) < \deg(\bar{P})$, the uniqueness part of Proposition 11.5.2 implies that $\pi(U) = \pi(V) = 0$, in other words the coefficients of P_1 and Q_1 belong to $\mathfrak{m}$ and the relation $\mathfrak{m}^2 = 0$ gives

$$T = P_1Q_1 + P_1U + Q_1V = P_1Q_1 + P_1U + Q_1V + UV = (P_1 + V)(Q_1 + U)$$

so the polynomials $P = P_1 + V$ and $Q = Q_1 + U$ are the solutions to the problem.

Now suppose that $\mathfrak{m}$ is nilpotent and let n be the smallest integer such that $\mathfrak{m}^n = 0$ and let us argue by induction on $n > 2$, the theorem having been shown for $n = 2$. Let

$$A' = A/\mathfrak{m}^{n-1}, \quad \mathfrak{m}' = \mathfrak{m}/\mathfrak{m}^{n-1}$$

As $(\mathfrak{m}')^{n-1} = 0$, by induction hypothesis there exists a unique ordered pair (P', Q') of polynomials in $A'[X]$ such that P' is monic and

$$T' = P'Q', \quad \pi'(P') = \bar{P}, \quad \pi'(Q') = \bar{Q},$$

where $\pi' : A' \to A'/\mathfrak{m}' = A/\mathfrak{m}$ and $\theta : A \to A'$ denote the canonical homomorphisms, and $T' = \theta(T)$. On the other hand, as $(\mathfrak{m}')^2 = 0$, there exists a unique ordered pair (P, Q) of polynomials in $A[X]$ such that P is monic and

$$T = PQ, \quad \theta(P) = P', \quad \theta(Q) = Q'.$$

As $\pi = \pi' \circ \theta$, this shows the existence and uniqueness of P and Q satisfying (5.2.1). Moreover P' and Q' are strongly relatively prime by the induction hypothesis and hence so are P and Q.

Next we turn to the case where A is discrete. In this case $\mathfrak{m}$ is no longer necessarily nilpotent, but it is always a nilideal (that is, every element in $\mathfrak{m}$ is nilpotent), since $\mathfrak{m}$ is topological nilpotent and $\{0\}$ is open in A. Let P_0, Q_0 be two polynomials of $A[X]$ such that $(P_0) = \bar{P}$, $\pi(Q_0) = \bar{Q}$ and P_0 is monic. Let us consider the ideal $\mathfrak{n}$ of A generated by the coefficients of $T - P_0Q_0$; it is finitely generated and contained in $\mathfrak{m}$, hence it is nilpotent and by definition, if $\psi : A \to A/\mathfrak{n}$ is the canonical mapping, then $\psi(T) = \psi(P_0)\psi(Q_0)$. Moreover, $\psi(P_0)$ and $\psi(Q_0)$ are strongly relatively prime, as follows from the hypothesis on P and Q and Proposition 11.5.4 applied to the canonical homomorphism $A/\mathfrak{n} \to A/\mathfrak{m}$. By virtue of the nilpotent case, there therefore exists an ordered pair (P, Q) of polynomials in $A[X]$ such that P is monic and relations (5.2.1) hold. The fact that P and Q are strongly relatively prime implies also here that P and Q are strongly relatively prime in $A[X]$ by virtue of Proposition 11.5.4, for $\mathfrak{m}$ is contained in the Jacobson radical of A. Suppose finally that P_1, Q_1 are two polynomials in $A[X]$ satisfying (5.2.1) and such that P_1 is monic and let $\mathfrak{n}_1$ be the finitely generated ideal of A generated by the coefficients of $P - P_1$ and the coefficients of $Q - Q_1$; as $\mathfrak{n}_1$ is contained in $\mathfrak{m}$, it is nilpotent and, if $\psi_1 : A \to A/\mathfrak{n}_1$ is the canonical mapping, then $\psi_1(P) = \psi_1(P_1)$ and $\psi_1(Q) = \psi_1(Q_1)$. The uniqueness property for nilpotent case therefore implies $P = P_1$ and $Q = Q_1$.

Finally, we deal with the general case. Let $\mathcal{B}$ be a fundamental system of neighbourhoods

of 0 in A consisting of ideals of A. For all $\mathfrak{a} \in \mathcal{B}$, let $\pi_\mathfrak{a}$ be the canonical mapping $A \to A/\mathfrak{a}$, $\phi_\mathfrak{a}$ the canonical mapping

$$A/\mathfrak{a} \to (A/\mathfrak{a})/((\mathfrak{m}+\mathfrak{a})/\mathfrak{a}) = A/(\mathfrak{m}+\mathfrak{a}),$$

and $\psi_\mathfrak{a}$ the canonical mapping $A/\mathfrak{m} \to A/(\mathfrak{m}+\mathfrak{a})$ and write $T_\mathfrak{a} = \pi_\mathfrak{a}(T)$, $\bar{P}_\mathfrak{a} = \psi_\mathfrak{a}(\bar{P})$, $\bar{Q}_\mathfrak{a} = \psi_\mathfrak{a}(\bar{Q})$. As each ring $A/\mathfrak{a}$ is discrete, the preceeding argument can be applied to it and we see that there exists a unique ordered pair $(P_\mathfrak{a}, Q_\mathfrak{a})$ of polynomials in $(A/\mathfrak{a})[X]$ such that $P_\mathfrak{a}$ is monic and $T_\mathfrak{a} = P_\mathfrak{a}Q_\mathfrak{a}$, $\phi_\mathfrak{a}(P_\mathfrak{a}) = \bar{P}_\mathfrak{a}$, $\phi_\mathfrak{a}(Q_\mathfrak{a}) = \bar{Q}_\mathfrak{a}$. The uniqueness of this ordered pair implies that, if $\mathfrak{a}, \mathfrak{b} \in \mathcal{B}$, $\mathfrak{b} \subseteq \mathfrak{a}$ and $\pi_{\mathfrak{a}\mathfrak{b}} : A/\mathfrak{b} \to A/\mathfrak{a}$ is the canonical mapping, then $P_\mathfrak{a} = \pi_{\mathfrak{a}\mathfrak{b}}(P_\mathfrak{b})$ and $Q_\mathfrak{a} = \pi_{\mathfrak{a}\mathfrak{b}}(Q_\mathfrak{b})$. Then it follows from the canonical identification of $A\{X\}$ with $\varprojlim_\mathfrak{a} (A/\mathfrak{a})[X]$ that there exists $P \in A\{X\}$ and $Q \in A\{X\}$ such that $T = PQ$ and $\pi_\mathfrak{a}(P) = P_\mathfrak{a}$,$\pi_\mathfrak{a}(Q) = Q_\mathfrak{a}$ for all $\mathfrak{a} \in \mathcal{B}$. Moreover

$$\psi_\mathfrak{a}(\bar{P} - \pi(P)) = \psi_\mathfrak{a}(\bar{Q} - \pi(Q)) = 0,$$

for all $\mathfrak{a} \in \mathcal{B}$, which means that for all $\mathfrak{a} \in \mathcal{B}$ the coefficients of $\bar{P} - \pi(P)$ and $\bar{Q} - \pi(Q)$ all belong to $(\mathfrak{m}+\mathfrak{a})/\mathfrak{m}$. But, as $\mathfrak{m}$ is closed in A, $\bigcap_\mathfrak{a}(\mathfrak{m}+\mathfrak{a}) = \mathfrak{m}$, whence $\bar{P} = \pi(P)$, $\bar{Q} = \pi(Q)$ and P and Q certainly satisfy (5.2.1). Moreover, as the $P_\mathfrak{a}$ are monic and of the same degree, the restricted formal power series P is a monic polynomial. If (P', Q') were another ordered pair satisfying (5.2.1) and such that P' is a monic polynomial, we would deduce that

$$T_\mathfrak{a} = \pi_\mathfrak{a}(P')\pi_\mathfrak{a}(Q'), \quad \phi_\mathfrak{a}(\pi_\mathfrak{a}(P')) = \bar{P}_\mathfrak{a}, \quad \phi_\mathfrak{a}(\pi_\mathfrak{a}(Q')) = \bar{Q}_\mathfrak{a}.$$

By the uniqueness in the discrete case we have $\pi_\mathfrak{a}(P') = P_\mathfrak{a}$ and $\pi_\mathfrak{a}(Q') = Q_\mathfrak{a}$ for all $\mathfrak{a} \in \mathcal{B}$, which implies that $P = P'$ and $Q = Q'$. Let us show finally that P and Q are strongly relatively prime; by virtue of the discrete case and Proposition 11.5.2, for all $\mathfrak{a} \in \mathcal{B}$, there exists a unique ordered pair $(U_\mathfrak{a}, V_\mathfrak{a})$ of polynomials in $(A/\mathfrak{a})[X]$ such that

$$1 = P_\mathfrak{a}U_\mathfrak{a} + Q_\mathfrak{a}V_\mathfrak{a}, \quad \deg(V_\mathfrak{a}) < \deg(P_\mathfrak{a}) = \deg(\bar{P}).$$

The uniqueness of this ordered pair shows immediately that, for $\mathfrak{a}, \mathfrak{b} \in \mathcal{B}$ with $\mathfrak{b} \subseteq \mathfrak{a}$, $U_\mathfrak{a} = \pi_{\mathfrak{a}\mathfrak{b}}(U_\mathfrak{b})$ and $V_\mathfrak{a} = \pi_{\mathfrak{a}\mathfrak{b}}(V_\mathfrak{b})$. Taking account of Proposition 11.5.7, we conclude that there exist two restricted formal power series U, V of $A\{X\}$ such that $U_\mathfrak{a} = \pi_\mathfrak{a}(U)$, $V_\mathfrak{a} = \pi_\mathfrak{a}(V)$ and $1 = PU + QV$.

It remains to verify that, if T is a polynomial, so is Q. Now, the $Q_\mathfrak{a}$ are polynomials by construction and, as $P_\mathfrak{a}$ is monic, the relation $T_\mathfrak{a} = P_\mathfrak{a}Q_\mathfrak{a}$ implies

$$\deg(Q_\mathfrak{a}) \leq \deg(T_\mathfrak{a}) \leq \deg(T)$$

for all $\mathfrak{a} \in \mathcal{B}$, whence immediately the required result by definition of Q. □

11.5.3 System of equations in complete rings

Let A be a ring; we shall say that a system

$$\boldsymbol{f} = (f_1, \ldots, f_p) \in (A[\![X_1, \ldots, X_q]\!])^p$$

of formal power series in the $X_1, \dots, X_q$ with coefficients in A, is **without constant term** if this is true of all the f_j. For every systems of formal power series

$$\boldsymbol{f} = (f_1, \dots, f_p) \in (A[\![X_1, \dots, X_q]\!])^p, \quad \boldsymbol{g} = (g_1, \dots, g_q) \in (A[\![X_1, \dots, X_r]\!])^q$$

such that $\boldsymbol{g}$ is without constant term, we shall denote by $\boldsymbol{f} \circ \boldsymbol{g}$ (or $\boldsymbol{f}(\boldsymbol{g})$) the system of formal power series $f_j(g_1, \dots, g_q)$ in $(A[\![X_1, \dots, X_r]\!])^p$. If

$$\boldsymbol{h} = (h_1, \dots, h_r) \in (A[\![X_1, \dots, X_s]\!])^r$$

is a third system without constant term, then we have

$$(\boldsymbol{f} \circ \boldsymbol{g}) \circ \boldsymbol{h} = \boldsymbol{f} \circ (\boldsymbol{g} \circ \boldsymbol{h}).$$

For every system $\boldsymbol{f}$, we shall denote by $M_{\boldsymbol{f}}$ or $M_{\boldsymbol{f}}(X)$ the Jacobian matrix $(\partial f_i / \partial X_j)$, where i is the index of the rows and j that of the columns. For two systems $\boldsymbol{f}$ and $\boldsymbol{g}$, where $\boldsymbol{g}$ is without constant term, we have

$$M_{\boldsymbol{f} \circ \boldsymbol{g}} = M_{\boldsymbol{f}}(\boldsymbol{g}) \cdot M_{\boldsymbol{g}}. \tag{5.3.1}$$

where $M_{\boldsymbol{f}}(\boldsymbol{g})$ is the matrix whose elements are obtained by substituting g_j for X_j in each series element of $M_{\boldsymbol{f}}$. We shall denote by $M_{\boldsymbol{f}}(0)$ the matrix of constant terms of the elements of $M_{\boldsymbol{f}}$. Then we deduce from (5.3.1) that

$$M_{\boldsymbol{f} \circ \boldsymbol{g}}(0) = M_{\boldsymbol{f}}(0) \cdot M_{\boldsymbol{g}}(0).$$

Given an integer $n > 0$, we shall write

$$\mathbf{1}_n = \boldsymbol{X} = (X_1, \dots, X_n) \in (A[\![X_1, \dots, X_n]\!])^n$$

which will be considered as a matrix with a single column.

For every system $\boldsymbol{f} = (f_1, \dots, f_n) \in (A[\![X_1, \dots, X_n]\!])^n$, $M_{\boldsymbol{f}}$ is a square matrix of order n; we shall denote by $J_{\boldsymbol{f}}$ or $J_{\boldsymbol{f}}(X)$ its determinant and by $J_{\boldsymbol{f}}(0)$ the constant term of $J_{\boldsymbol{f}}$, equal to $\det M_{\boldsymbol{f}}(0)$. If $\boldsymbol{g} = (g_1, \dots, g_n)$ is a system without constant term in $(A[\![X_1, \dots, X_n]\!])^n$, then

$$J_{\boldsymbol{f} \circ \boldsymbol{g}} = J_{\boldsymbol{f}}(\boldsymbol{g}) J_{\boldsymbol{g}}, \quad J_{\boldsymbol{f} \circ \boldsymbol{g}}(0) = J_{\boldsymbol{f}}(0) J_{\boldsymbol{g}}(0).$$

Proposition 11.5.11. *Let A be a ring and $\boldsymbol{f} = (f_1, \dots, f_n)$ a system without constant term of n series in $A[\![X_1, \dots, X_n]\!]$. Suppose that $J_{\boldsymbol{f}}(0)$ is invertible in A. Then there exists a system without constant term $\boldsymbol{g} = (g_1, \dots, g_n)$ of n series in $A[\![X_1, \dots, X_n]\!]$ such that $\boldsymbol{f} \circ \boldsymbol{g} = \mathbf{1}_n$. This system is unique and $\boldsymbol{g} \circ \boldsymbol{f} = \mathbf{1}_n$.*

Proof. The existence and uniqueness of $\boldsymbol{g}$ are clear. It then follows that $J_{\boldsymbol{f}}(0) J_{\boldsymbol{g}}(0) = 1$ and hence $J_{\boldsymbol{g}}(0)$ is also invertible. We conclude that there exists a system $\boldsymbol{h} = (h_1, \dots, h_n)$ of n series without constant term in $A[\![X_1, \dots, X_n]\!]$ such that $\boldsymbol{g} \circ \boldsymbol{h} = \mathbf{1}_n$; from this relation it then follows that

$$\boldsymbol{h} = \mathbf{1}_n \circ \boldsymbol{h} = (\boldsymbol{f} \circ \boldsymbol{g}) \circ \boldsymbol{h} = \boldsymbol{f} \circ (\boldsymbol{g} \circ \boldsymbol{h}) = \boldsymbol{f} \circ \mathbf{1}_n = \boldsymbol{f}$$

so the second clam follows. □

To abbreviate, we shall say in what follows that a ring satisfies **Hensel's conditions** if it is linearly topologized, Hausdorff and complete; given an ideal $\mathfrak{m}$ in such a ring, $\mathfrak{a}$ (or the ordered pair $(A, \mathfrak{m})$) will be said to satisfy Hensel's conditions if $\mathfrak{m}$ is closed in A and its elements are topologically nilpotent. The ideal $\mathfrak{t}$ of A consisting of all the topologically nilpotent elements satisfies Hensel's conditions.

In particular, if A is a ring and $\mathfrak{m}$ an ideal of A and A is Hausdorff and complete with respect to the $\mathfrak{m}$-adic topology, the ordered pair $(A, \mathfrak{m})$ satisfies Hensel's conditions.

Proposition 11.5.12. *Let A be a commutative ring, B a ring satisfying Hensel's conditions and $\phi : A \to B$ a homomorphism. For every family $\boldsymbol{x} = (x_1, \dots, x_n)$ of topologically nilpotent elements of B, there exists a unique homomorphism $\tilde{\phi}$ from $A[\![X_1, \dots, X_n]\!]$ to B such that $\tilde{\phi}(a) = \phi(a)$ for all $a \in A$ and $\tilde{\phi}(X_i) = x_i$ for $1 \leq i \leq n$. Moreover, if $\mathfrak{m}$ denotes the ideal of series without constant term in $A[\![X_1, \dots, X_n]\!]$, then $\tilde{\phi}$ is continuous for the $\mathfrak{m}$-adic topology.*

Proof. Let $\mathfrak{a}$ be the finitely generated ideal generated in B by the x_i's; for every open ideal $\mathfrak{b}$ of B, the images of the x_i in $B/\mathfrak{b}$ are nilpotent, hence the ideal $(\mathfrak{a} + \mathfrak{b})/\mathfrak{b}$ is nilpotent in $B/\mathfrak{b}$ and there exists an integer k such that, for $\alpha \in \mathbb{N}^n$ with $|\alpha| \geq k$ we have $\boldsymbol{x}^\alpha \in \mathfrak{b}$. As every element of $\mathfrak{m}^k$ is a finite sum of formal power series of the form $X^\alpha g(X)$, where $|\alpha| \geq k$, it is seen that, if $\tilde{\phi}$ solves the problem, then $\tilde{\phi}(\mathfrak{m}^k) \subseteq \mathfrak{b}$, which proves the continuity of $\tilde{\phi}$. There obviously exists a unique homomorphism

$$v : A[X_1, \dots, X_n] \to B$$

such that $v(a) = \phi(a)$ for $a \in A$ and $v(X_i) = x_i$, for $1 \leq i \leq n$ and the above argument shows that v is continuous with respect to the topoloogy induced on $A[X_1, \dots, X_n]$ by the $\mathfrak{m}$-adic topology. As $A[X_1, \dots, X_n]$ is dense in $A[\![X_1, \dots, X_n]\!]$ with the $\mathfrak{m}$-adic topology and B is Hausdorff and complete, this completes the proof of the existence and uniqueness of $\tilde{\phi}$. □

If $B = A$ and ϕ is the identity mapping, we shall write $f(x_1, \dots, x_n)$ or $f(\boldsymbol{x})$ for the element $\tilde{\phi}(f)$ for every formal power seriesfe $A[\![X_1, \dots, X_n]\!]$. For every system $\boldsymbol{f} = (f_1, \dots, f_r)$ of formal power series of $A[\![X_1, \dots, X_n]\!]$, let $\boldsymbol{f}(\boldsymbol{x})$ denote the element $(f_1(\boldsymbol{x}), \dots, f_r(\boldsymbol{x}))$ of A^r, then it is said to be obtained by substituting the x_i for the X_i in $\boldsymbol{f}$. If $n \leq m$ and F is a formal power series of $A[\![X_1, \dots, X_m]\!]$, it is possible to consider F as a formal power series in $X_{n+1}, \dots, X_m$ with coefficients in $A[\![X_1, \dots, X_n]\!]$; let

$$F(x_1, \dots, x_n, X_{n+1}, \dots, X_m)$$

denote the formal power series in $A[\![X_{n+1}, \dots, X_m]\!]$ obtained by substituting the x_i for the X_i in the coefficients of F, for $1 \leq i \leq n$.

Corollary 11.5.13. *Let A be a ring satisfying Hensel's condition and $\boldsymbol{x} = (x_1, \dots, x_n)$ a family of topologically nilpotent elements of A. Let $\boldsymbol{g} = (g_1, \dots, g_q)$ be a system without constant term of series in $A[\![X_1, \dots, X_n]\!]$ and $\boldsymbol{f} = (f_1, \dots, f_p)$ a system of formal power series in $A[\![X_1, \dots, X_q]\!]$. Then $\boldsymbol{g}(\boldsymbol{x}) = (g_1(\boldsymbol{x}), \dots, g_q(\boldsymbol{x}))$ is a family of topologically nilpotent elements of A and*

$$(\boldsymbol{f} \circ \boldsymbol{g})(\boldsymbol{x}) = \boldsymbol{f}(\boldsymbol{g}(\boldsymbol{x})). \tag{5.3.2}$$

Proof. The fact that the $g_i(\boldsymbol{x})$ are topologically nilpotent follows immediately from Proposition 11.5.12 and the fact that in A the ideal of topologically nilpotent elements is closed. Relation (5.3.2) is obvious when the f, g are polynomials; on the other hand, if $\mathfrak{m}$ and $\mathfrak{m}'$ are the ideals of series without constant term in $A[\![X_1, \dots, X_q]\!]$ and $A[\![X_1, \dots, X_n]\!]$, respectively, clearly the relation $f \in \mathfrak{m}^k$ implies $f(g_1, \dots, g_q) \in (\mathfrak{m}')^k$. The two sides of (5.3.2) are therefore continuous functions of $\boldsymbol{f}$ to $(A[\![X_1, \dots, X_q]\!])^p$ if $A[\![X_1, \dots, X_q]\!]$ is given the $\mathfrak{m}$-adic topology, by virtue of the above remark and Proposition 11.5.12, whence the claim. □

In what follows, for a ring A and an ideal $\mathfrak{m}$ of A we shall denote by $\mathfrak{m}^{\times n}$ the product set $\prod_{i=1}^n \mathfrak{m}_i$ in A^n, where $\mathfrak{m}_i = \mathfrak{m}$ for all i, to avoid ambiguity.

Proposition 11.5.14. *Let A be a ring and $\mathfrak{m}$ an ideal of A such that the ordered pair $(A, \mathfrak{m})$ satisfies Hensel's conditions. Let $\boldsymbol{f} = (f_1, \dots, f_n)$ be a system without constant term of series in $A[\![X_1, \dots, X_n]\!]$ such that $J_{\boldsymbol{f}}(0)$ is invertible in A. Then, for all $\boldsymbol{x} \in \mathfrak{m}^{\times n}$, $\boldsymbol{f}(\boldsymbol{x}) \in \mathfrak{m}^{\times n}$ and $\boldsymbol{x} \mapsto \boldsymbol{f}(\boldsymbol{x})$ is a bijection of $\mathfrak{m}^{\times n}$ onto itself, the inverse bijection being $\boldsymbol{x} \mapsto \boldsymbol{g}(\boldsymbol{x})$, where $\boldsymbol{g}$ is given by relation $\boldsymbol{f} \circ \boldsymbol{g} = \mathbf{1}_n$.*

Proof. The fact that $\boldsymbol{f}(\boldsymbol{x}) \in \mathfrak{m}^{\times n}$ is obvious when the f_i are polynomials and follows in the general case from Proposition 11.5.12 and the fact that $\mathfrak{m}$ is closed in A. The other assertions of the proposition are then immediate consequences of (5.3.2). □

Corollary 11.5.15. *With the assumption of Proposition 11.5.14, let $\mathfrak{a}$ be a closed ideal of A contained in $\mathfrak{m}$. Then the relation $\boldsymbol{x} \equiv \boldsymbol{y}$ mod $\mathfrak{a}^{\times n}$ is equivalent to $\boldsymbol{f}(\boldsymbol{x}) \equiv \boldsymbol{f}(\boldsymbol{y})$ mod $\mathfrak{a}^{\times n}$.*

Proof. For every formal power series $f \in A[\![X_1, \dots, X_n]\!]$,

$$f(X_1, \dots, X_n) - f(Y_1, \dots, Y_n) = \sum_{i=1}^n (X_i - Y_i) h_i(X_1, \dots, X_n, Y_1, \dots, Y_n)$$

where the h_i belong to $A[\![X_1, \dots, X_n, Y_1, \dots, Y_n]\!]$. It follows immediately that the relation $\boldsymbol{x} \equiv \boldsymbol{y}$ mod $\mathfrak{a}^{\times n}$ implies $\boldsymbol{f}(\boldsymbol{x}) \equiv \boldsymbol{f}(\boldsymbol{y})$ mod $\mathfrak{a}^{\times n}$. The converse is obtained by replacing $\boldsymbol{f}$ by its "inverse" $\boldsymbol{g}$. □

Theorem 11.5.16. *Let A be a ring and $\mathfrak{m}$ an ideal of A such that the ordered pair $(A, \mathfrak{m})$ satisfies Hensel's conditions. Let $\boldsymbol{f} = (f_1, \dots, f_n)$ be a system of n elements of $A\{X_1, \dots, X_n\}$, let $\boldsymbol{a} \in A^n$ and write $e = J_{\boldsymbol{f}}(\boldsymbol{a})$. There exists a system $\boldsymbol{g} = (g_1, \dots, g_n)$ of restricted formal power series without constant term in $A\{X_1, \dots, X_n\}$ such that*

(a) $M_{\boldsymbol{g}}(0) = \mathfrak{a}_n$.

(b) For all $\boldsymbol{x} \in A^n$,

$$\boldsymbol{f}(\boldsymbol{a} + e\boldsymbol{x}) = \boldsymbol{f}(\boldsymbol{a}) + M_{\boldsymbol{f}}(\boldsymbol{a}) \cdot e\boldsymbol{g}(\boldsymbol{x}). \tag{5.3.3}$$

(c) Let $\boldsymbol{h} = (h_1, \dots, h_n)$ be the system offormal power series without constant term such that $\boldsymbol{g} \circ \boldsymbol{h} = \mathfrak{a}_n$. For all $\boldsymbol{y} \in \mathfrak{m}^{\times n}$,

$$\boldsymbol{f}(\boldsymbol{a} + e\boldsymbol{h}(\boldsymbol{y})) = \boldsymbol{f}(\boldsymbol{a}) + M_{\boldsymbol{f}}(\boldsymbol{a}) \cdot e\boldsymbol{y}. \tag{5.3.4}$$

Proof. For every formal power series $f \in A[\![X_1, \dots, X_n]\!]$,

$$f(\boldsymbol{X} + \boldsymbol{Y}) = f(\boldsymbol{X}) + M_f(\boldsymbol{X}) \cdot \boldsymbol{Y} + \sum_{1 \le i \le j \le n} G_{ij}(\boldsymbol{X}, \boldsymbol{Y}) Y_i Y_j \tag{5.3.5}$$

where the G_{ij} are well determined formal power series in $A[\![X_1, \dots, X_n, Y_1, \dots, Y_n]\!]$. If f is restricted, so are the elements of M_f, and the G_{ij} for these formal power series are polynomials if f is a polynomial and it follows from their uniqueness that for every open ideal $\mathfrak{a}$ of A, denoting by $\pi_{\mathfrak{a}} : A \to A/\mathfrak{a}$ the canonical mapping, the image of G_{ij} under $\pi_{\mathfrak{a}}$ is the coefficient of $Y_i Y_j$ in $\pi_{\mathfrak{a}}(F)$ where F is the formal power series $f(\boldsymbol{X} + \boldsymbol{Y})$ in $A[\![X_1, \dots, X_n, Y_1, \dots, Y_n]\!]$; whence our assertion.

This being so, writing formula (5.3.5) for each series f_i, we obtain for all $x \in A^n$,

$$\boldsymbol{f}(\boldsymbol{a} + e\boldsymbol{x}) = \boldsymbol{f}(\boldsymbol{a}) + M_{\boldsymbol{f}}(\boldsymbol{a}) \cdot e\boldsymbol{x} + e^2 \boldsymbol{r}(\boldsymbol{x}) \tag{5.3.6}$$

where $\boldsymbol{r} = (r_1, \dots, r_n)$ is a system of restricted formal power series each of which is of total order ≥ 2. Now there exists a square matrix $N \in \mathcal{M}_n(A)$ such that $M_{\boldsymbol{f}}(\boldsymbol{a})N = e\mathfrak{a}_n$, whence using this in (5.3.6),

$$\boldsymbol{f}(\boldsymbol{a} + e\boldsymbol{x}) = \boldsymbol{f}(\boldsymbol{a}) + M_{\boldsymbol{f}}(\boldsymbol{a}) \cdot e\boldsymbol{x} + M_{\boldsymbol{f}}(\boldsymbol{a})N \cdot e\boldsymbol{r}(\boldsymbol{x})$$

Writing $\boldsymbol{g} = \boldsymbol{1}_n + N \cdot \boldsymbol{r}$, we see that $\boldsymbol{g}$ satisfies conditions (a) and (b); then it is sufficient to replace $\boldsymbol{x}$ by $\boldsymbol{h}(\boldsymbol{y})$ to obtain (c). □

Corollary 11.5.17. *Let A be a ring and $\mathfrak{m}$ an ideal of A such that the ordered pair $(A, \mathfrak{m})$ satisfies Hensel's conditions. Let $f \in A\{X\}$, $a \in A$ and write $e = f'(a)$. If $f(a) \equiv 0$ mod $e^2\mathfrak{m}$, then there exists $b \in A$ such that $f(b) = 0$ and $b \equiv a$ mod $e\mathfrak{m}$. If b' is another element such that $f(b') = 0$ and $b' \equiv a$ mod $e\mathfrak{m}$, then $e(b - b') = 0$. In particular, b is unique if e is not a divisor of zero in A.*

Proof. Let $f(a) = e^2 c$ where $c \in \mathfrak{m}$; formula (5.3.4) for $n = 1$ gives

$$f(a + eh(y)) = e^2(c + y)$$

and it is therefore sufficient to take $y = -c$, whence $b = a + eh(-y)$. Moreover if $b = a + ex$, $b' = a + ex'$ are such that $x, x' \in \mathfrak{m}$ and $f(b) = f(b') = 0$, then we deduce from (5.3.3) that $e^2(g(x) - g(x')) = 0$. As $g(X) - g(Y) = (X - Y)p(X, Y)$, where p is restricted and $p(0, 0) = 1$, we see $g(x) - g(x') = (x - x')v$ where $v \in A$. Note that since $\mathfrak{m}$ is closed, p is restricted and 1 is the constant term of p, we have $p(x, x') - 1 \in \mathfrak{m}$, whence $v \in 1 + \mathfrak{m}$ and so v is invertible. This proves the relation $e(b - b') = 0$. □

Example 11.5.18. Let p be a prime number $\neq 2$ and n an integer whose class mod p is a nonzero square in the prime field $\mathbb{F}_p$. If $\mathbb{Z}_p$ is the ring of p-adic integers, the application of Corollary 11.5.17 to the polynomial $X^2 - n$ shows that n is a square in $\mathbb{Z}_p$; for example 7 is a square in $\mathbb{Z}_3$.

Example 11.5.19. Let $A = K[\![Y]\!]$ be the ring of formal power series in one indeterminate with coefficients in a field K; with the (Y)-adic topology, the ring A is Hausdorff and complete and the map $f(Y) \mapsto f(0)$ defines by passing to the quotient ring an isomorphism of κ_A onto the

field K. By Corollary 11.5.17, if $F(Y, X)$ is a polynomial in X with coefficients in A and a is a simple root of $F(0, X)$ in K, there exists a unique formal power series $f(Y)$ such that $f(0) = a$ and $F(Y, f(Y)) = 0$.

Corollary 11.5.20. *Let A be a ring and $\mathfrak{m}$ an ideal of A such that the ordered pair $(A, \mathfrak{m})$ satisfies Hensel's conditions. Let r, n be integers such that $0 \le r < n$ and $\boldsymbol{f} = (f_{r+1}, \dots, f_n)$ is a system of $n - r$ elements of $A\{X_1, \dots, X_n\}$. Let $J_{\boldsymbol{f}}^{(n-r)}$ denote the minor of $M_{\boldsymbol{f}}(X)$ consisting of the columns of index j such that $r + 1 \le j \le n$. Let $\boldsymbol{a} \in A^n$ be such that $J_{\boldsymbol{f}}(\boldsymbol{a})$ is invertible in A and $\boldsymbol{f}(\boldsymbol{a}) \equiv 0$ mod $\mathfrak{m}^{\times(n-r)}$. Then there exists a unique $\boldsymbol{x} = (x_1, \dots, x_n) \in A^n$ such that $x_j = a_j$ for $1 \le j \le r$ and $x \equiv a$ mod $\mathfrak{m}^{\times n}$ and $\boldsymbol{f}(\boldsymbol{x}) = 0$.*

Proof. Substituting a_j for X_j for $1 \le j \le r$ in the f_i, we see immediately that we may restrict our attention to the case where $r = 0$ to prove the corollary. Proposition 11.5.14 shows then that $\boldsymbol{f}$ defines a bijection on $\boldsymbol{a} + \mathfrak{m}^{\times n}$ onto $\boldsymbol{f}(\boldsymbol{a}) + \mathfrak{m}^{\times n} = \mathfrak{m}^{\times n}$; the corollary follows from the fact that $0 \in \mathfrak{m}^{\times n}$. □

11.6 Flatness of graded modules

Let A be a ring and $\mathfrak{I}$ an ideal of A. An A-module M is called **ideally Hausdorff with respect to** $\mathfrak{I}$ (or simply ideally Hausdorff if there is no ambiguity) if, for every finitely generated ideal $\mathfrak{a}$ of A, the A-module $\mathfrak{a} \otimes_A M$ is Hausdorff with the $\mathfrak{I}$-adic topology.

Example 11.6.1 (Examples of ideally Hausdorff modules).

(a) If A is Noetherian and $\mathfrak{I}$ is contained in the Jacobson radical of A (in other words if A is a Zariski ring with the $\mathfrak{I}$-adic topology), every finitely generated A-module is ideally Hausdorff by Proposition 11.4.25.

(b) Every direct sum of ideally Hausdorff modules is an ideally Hausdorff module, by virtue of the observation

$$\mathfrak{I}^n(\mathfrak{a} \otimes_A \bigoplus_{i \in I} M_i) = \mathfrak{I}^n \bigoplus_{i \in I} (\mathfrak{a} \otimes_A M_i) = \bigoplus_{i \in I} \mathfrak{I}^n(\mathfrak{a} \otimes_A M_i).$$

(c) If an A-module M is flat and Hausdorff with the $\mathfrak{I}$-adic topology, it is ideally Hausdorff, for $\mathfrak{a} \otimes_A M$ is then identified with a submodule of M and the $\mathfrak{I}$-adic topology on $\mathfrak{a} \otimes_A M$ is finer than the topology induced on $\mathfrak{a} \otimes_A M$ by the $\mathfrak{I}$-adic topology on M, which is Hausdorff by hypothesis.

Let A be a ring, $\mathfrak{I}$ an ideal of A, M an A-module and $\mathrm{gr}(A)$ and $\mathrm{gr}(M)$ the graded ring and graded $\mathrm{gr}(A)$-module associated respectively with the ring A and with the module M with the $\mathfrak{I}$-adic filtrations. We have seen that for every nonngegative integer n there is a surjective $\mathbb{Z}$-module homomorphism (see (2.2.2))

$$\gamma_n : (\mathfrak{I}^n/\mathfrak{I}^{n+1}) \otimes_{A/\mathfrak{I}} (M/\mathfrak{I}M) \to \mathfrak{I}^n M/\mathfrak{I}^{n+1} M$$

and a graded homomorphism of degree 0 of graded $\mathrm{gr}(A)$-modules

$$\gamma_M : \mathrm{gr}(A) \otimes_{\mathrm{gr}_0(A)} \mathrm{gr}_0(M) \to \mathrm{gr}(M)$$

whose restriction to $\mathrm{gr}_n(A) \otimes \mathrm{gr}_0(M)$ is γ_n for all n and which is therefore surjective.

Proposition 11.6.2. *Let A be a ring, $\mathfrak{I}$ an ideal of A and M an A-module. The following conditions are equivalent:*

(i) For all $n > 0$, $\mathrm{Tor}_1^A(A/\mathfrak{I}^n, M) = 0$.

(ii) For all $n > 0$, the canonical homomorphism $\theta_n : \mathfrak{I}^n \otimes_A M \to \mathfrak{I}^n M$ is bijective.

Moreover these conditions imply:

(iii) The canonical homomorphism $\gamma_M : \mathrm{gr}(A) \otimes_{\mathrm{gr}_0(A)} \mathrm{gr}_0(M) \to \mathrm{gr}(M)$ bijective.

Conversely, if $\mathfrak{I}$ is nilpotent, then (iii) implies (i) and (ii).

Proof. The equivalence of (i) and (ii) follows from the exact sequence

$$\mathrm{Tor}_1^A(A, M) \longrightarrow \mathrm{Tor}_1^A(A/\mathfrak{I}^n, M) \longrightarrow \mathfrak{I}^n \otimes_A M \longrightarrow A \otimes_A M$$

Consider next the diagram

$$\begin{tikzcd}
 & \mathfrak{I}^{n+1} \otimes_A M \arrow[r] \arrow[d, "\theta_{n+1}"] & \mathfrak{I}^n \otimes_A M \arrow[r] \arrow[d, "\theta_n"] & (\mathfrak{I}^n/\mathfrak{I}^{n+1}) \otimes_A (M/\mathfrak{I}M) \arrow[r] \arrow[d, "\gamma_n"] & 0 \\
0 \arrow[r] & \mathfrak{I}^{n+1}M \arrow[r] & \mathfrak{I}^n M \arrow[r] & \mathrm{gr}_n(M) \arrow[r] & 0
\end{tikzcd} \tag{6.0.1}$$

where we note that $(\mathfrak{I}^n/\mathfrak{I}^{n+1}) \otimes_A (M/\mathfrak{I}M)$ is canonically identified with $(\mathfrak{I}^n/\mathfrak{I}^{n+1}) \otimes_{A/\mathfrak{I}} (M/\mathfrak{I}M)$. This diagram is commutative by definition of γ_n, and its rows are exact. If (ii) holds, θ_n and θ_{n+1} are bijective and so therefore is γ_n, by definition of cokernel, hence (ii) implies (iii).

Conversely, assuming that $\mathfrak{I}$ is nilpotent, let us show that (iii) implies (ii). We shall argue by descending induction on n, since $\mathfrak{I}^n \otimes_A M = 0$ for n sufficiently large. Suppose then that in diagram (6.0.1), γ_n and θ_{n+1} are bijective. Then so is θ_n by the snake lemma, and the induction proves θ_n is bijective for all n. □

Theorem 11.6.3. *Let A be a ring, $\mathfrak{I}$ an ideal of A and M an A-module. Consider the following properties:*

(i) M is a flat A-module.

(ii) $\mathrm{Tor}_1(N, M) = 0$ for every A-module N annihilated by $\mathfrak{I}$.

(iii) $M/\mathfrak{I}M$ is a flat $A/\mathfrak{I}$-module and the canonical map $\mathfrak{I} \otimes_A M \to \mathfrak{I}M$ is bijective.

(iv) $M/\mathfrak{I}M$ is a flat $A/\mathfrak{I}$-module and the canonical map $\gamma_M : \mathrm{gr}(A) \otimes_{\mathrm{gr}_0(A)} \mathrm{gr}_0(M) \to \mathrm{gr}(M)$ is bijective.

(v) For all $n > 0$, $M/\mathfrak{I}^n M$ is a flat $(A/\mathfrak{I}^n)$-module.

Then (i)⇒(ii)⇔(iii)⇒(iv)⇔(v). If further $\mathfrak{I}$ is nilpotent or if A is Noetherian and M is ideally Hausdorff, then these properties are equivalent.

Proof. The implication (i)⇒(ii) is immediate. Also, condition (ii) is equivalent to the following:

(ii′) $\mathrm{Tor}_1^A(N, M) = 0$ for every A-module N annihilated by a power of $\mathfrak{I}$.

In fact, if (ii) holds, then then in particular $\mathrm{Tor}_1^A(\mathfrak{I}^n/\mathfrak{I}^{n+1}, M) = 0$ for all n. From the exact sequence

$$0 \to \mathfrak{I}^{n+1}N \longrightarrow \mathfrak{I}^n N \longrightarrow \mathfrak{I}^n N/\mathfrak{I}^{n+1}N \longrightarrow 0$$

wc derive the exact sequence

$$\mathrm{Tor}_1^A(\mathfrak{I}^{n+1}N, M) \longrightarrow \mathrm{Tor}_1^A(\mathfrak{I}^n N, M) \longrightarrow \mathrm{Tor}_1^A(\mathfrak{I}^n N/\mathfrak{I}^{n+1}N, M)$$

and, as there exists an integer m such that $\mathfrak{I}^m N = 0$, we deduce by descending induction on n that $\mathrm{Tor}_1^A(\mathfrak{I}^n N, M) = 0$ for all $n < m$ and in particular for $n = 0$. It follows from this that if $\mathfrak{I}$ is nilpotent, (ii) implies (i), for (ii′) then means that $\mathrm{Tor}_1^A(N, M) = 0$ for every A-module N and hence that M is flat. Note that the equivalence (ii)⇔(iii) is a special case of Proposition 7.2.24 applied to $R = A$, $S = A/\mathfrak{I}$, $F = M$, $E = N$, taking account of the fact that an $(A/\mathfrak{I})$-module N is the same as an A-module N annihilated by $\mathfrak{I}$.

Now if (ii) holds, so does (ii′) and Proposition 11.6.2 shows that γ_M is an isomorphism. On the other hand, we already know that (ii) implies (iii) and hence $M/\mathfrak{I}M$ is a flat $(A/\mathfrak{I})$-module, which completes the proof that (ii) implies (iv). Also, Proposition 11.6.2 shows that, if $\mathfrak{I}$ is nilpotent, (iv) implies (iii). Taking account of the equivalence of (ii) and (iii), we have therefore proved in this case that (i), (ii), (iii) and (iv) are equivalent.

We prove the equivalence of (iv) and (v). For all $n > 0$, $M/\mathfrak{I}^n M$ has a canonical $(A/\mathfrak{I}^n)$-module structure. If it is filtered by the $(\mathfrak{I}/\mathfrak{I}^n)$-adic filtration, it is immediate that

$$\mathrm{gr}_m(M/\mathfrak{I}^n M) = \begin{cases} \mathrm{gr}_m(M) & m < n \\ 0 & m \geq n. \end{cases}$$

For all $k > 0$, let $A_k = A/\mathfrak{I}^k$, $\mathfrak{I}_k = \mathfrak{I}/\mathfrak{I}^k$, and $M_k = M/\mathfrak{I}^k M$. Let $(\mathrm{iv})_k$ (resp. $(\mathrm{v})_k$) denote the assertion derived from (iv) (resp. (v)) by replacing A, $\mathfrak{I}$, M by A_k, $\mathfrak{I}_k$, M_k. It follows from what has just been said that (iv) is equivalent to "for all $k > 0$, $(\mathrm{iv})_k$" and obviously (v) is equivalent to "for all $k > 0$, $(\mathrm{v})_k$". Then it will suffice to establish the equivalence $(\mathrm{iv})_k$ and $(\mathrm{v})_k$ for all k or also to show that (iv)⇔(v) when $\mathfrak{I}$ is nilpotent. Now we have seen that in that case (iv) is equivalent to (i), and (i) is clearly equivalent to (v). We have therefore shown the equivalence (iv)⇔(v) in all cases and also that of all the properties of the theorem in the case where $\mathfrak{I}$ is nilpotent.

Finaly we show the implication (v)⇒(i) when A is Noetherian and M ideally Hausdorff. It is sufficient to prove that for every ideal $\mathfrak{a}$ of A the canonical mapping $j : \mathfrak{a} \otimes_A M \to M$ is injective. As $\mathfrak{a} \otimes_A M$ is Hausdorff with the $\mathfrak{I}$-adic topology, it suffices to verify that $\ker j \subseteq \mathfrak{I}^n(\mathfrak{a} \otimes_A M)$ for every integer $n > 0$. By Theorem 11.4.12, there exists an integer k such that $\mathfrak{a}_k := \mathfrak{a} \cap \mathfrak{I}^k \subseteq \mathfrak{I}^n\mathfrak{a}$. Now, denoting by $\iota : \mathfrak{a}_k \to \mathfrak{a}$, $\pi : \mathfrak{a} \to \mathfrak{a}/\mathfrak{a}_k$ and $\psi : \mathfrak{a}/\mathfrak{a}_k \to A/\mathfrak{I}^k$ the canonical mappings, there is a commutative diagram

$$\begin{tikzcd}
\mathfrak{a}_k \otimes_A M \arrow[r, "\iota\otimes 1_M"] & \mathfrak{a} \otimes_A M \arrow[r, "\pi\otimes 1_M"] \arrow[d] & (\mathfrak{a}/\mathfrak{a}_k) \otimes_A M \arrow[r] \arrow[d, "\psi\otimes 1_M"] & 0 \\
& M \arrow[r] & (A/\mathfrak{I}^k) \otimes_A M &
\end{tikzcd}$$

in which the first row is exact. The map $\psi \otimes 1_M$ is injective since it can also be written into

$$\psi \otimes 1_{M/\mathfrak{I}^k M} : (\mathfrak{a}/\mathfrak{a}_k) \otimes_{A/\mathfrak{I}^k} (M/\mathfrak{I}^k M) \to M/\mathfrak{I}^k M$$

and, as ψ is injective and by (v) $M/\mathfrak{I}^k M$ is a flat $(A/\mathfrak{I}^k)$-module. By a simple diagram chasing we see $\ker j \subseteq \operatorname{im}(\iota \otimes 1_M)$, which shows the claim and completes the proof. □

Proposition 11.6.4. *Let A be a ring, $\mathfrak{I}$ an ideal of A and B a Noetherian A-algebra such that $\mathfrak{I}$ is contained in the Jacobson radical of B. Then every finitely generated B-module M is an ideally Hausdorff A-module with respect to $\mathfrak{I}$.*

Proof. Wc shall see more generally that for every finitely generated A-module N, $N \otimes_A M$ is Hausdorff with the $\mathfrak{I}$-adic topology. Let $\mathfrak{r}$ be the Jacobson radical of B. As $\mathfrak{I}B$ is contained in $\mathfrak{r}$ and the B-module $N \otimes_A M$ is canonically identified with $N_{(B)} \otimes_B M$ by virtue of the associativity of the tensor product, the $\mathfrak{I}$-adic topology on $N \otimes_A M$ is therefore identified with a finer topology than the $\mathfrak{r}$-adic topology on $N_{(B)} \otimes_B M$. But this latter topology is Hausdorff since $N_{(B)} \otimes_B M$ is a finitely generated B-module, whence the conclusion. □

Proposition 11.6.5. *Let A be a ring, B an A-algebra, $\mathfrak{I}$ an ideal of A and M a B-module. Suppose that B is a Noetherian ring and a flat A-module and that M is ideally Hausdorff with respect to $\mathfrak{I}B$. The following conditions are equivalent:*

(i) M is a flat B-module.

(ii) M is a flat A-module and $M/\mathfrak{I}M$ is a flat $(B/\mathfrak{I}B)$-module.

If further the canonical homomorphism $A/\mathfrak{I} \to B/\mathfrak{I}B$ is bijective, then these are also equivalent to:

(iii) M is a flat A-module.

Proof. Condition (i) implies (ii) by Corollary 7.2.21 and Corollary 7.2.22 and the fact that $M/\mathfrak{I}M$ is isomorphic to $M \otimes_B B/\mathfrak{I}B$. Suppose condition (ii) holds. To show that M is a flat B-module, we shall apply Theorem 11.6.3 with A replaced by B and $\mathfrak{I}$ by $\mathfrak{I}B$. It will therefore be sufficient to show that the canonical mapping $\phi : \mathfrak{I}B \otimes_B M \to \mathfrak{I}M$ is injective. Let ϕ_1 be the canonical mapping $\mathfrak{I} \otimes_A B \to \mathfrak{I}B$ and ϕ_2 the canonical isomorphism $\mathfrak{I} \otimes_A M \to (\mathfrak{I} \otimes_A B) \otimes_B M$. Then

$$\mathfrak{I} \otimes_A M \xrightarrow{\phi_2} (\mathfrak{I} \otimes_A B) \otimes_B M \xrightarrow{\phi_1 \otimes 1_M} \mathfrak{I}B \otimes_B M \xrightarrow{\phi} \mathfrak{I}M$$

Now $\psi : \mathfrak{I} \otimes_A M \to \mathfrak{I}M$ is an isomorphism since M is a flat A-module, whilst ϕ_1 is an isomorphism because B is flat over A. Therefore ϕ is then an isomorphism.

Let $\rho : A/\mathfrak{I} \to B/\mathfrak{I}B$ be the canonical homomorphism. The $(A/\mathfrak{I})$-module structure on $M/\mathfrak{I}M$ derived by means of ρ is isomorphic to that on $M \otimes_A (A/\mathfrak{I})$. Then it follows that, if M is a flat A-module, $M/\mathfrak{I}M$ is a flat $(A/\mathfrak{I})$-module and hence also a flat $(B/\mathfrak{I}B)$-module if ρ is an isomorphism. We have thus proved that (iii)⇒(ii) in that case. □

Corollary 11.6.6. *Let A be a Noetherian ring, $\mathfrak{I}$ an ideal of A, $\widehat{A}$ the Hausdorff completion of A with respect to the $\mathfrak{I}$-adic topology and M an ideally Hausdorff $\widehat{A}$-module with respect to $\widehat{\mathfrak{I}}$. For M ta be a flat A-module, it is necessary and sufficient that M be a flat $\widehat{A}$-module.*

Proof. We know in fact that A is a Noetherian ring and a flat A-module, that $\widehat{\mathfrak{I}} = \mathfrak{I}\widehat{A}$ and that the canonical homomorphism $A/\mathfrak{I} \to \widehat{A}/\widehat{\mathfrak{I}}$ is bijective. Proposition 11.6.5 can therefore be applied. □

Proposition 11.6.7. *Let A and B be two Noetherian rings, $\rho : A \to B$ a ring homomorphism, $\mathfrak{I}$ an ideal of A and $\mathfrak{K}$ an ideal of B containing $\mathfrak{I}B$ and contained in the Jacobson radical of B. Let $\widehat{A}$ be the Hausdorff completion of A with respect to the $\mathfrak{I}$-adic topology and B the Hausdorff completion of B with respect to the $\mathfrak{K}$-adic topology. Let M be a finitely generated B-module and $\widehat{M}$ its Hausdorff completion with respect to the $\mathfrak{K}$-adic topology. Then the following properties are equivalent:*

(i) M is a flat A-module.

(ii) $\widehat{M}$ is a flat A-module.

(iii) $\widehat{M}$ is a flat $\widehat{A}$-module.

Proof. As B with the $\mathfrak{K}$-adic topology is a Zariski ring, $\widehat{B}$ is a faithfully flat B-module and $\widehat{M}$ is canonically isomorphic to $M \otimes_B \widehat{B}$. It is immediately verified that this canonical isomorphism is an isomorphism of the A-module structure on $\widehat{M}$ onto the A-module structure on $M \otimes_B \widehat{B}$ derived from that on M. Applying Proposition 7.3.5, we see that for M to be a flat A-module, it is necessary and sufficient that $\widehat{M}$ be a flat A-module. Moreover, $\widehat{M}$ is a finitely generated B-module and $\mathfrak{I}\widehat{B}$ is contained in $\widehat{\mathfrak{K}} = \mathfrak{K}\widehat{B}$ and hence in the Jacobson radical of $\widehat{B}$ (Proposition 11.4.22). Therefore $\widehat{M}$ is an ideally Hausdorff $\widehat{A}$-module with respect to $\widehat{\mathfrak{I}}$ by Proposition 11.6.4. Conditions (ii) and (iii) are therefore equivalent by the Corollary to Proposition 11.6.5. □

11.7 Exercise

Exercise 11.7.1. Show that p-adic completion is not a right-exact functor on the category of all $\mathbb{Z}$-modules.

Proof. Let $A = (\mathbb{Z}/p\mathbb{Z})^{\oplus\mathbb{N}}$ and $B = \bigoplus_n \mathbb{Z}/p^n\mathbb{Z}$. Consider the short exact sequence

$$0 \longrightarrow A \xhookrightarrow{\iota} B \xrightarrow{\pi} B/A \longrightarrow 0$$

If we give them the topology induced by B, namely $\{\iota^{-1}(p^nB)\}$ and $\{\pi(p^nB)\}$, then by Corollary 11.3.7 the induced conplition sequence is exact. Note that on $B/\alpha(A)$, the induced topology is just the same as the p-adic topology. So if we instead use the p-adic topology, the sequence is not exact. □

Remark 11.7.1. Though it does preserve surjectivity, because if $\rho : B \to C$ is a surjection, we have

$$\rho(p^nB) = p^n\rho(B) = p^nC,$$

so we have a surjective map of surjective inverse systems, and Corollary 11.3.7 tells us the map $\widehat{\rho} : \widehat{B} \to \widehat{C}$ is surjective.

The p-adic completion is not left-exact, by the same example; the essential reason is that given a general homomorphism $\alpha : A \to B$, we needn't have $\alpha(p^nA) = \alpha(A) \cap p^nB$, so the

p-adic topology on A is not that induced from B and the hypotheses of Corollary 11.3.7 are not met.

Exercise 11.7.2. In Exercise 11.7.1, let $A_n = \iota^{-1}(p^n B)$, and consider the exact sequence

$$0 \longrightarrow A_n \longrightarrow A \longrightarrow A/A_n \longrightarrow 0$$

Show that $\varprojlim$ is not right exact, and compute $\varprojlim^1 A_n$.

Proof. From Exercise 11.7.1 we already have

$$A_n = \bigoplus_{j>n} G_j, \quad A/A_n = \bigoplus_{j=1}^{n} G_j$$

where $G_i = \mathbb{Z}/p\mathbb{Z}$ for all i. The maps

$$A_{n+1} \hookrightarrow A_n, \quad A \xrightarrow{\text{id}} A, \quad A/A_{n+1} \rightarrowtail A/A_n$$

give rise to an inverse system, hence we can form the inverse limits, and by Proposition 11.3.6 we get an exact sequence

$$0 \longrightarrow \varprojlim A_n \longrightarrow \varprojlim A \longrightarrow \varprojlim A/A_n \longrightarrow \varprojlim^1 A_n \longrightarrow \varprojlim^1 A \longrightarrow \varprojlim^1 A/A_n \longrightarrow 0$$

Since $\{A\}$ and $\{A/A_n\}$ are surjective inverse systems, $\varprojlim^1 A = \varprojlim^1 A/A_n = 0$. Also, the inverse limits can be calculate to be

$$\varprojlim A_n = 0, \quad \varprojlim A = A = \bigoplus_{j=1}^{n} G_j, \quad \varprojlim A/A_n = \prod_{i=1}^{\infty} G_j$$

Hence we get a short exact sequence

$$0 \longrightarrow \bigoplus_{j=1}^{n} G_j \xrightarrow{\psi} \prod_{j=1}^{\infty} G_j \longrightarrow \varprojlim^1 A_n \longrightarrow 0$$

Then the map ψ is simply the inclusion, and we see $\varprojlim^1 A_n = \prod_{j=1}^{\infty} G_j / \bigoplus_{j=1}^{n} G_j$. □

Exercise 11.7.3. Let A be a Noetherian ring and let $\mathfrak{a}, \mathfrak{b}$ be ideals in A. If M is any A-module, let $M^{\mathfrak{a}}, M^{\mathfrak{b}}$ denote its $\mathfrak{a}$-adic and $\mathfrak{b}$-adic completions respectively. If M is finitely generated, prove that $(M^{\mathfrak{a}})^{\mathfrak{b}} \cong M^{\mathfrak{a}+\mathfrak{b}}$.

Proof. Take the $\mathfrak{a}$-adic complition of $0 \longrightarrow \mathfrak{b}^m M \longrightarrow M \longrightarrow M/\mathfrak{b}^m M \longrightarrow 0$, we get

$$0 \longrightarrow (\mathfrak{b}^m M)^{\mathfrak{a}} \longrightarrow M^{\mathfrak{a}} \longrightarrow (M/\mathfrak{b}^m M)^{\mathfrak{a}} \longrightarrow 0$$

By Theorem 11.4.17 we have

$$\begin{aligned}(\mathfrak{b}^m M)^{\mathfrak{a}} &\cong A^{\mathfrak{a}} \otimes_A \mathfrak{b}^m M = A^{\mathfrak{a}} \otimes_A \mathfrak{b}^m \otimes_A M = A^{\mathfrak{a}} \otimes_A M \otimes_A \mathfrak{b}^m \\ &\cong \mathfrak{b}^m \otimes M^{\mathfrak{a}} = \mathfrak{b}^m M^{\mathfrak{a}}\end{aligned}$$

so from the sequence we get $(M/\mathfrak{b}^m M)^{\mathfrak{a}} \cong M^{\mathfrak{a}}/\mathfrak{b}^m M^{\mathfrak{a}}$. Now we have

$$(M^{\mathfrak{a}})^{\mathfrak{b}} = \varprojlim_m M^{\mathfrak{a}}/\mathfrak{b}^m M^{\mathfrak{a}} = \varprojlim_m (M/\mathfrak{b}^m M)^{\mathfrak{a}} = \varprojlim_m \varprojlim_n \frac{M/\mathfrak{b}^m M}{\mathfrak{a}^n (M/\mathfrak{b}^m M)}.$$

Since we have

$$\mathfrak{a}^n (M/\mathfrak{b}^m M) \cong \frac{\mathfrak{a}^n M + \mathfrak{b}^m M}{\mathfrak{b}^m M}.$$

we get

$$(M^{\mathfrak{a}})^{\mathfrak{b}} = \varprojlim_m \varprojlim_n M/(\mathfrak{a}^n M + \mathfrak{b}^m M) \cong \varprojlim_n M/(\mathfrak{a}^n M + \mathfrak{b}^n M)$$

Now note that

$$(\mathfrak{a} + \mathfrak{b})^{2n} \subseteq \mathfrak{a}^n + \mathfrak{b}^n \subseteq (\mathfrak{a} + \mathfrak{b})^n$$

so the topology induced by $\mathfrak{a}^n M + \mathfrak{b}^n M$ is the same as that by $(\mathfrak{a} + \mathfrak{b})^n$, hence we get the desired result. □

Exercise 11.7.4. Let A be the local ring of the origin in $\mathbb{C}^n$ (i.e., the ring of all rational functions $f/g \in \mathbb{C}(z_1, \ldots, z_n)$ with $g(0) \neq 0$), let B be the ring of power series in $z_1, \ldots, z_n$ which converge in some neighborhood of the origin, and let C be the ring of formal power series in $z_1, \ldots, z_n$, so that $A \subseteq B \subseteq C$. Show that B is a local ring and that its completion for the maximal ideal topology is C. Assuming that B is Noetherian, prove that B is A-flat.

Proof. The surjective ring homomorphism

$$\phi : B \to \mathbb{C}, \quad f \mapsto f(0)$$

shows the ideal $\mathfrak{m} = (z_1, \ldots, z_n)$ of power series with zero constant term is maximal. To show B is local, note that if $f \notin \mathfrak{m}$, then $f(0) \neq 0$ and f is a unit in C, and thus a unit in B. So $\mathfrak{m}$ is maximal.

We first compute the complition, note that

$$\mathbb{C}[z_1, \ldots, z_n] \subseteq A \subseteq B \subseteq C$$

and that C is the complition of $\mathbb{C}[z_1, \ldots, z_n]$ by the $(z_1, \ldots, z_n)$-adic topology. Thus we have

$$C = \widehat{\mathbb{C}[z_1, \ldots, z_n]} \subseteq \widehat{A} \subseteq \widehat{B} \subseteq \widehat{C} = C$$

So $\widehat{A} = \widehat{B} = C$. Since we know C is a faithfully flat B-algebra and A-algebra, we conclude B is a flat A-algebra. □

Chapter 12

Associated prime ideals and primary decomposition

12.1 Associated prime ideals of a module

12.1.1 Definition of associated prime ideals

Let M be a module over a ring A. A prime ideal $\mathfrak{p}$ is said to be **associated with M** if there exists $x \in M$ such that $\mathfrak{p}$ is equal to the annihilator of x. The set of prime ideals associated with M is denoted by $\mathrm{Ass}_A(M)$, or simply $\mathrm{Ass}(M)$.

Example 12.1.1. Let $\mathfrak{a}$ be an ideal in the polynomial ring $A = \mathbb{C}[X_1, \dots, X_n]$, V the corresponding affine algebraic variety and $V_1, \dots, V_p$ the irreducible components of V. If M is taken to be the ring $A/\mathfrak{a}$ of functions which are regular on V, the set of prime ideals associated with M consists of the ideals of $V_1, \dots, V_p$ and in general other prime ideals each of which contains one of the ideals of the V_i.

As the annihilator of 0 is A, an element $x \in M$ whose annihilator is a prime ideal is necessarily nonzero. To say that a prime idea $\mathfrak{p}$ is associated with M amounts to saying that M contains a submodule isomorphic to $A/\mathfrak{p}$ (namely Ax, for all $x \in M$ whose annihilator is $\mathfrak{p}$). If an A-module M is the union of a family $(M_i)_{i \in I}$ of submodules, then clearly

$$\mathrm{Ass}(M) = \bigcup_{i \in I} \mathrm{Ass}(M_i). \tag{1.1.1}$$

Proposition 12.1.2. *For every prime ideal $\mathfrak{p}$ of a ring A and every nonzero submodule M of $A/\mathfrak{p}$, $\mathrm{Ass}(M) = \{\mathfrak{p}\}$.*

Proof. As the ring $A/\mathfrak{p}$ is an integral domain, the annihilator of an nonzero element of $A/\mathfrak{p}$ is $\mathfrak{p}$. □

Proposition 12.1.3. *Let M be a module over a ring A. Every maximal element of the set of ideals $\mathrm{Ann}(x)$ of A, where x runs through the set of nonzero elements of M, belongs to $\mathrm{Ass}(M)$.*

Proof. Let $\mathfrak{p} = \mathrm{Ann}(x)$ (where $x \in M$ is nonzero) be such a maximal element; it is sufficient to show that $\mathfrak{p}$ is prime. As $x \neq 0$, $\mathfrak{p}$ is proper. Let a, b be elements of A such that $ab \in \mathfrak{p}$ but $a \notin \mathfrak{p}$. Then $ax \neq 0$ and $\mathfrak{p} \subseteq \mathrm{Ann}(ax)$. As $\mathfrak{p}$ is maximal, $\mathrm{Ann}(ax) = \mathfrak{p}$, whence $b \in \mathfrak{p}$, so that $\mathfrak{p}$ is prime. □

Corollary 12.1.4. *Let M be a module over a Noetherian ring A. Then the condition $M \neq \{0\}$ is equivalent to* $\mathrm{Ass}(M) \neq \varnothing$.

Proof. If $M = \{0\}$, clearly $\mathrm{Ass}(M)$ is empty (without any hypothesis on A). If $M \neq \{0\}$, the set of ideals of the form $\mathrm{Ann}(x)$, where $x \in M$ and $x \neq 0$, is non-empty and consists of ideals of A. As A is Noetherian, this set has a maximal element; then it suffices to apply Proposition 12.1.3. □

Corollary 12.1.5. *Let A be a Noetherian ring, M an A-module and $a \in A$. For the homothety on M with ratio a to be injective, it is necessary and sufficient that a belong to no prime ideal associated with M.*

Proof. If a belongs to a prime ideal $\mathfrak{p} \in \mathrm{Ass}(M)$, then $\mathfrak{p} = \mathrm{Ann}(x)$ where $x \in M$ and $x \neq 0$, whence $ax = 0$ and the homothety with ratio a is not injective. Conversely, if $ax = 0$ for some $x \in M$ such that $x \neq 0$, then $Ax \neq \{0\}$, whence $\mathrm{Ass}(Ax) \neq \varnothing$. Let $\mathfrak{p} \in \mathrm{Ass}(Ax)$, then obviously $\mathfrak{p} \in \mathrm{Ass}(M)$ and $\mathfrak{p} = \mathrm{Ann}(bx)$ for some $b \in A$; then $a \in \mathfrak{p}$, since $abx = 0$. □

Corollary 12.1.6. *The set of divisors of zero in a Noetherian ring A is the union of the ideals in* $\mathrm{Ass}(A)$.

Proposition 12.1.7. *If we have a short exact sequence of A-modules*

$$0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$$

then $\mathrm{Ass}(L) \subseteq \mathrm{Ass}(M) \subseteq \mathrm{Ass}(L) \cup \mathrm{Ass}(N)$.

Proof. The inclusion $\mathrm{Ass}(L) \subseteq \mathrm{Ass}(M)$ is obvious. Let $\mathfrak{p} \in \mathrm{Ass}(M)$, E be a submodule of M isomorphic to $A/\mathfrak{p}$ and $F = E \cap L$. If $F = \{0\}$, E is isomorphic to a submodule of N, whence $\mathfrak{p} \in \mathrm{Ass}(N)$. If $F \neq \{0\}$, the annihilator of every nonzero element of F is $\mathfrak{p}$ (Proposition 12.1.3) and hence $\mathfrak{p} \in \mathrm{Ass}(F) \subseteq \mathrm{Ass}(L)$. □

Corollary 12.1.8. *If $M = \bigoplus_{i \in I} M_i$ then* $\mathrm{Ass}(M) = \bigcup_{i \in I} \mathrm{Ass}(M_i)$.

Proof. It may be reduced to the case where I is finite by means of (1.1.1), then to the case where $|I| = 2$ by induction. Then let $I = \{i, j\}$, where $i \neq j$. As M/M_i is isomorphic to M_j, we have $\mathrm{Ass}(M) \subseteq \mathrm{Ass}(M_i) \cup \mathrm{Ass}(M_j)$. Moreover, $\mathrm{Ass}(M_i)$ and $\mathrm{Ass}(M_j)$ are contained in $\mathrm{Ass}(M)$ by Proposition 12.1.7, whence the result. □

Corollary 12.1.9. *Let M be an A-module and $(Q_i)_{i \in I}$ a finite family of submodules of M. If $\bigcap_{i \in I} Q_i = \{0\}$ then*

$$\mathrm{Ass}(M) \subseteq \bigcup_{i \in I} \mathrm{Ass}(M/Q_i).$$

Proof. The canonical mapping $M \to \bigoplus_i (M/Q_i)$ is injective; then it suffices to apply Proposition 12.1.7 and Corollary 12.1.8. □

Proposition 12.1.10. *Let M be an A-module and Φ a subset of* $\mathrm{Ass}(M)$. *Then there exists a submodule N of M such that* $\mathrm{Ass}(N) = \mathrm{Ass}(M) - \Phi$ *and* $Ass(M/N) = \Phi$.

Proof. Let $\mathcal{M}$ be the set of submodules P of M such that $\mathrm{Ass}(P) \subseteq \mathrm{Ass}(M) - \Phi$. Formula (1.1.1) shows that the set $\mathcal{M}$, ordered by inclusion, is inductive. Moreover, $\{0\} \in \mathcal{M}$ and hence $\mathcal{M} \neq \varnothing$. Let N be a maximal element of $\mathcal{M}$. Then $\mathrm{Ass}(N) \subseteq \mathrm{Ass}(M) - \Phi$. We shall see that $\mathrm{Ass}(M/N) \subseteq \Phi$, which, by Proposition 12.1.7, will complete the proof. Let $\mathfrak{p} \in \mathrm{Ass}(M/N)$; then M/N contains a submodule F/N isomorphic to $A/\mathfrak{p}$. By Proposition 12.1.7 and Proposition 12.1.2, $\mathrm{Ass}(F) \subseteq \mathrm{Ass}(N) \cup \{\mathfrak{p}\}$. Since N is maximal in $\mathcal{M}$, $F \notin \mathcal{M}$ and hence $\mathfrak{p} \in \Phi$. □

12.1.2 Associated prime ideal of localizations

Proposition 12.1.11. *Let A be a ring, S a multiplicative subset of A, Φ the set of ideals of A which do not meet S and M an A-module. Then:*

(a) The mapping $\mathfrak{p} \mapsto S^{-1}\mathfrak{p}$ is a bijection of $\mathrm{Ass}_A(M) \cap \Phi$ onto a subset of $\mathrm{Ass}_{S^{-1}A}(S^{-1}M)$.

(b) If $\mathfrak{p} \in \Phi$ is a finitely generated ideal and $S^{-1}\mathfrak{p} \in \mathrm{Ass}_{S^{-1}A}(S^{-1}M)$, then $\mathfrak{p} \in \mathrm{Ass}_A(M)$.

Proof. Recall that the mapping $\mathfrak{p} \mapsto S^{-1}\mathfrak{p}$ is a bijection of Φ onto the set of prime ideals of $S^{-1}A$. If $\mathfrak{p} \in \mathrm{Ass}_A(M) \cap \Phi$, $\mathfrak{p}$ is the annihilator of a monogenous submodule N of M; then $S^{-}1\mathfrak{p}$ is the annihilator of the monogenous submodule $S^{-1}\mathbb{N}$ of $S^{-1}M$ (Proposition 10.2.32) and hence $S^{-1}\mathfrak{p} \in \mathrm{Ass}_{S^{-1}A}(S^{-1}M)$. Conversely, suppose that $\mathfrak{p} \in \Phi$ is finitely generated and such that $S^{-1}\mathfrak{p}$ is associated with $S^{-1}M$, then there exists $x \in M$ and $t \in S$ such that $S^{-1}\mathfrak{p}$ is the annihilator of x/t. Let $a_1, \ldots, a_n$ be a system of generators of $\mathfrak{p}$; then $(a_i)(x/t) = 0$ and hence there exists $s_i \in S$ such that $s_i a_i x = 0$. Let us write $s = s_1 \cdots s_n$, then for all $a \in \mathfrak{p}$ we have $sax = 0$, whence $\mathfrak{p} \subseteq \mathrm{Ann}(sx)$. On the other hand, if $b \in A$ satisfies $bsx = 0$, then $b/1 \in S^{-1}\mathfrak{p}$ by definition, whence $b \in \mathfrak{p}$. Then $\mathfrak{p} = \mathrm{Ann}(sx)$ and $\mathfrak{p} \in \mathrm{Ass}_A(M)$. □

Corollary 12.1.12. *If the ring A is Noetherian, the mapping $\mathfrak{p} \mapsto S^{-1}\mathfrak{p}$ is a bijection of $\mathrm{Ass}_A(M) \cap \Phi$ onto $\mathrm{Ass}_{S^{-1}A}(S^{-1}M)$.*

Proposition 12.1.13. *Let A be a Noetherian ring, M an A-module, S a multiplicative subset of A and Φ the set of elements of $\mathrm{Ass}_A(M)$ which do not meet S. Then the kernel N of the canonical mapping $M \mapsto S^{-1}M$ is the unique submodule of M which satisfies the relations*

$$\mathrm{Ass}(N) = \mathrm{Ass}(M) - \Phi, \quad \mathrm{Ass}(M/N) = \Phi.$$

Proof. By Proposition 12.1.10, there exists a submodule N' of M which satisfies the relations $\mathrm{Ass}(N') = \mathrm{Ass}(M) - \Phi$ and $\mathrm{Ass}(M/N') = \Phi$. We need to prove $N' = N$. Consider the commutative diagram

$$\begin{tikzcd} M \arrow[r, "\pi"] \arrow[d, "i_M^S"'] & M/N' \arrow[d, "i^S_{M/N'}"] \\ S^{-1}M \arrow[r, "S^{-1}\pi"] & S^{-1}(M/N') \end{tikzcd}$$

where π, i_M^S, and $i^S_{M/N'}$ are the canonical homomorphisms. We shall show that $S^{-1}\pi$ and $i^S_{M/N'}$ are injective, which will prove that i_M^S and π have the same kernel and hence $N = N'$.

As $\mathrm{Ass}(N') \cap \Phi = \varnothing$, every element of $\mathrm{Ass}(N')$ meets S. Then by Proposition 12.1.11 we have $\mathrm{Ass}_{S^{-1}A}(S^{-1}N') = \varnothing$, whence $S^{-1}N' = \{0\}$ by Corollary 12.1.4. This proves that $S^{-1}\pi$ is injective. On the other hand, if x belongs to the kernel K of $i^S_{M/N'}$, then $\mathrm{Ann}(x) \cap S \neq \varnothing$, so $\mathrm{Ass}(K) \cap \Phi = \varnothing$. But $\mathrm{Ass}(K) \subseteq \mathrm{Ass}(M/N') = \Phi$, which means $\mathrm{Ass}(K) = \varnothing$ and $K = \{0\}$ by Corollary 12.1.4. This shows $i^S_{M/N'}$ is injective. □

12.1.3 Associated prime ideals and supports

Let M be a module over a ring A. Recall that the set of prime ideals $\mathfrak{p}$ of A such that $M_\mathfrak{p} \neq 0$ is called the support of M and is denoted by $\mathrm{supp}(M)$.

Proposition 12.1.14. *Let A be a ring and M an A-module.*

(a) *Every prime ideal* $\mathfrak{p}$ *of* A *containing an element of* $\mathrm{Ass}(M)$ *belongs to* $\mathrm{supp}(M)$.

(b) *Conversely, if* A *is Noetherian, every ideal* $\mathfrak{p} \in \mathrm{supp}(M)$ *contains an element of* $\mathrm{Ass}(M)$.

Proof. If $\mathfrak{p}$ contains an element $\mathfrak{q}$ of $\mathrm{Ass}(M)$, then $\mathfrak{q} \cap (A - \mathfrak{p}) = \varnothing$ and hence, if we write $S = A - \mathfrak{p}$, $S^{-1}\mathfrak{p}$ is a prime ideal associated with $S^{-1}M = M_{\mathfrak{p}}$, and a fortiori $M_{\mathfrak{p}} \neq \varnothing$, hence $\mathfrak{p} \in \mathrm{supp}(M)$. Conversely, if A is Noetherian, so is $A_{\mathfrak{p}}$. If $M_{\mathfrak{p}} \neq \varnothing$, then $\mathrm{Ass}_{A_{\mathfrak{p}}}(M_{\mathfrak{p}}) \neq \varnothing$ and hence there exists $\mathfrak{q} \in \mathrm{Ass}_A(M)$ such that $\mathfrak{q} \cap (A - \mathfrak{p}) = \varnothing$ by Proposition 12.1.11. □

Corollary 12.1.15. *If* M *is a module over a Noetherian ring, then* $\mathrm{Ass}(M) \subseteq \mathrm{supp}(M)$ *and these two sets have the same minimal elements.*

Corollary 12.1.16. *The nilradical of a Noetherian ring* A *is the intersection of the ideals* $\mathfrak{p} \in \mathrm{Ass}(A)$.

12.1.4 Associated prime ideals of modules over Noetherian rings

Proposition 12.1.17. *Let* A *be a Noetherian ring and* M *a finitely generated* A*-module. Then there exists a chain* $(M_i)_{0 \leq i \leq n}$ *of submodules of* M *such that* M_i/M_{i+1} *is isomorphic to* $A/\mathfrak{p}_i$ *where* $\mathfrak{p}_i$ *is a prime ideal of* A.

Proof. Let $\mathcal{M}$ be the set of submodules of M which have a chain with the property of the statement. As $\mathcal{M}$ is non-empty (for $\{0\}$ belongs to $\mathcal{M}$) and M is Noetherian, $\mathcal{M}$ has a maximal element N. If $M \subseteq N$, then $M/N \neq \varnothing$ and hence $\mathrm{Ass}(M/N) \neq \varnothing$ by Corollary 12.1.4. The module M/N therefore contains a submodule N'/N isomorphic to an A-module of the form $A/\mathfrak{p}$, where $\mathfrak{p}$ is prime; then by definition $N' \in \mathcal{M}$, which contradicts the maximal character of N. Then necessarily $N = M$. □

Theorem 12.1.18. *Let* M *be a finitely generated module over a Noetherian ring* A *and* $(M_i)_{0 \leq i \leq n}$ *a chain of submodules of* M *such that* M_i/M_{i+1} *is isomorphic to* $A/\mathfrak{p}_i$ *where* $\mathfrak{p}_i$ *is a prime ideal of* A. *Then*

$$\mathrm{Ass}(M) \subseteq \{\mathfrak{p}_0, \ldots, \mathfrak{p}_{n-1}\} \subseteq \mathrm{supp}(M). \tag{1.4.1}$$

The minimal elements of these three sets are the same and coincide with the minimal elements of the set of prime ideals containing $\mathrm{Ann}(M)$.

Proof. The inclusion $\mathrm{Ass}(M) \subseteq \{\mathfrak{p}_0, \ldots, \mathfrak{p}_{n-1}\}$ follows immediately from Proposition 12.1.7. For each i, we have

$$\mathfrak{p}_i \in \mathrm{supp}(A/\mathfrak{p}_i) = \mathrm{supp}(M_i/M_{i+1})$$

so $\mathfrak{p}_i \in \mathrm{supp}(M_i) \subseteq \mathrm{supp}(M)$ (Proposition 10.4.31), which shows $\{\mathfrak{p}_0, \ldots, \mathfrak{p}_{n-1}\} \subseteq \mathrm{supp}(M)$. Proposition 12.1.14 shows that $\mathrm{Ass}(M)$ and $\mathrm{supp}(M)$ have the same minimal elements and (1.4.1) shows that these are just the minimal elements of $\{\mathfrak{p}_0, \ldots, \mathfrak{p}_{n-1}\}$. The last assertion then follows from Proposition 10.4.33. □

Corollary 12.1.19. *If* M *is a finitely generated module over a Noetherian ring* A, $\mathrm{Ass}(M)$ *is finite.*

Proposition 12.1.20. *Let* A *be a Noetherian ring,* $\mathfrak{a}$ *an ideal of* A *and* M *a finitely generated* A*-module. The following conditions are equivalent:*

(i) *there exists a nonzero element* $x \in M$ *such that* $\mathfrak{a}x = 0$;

(ii) for all $a \in \mathfrak{a}$, there exists a nonzero element $x \in M$ such that $ax = 0$;

(iii) there exists $\mathfrak{p} \in \mathrm{Ass}(M)$ such that $\mathfrak{a} \subseteq \mathfrak{p}$.

Proof. Clearly (i) implies (ii). By virtue of Corollary 12.1.5, condition (ii) means that the ideal $\mathfrak{a}$ is contained in the union of the prime ideals associated with M and hence in one of them since $\mathrm{Ass}(M)$ is finite (Proposition 10.1.4), thus (ii) implies (iii). Finally, if there exists $\mathfrak{p} \in \mathrm{Ass}(M)$ such that $\mathfrak{a} \subseteq \mathfrak{p}$, then $\mathfrak{p}$ is the annihilator of a nonzero element $x \in M$ such that $\mathfrak{a}x = 0$, thus (iii) implies (i). □

Proposition 12.1.21. *Let A be a Noetherian ring, $\mathfrak{a}$ an ideal of A and M a finitely generated A-module. For there to exist an integer $n > 0$ such that $\mathfrak{a}^n M = 0$, it is necessary and sufficient that $\mathfrak{a}$ be contained in the intersection of the prime ideals associated with M.*

Proof. This intersection is also that of the minimal elements of $\mathrm{supp}(M)$ and to say that $\mathfrak{a}$ is contained in this intersection is equivalent to saying that $V(\mathfrak{a}) \supseteq \mathrm{supp}(M)$. The conclusion then follows from Corollary 10.4.35. □

Given an A-module M, an endomorphism ϕ of M is called **locally nilpotent** if, for all $x \in M$, there exists an integer $n(x) > 0$ such that $\phi(x)^{n(x)} = 0$. It is clear that, if M is finitely generated, every locally nilpotent endomorphism is nilpotent.

Corollary 12.1.22. *Let A be a Noetherian ring, M an A-module and a an element of A. For the homomorphism $h_a : x \mapsto ax$ of M to be locally nilpotent, it is necessary and suficient that a belong to every ideal of* $\mathrm{Ass}(M)$.

Proof. The condition of the statement is equivalent to saying that for all $x \in M$ there exists $n(x) > 0$ such that $(Aa)^{n(x)}(Ax) = 0$. By Proposition 12.1.21 this means also that a belongs to all the prime ideals associated with the submodule Ax of M. The corollary then follows from the fact that $\mathrm{Ass}(M)$ is the union of the $\mathrm{Ass}(Ax)$ where x runs through M. □

Proposition 12.1.23. *Let A be a Noetherian ring, M a finitely generated A-module and N an A-module. Then*

$$\mathrm{Ass}(\mathrm{Hom}_A(M, N)) = \mathrm{Ass}(N) \cap \mathrm{supp}(M).$$

Proof. By hypothesis, M is isomorphic to an A-module of the form A^n/R, hence $\mathrm{Hom}_A(M, N)$ is isomorphic to a submodule of $\mathrm{Hom}_A(A^n, N)$ and the latter is isomorphic to N^n. Now, $\mathrm{Ass}(N^n) = \mathrm{Ass}(N)$ by Corollary 12.1.8, thus $\mathrm{Ass}(\mathrm{Hom}_A(M, N)) \subseteq \mathrm{Ass}(N)$. On the other hand, for every prime ideal $\mathfrak{p}$ of A, $\mathrm{Hom}_{A_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p})$ is isomorphic to $(\mathrm{Hom}_A(M, N))_\mathfrak{p}$ by Proposition 10.2.46

$$\mathrm{supp}(\mathrm{Hom}_A(M, N)) \subseteq \mathrm{supp}(M).$$

Then we conclude from Theorem 12.1.18 that $\mathrm{Ass}(\mathrm{Hom}_A(M, N)) \subseteq \mathrm{supp}(M)$.

Conversely, let $\mathfrak{p}$ be a prime ideal of A belonging to $\mathrm{Ass}(N) \cap \mathrm{supp}(M)$. By definition, N contains a submodule isomorphic to $A/\mathfrak{p}$. On the other hand, since M is finitely generated and $M_\mathfrak{p} \neq 0$, we know that there exists a nonzero homomorphism $\eta : M \to A/\mathfrak{p}$ (Proposition 10.4.41). As there exists an injective homomorphism $\iota : A/\mathfrak{p} \to N$, we have $\iota \circ \eta \in \mathrm{Hom}(M, N)$ and it is nonzero. On the other hand, since the annihilator of every nonzero element of $A/\mathfrak{p}$ is $\mathfrak{p}$, we see $\mathrm{Ann}(\iota \circ \eta) = \mathfrak{p}$, whence $\mathfrak{p} \in \mathrm{Ass}(\mathrm{Hom}_A(M, N))$. □

12.2 Primary decomposition

12.2.1 Primary submodules

Proposition 12.2.1. *Let A be a Noetherian ring and M an A-module. Then the following conditions are equivalent:*

(i) $\mathrm{Ass}(M)$ *is reduced to a single element.*

(ii) $M \neq 0$ *and every homothety of M is either injective or locally nilpotent.*

If these conditions are fulfilled and $\mathfrak{p}$ is the set of $a \in A$ such that the homothety of ratio a is locally nilpotent, then $\mathrm{Ass}(M) = \{\mathfrak{p}\}$.

Proof. This follows from Corollary 12.1.22 and Corollary 12.1.5. □

Let A be a Noetherian ring, M an A-module and N a submodule of N. If the module M/N satisfies the conditions of Proposition 12.2.1, N is called **$\mathfrak{p}$-primary** with respect to M (or in M).

In particular consider the case $M = A$, where the submodules of M are then the ideals of A and hence an ideal $\mathfrak{q}$ of A is called primary if $\mathrm{Ass}(A/\mathfrak{q})$ has a single element or, what amounts to the same, *if $A \neq \mathfrak{q}$ and every divisor of zero in the ring $A/\mathfrak{q}$ is nilpotent*. If $\mathfrak{q}$ is $\mathfrak{p}$-primary, then since $\mathrm{supp}(A/\mathfrak{q}) = V(\mathrm{Ann}(A/\mathfrak{q})) = V(\mathfrak{q})$, by Theorem 12.1.18 $\mathfrak{p}$ is the radical of the ideal $\mathfrak{q}$.

Example 12.2.2 (Example of primary submodules).

(a) If $\mathfrak{p}$ is a prime ideal of A, then $\mathfrak{p}$ is $\mathfrak{p}$-primary.

(b) Let $\mathfrak{q}$ be an ideal of A such that there exists a single prime ideal $\mathfrak{m}$ (necessarily maximal) containing $\mathfrak{q}$. Then, if M is an A-module such that $\mathfrak{q}M \neq M$, $\mathfrak{q}M$ is $\mathfrak{m}$-primary with respect to M, for every element of $\mathrm{Ass}(M/\mathfrak{q}M)$ contains $\mathfrak{q}$, hence is equal to $\mathfrak{m}$ and $\mathrm{Ass}(M/\mathfrak{q}M) \neq \varnothing$. In particular we see $\mathfrak{q}$ is an $\mathfrak{m}$-primary ideal in A.

(c) Let $\mathfrak{m}$ be a maximal ideal of a Noetherian ring A. Then the $\mathfrak{m}$-primary ideals are the ideals $\mathfrak{q}$ of A for which there exists an integer $n > 0$ such that $\mathfrak{m}^n \subseteq \mathfrak{q} \subseteq \mathfrak{m}$, for if $\mathfrak{m}^n \subseteq \mathfrak{q} \subseteq \mathfrak{m}$, then $\mathfrak{m}$ is the only prime ideal containing $\mathfrak{q}$ and the conclusion follows from (b). Conversely, if $\mathfrak{q}$ is $\mathfrak{m}$-primary, then $\mathfrak{m}$ is the radical of $\mathfrak{q}$ and there therefore exists $n > 1$ such that $\mathfrak{m}^n \subseteq \mathfrak{q}$ by Proposition 6.2.3. In particular, if A is a PID then the primary ideals are (0) and the ideals of the form (p^n), where p is a prime element and $n > 0$.

Remark 12.2.1. The powers of any prime ideal are not necessarily primary ideals. For an example, let K be a field and A the quotient ring of $K[X, Y, Z]/(Z^2 - XY)$. Let x, y, z be the canonical images of X, Y, Z in A. Then the ideal $\mathfrak{p} = (x, z)$ is prime, since $A/\mathfrak{p} \cong K[X]$. Note that $\mathfrak{p}^2 = (x^2, z^2, xz) = (x^2, xy, xz)$ is not primary, since $x \notin \mathfrak{p}^2$, $y \notin \mathfrak{p}$ but $xy \in \mathfrak{p}^2$. Also, we have the following decomposition

$$\mathfrak{p}^2 = (x) \cap (x, y, z^2)$$

On the other hand, there exist primary ideals which are not powers of prime ideals. For example, consider the ring $A = \mathbb{Z}[X]$ and the maximal ideal $\mathfrak{m} = (2, X)$. The ideal $\mathfrak{q} = (4, X)$ is $\mathfrak{m}$-primary since $\sqrt{\mathfrak{q}} = \mathfrak{m}$, but it is not a power of $\mathfrak{m}$.

Proposition 12.2.3. *Let M be a module over a Noetherian ring A, $\mathfrak{p}$ a prime ideal of A and $(Q_i)_{i\in I}$ a non-empty finite family of submodules of M which are $\mathfrak{p}$-primary with respect to M. Then $\bigcap_{i\in I} Q_i$ is $\mathfrak{p}$-primary with respect to M.*

Proof. The quotient $M/(\bigcap_i Q_i)$ is isomorphic to a submodule of the direct sum $\bigoplus_i (M_i/Q_i)$. Now $\mathrm{Ass}(\bigoplus_i (M_i/Q_i)) = \bigcup_i \mathrm{Ass}(M_i/Q_i) = \{\mathfrak{p}\}$, whence $\mathrm{Ass}(M/(\bigcap_i Q_i)) = \{\mathfrak{p}\}$ and $\bigcap_i Q_i$ is $\mathfrak{p}$-primary. □

Proposition 12.2.4. *Let A be a Noetherian ring, S a multiplicative subset of A, $\mathfrak{p}$ a prime ideal of A, M an A-module, N a submodule of M and i_M^S the canonical mapping of M to $S^{-1}M$.*

(a) Suppose that $\mathfrak{p} \cap S \neq \varnothing$. If N is $\mathfrak{p}$-primary with respect to M, then $S^{-1}N = S^{-1}M$.

(b) Suppose that $\mathfrak{p} \cap S = \varnothing$. Then for N to be $\mathfrak{p}$-primary with respect to M, it is necessary and sufficient that N be of the form $(i_M^S)^{-1}(N')$, where N' is a sub-$S^{-1}A$-module of $S^{-1}M$ which is $(S^{-1}\mathfrak{p})$-primary with respect to $S^{-1}M$. In this case we have $N' = S^{-1}N$.

Proof. If $\mathfrak{p} \cap S \neq \varnothing$ and N is $\mathfrak{p}$-primary with respect to M, then

$$\mathrm{Ass}_{S^{-1}A}(S^{-1}(M/N)) = \varnothing$$

and hence $S^{-1}(M/N) = 0$, whence $S^{-1}N = S^{-1}M$.

Suppose that $\mathfrak{p} \cap S = \varnothing$. If N is $\mathfrak{p}$-primary with respect to M, then $\mathrm{Ass}_{S^{-1}A}(S^{-1}(M/N)) = \{S^{-1}\mathfrak{p}\}$ and hence the submodule $N' = S^{-1}N$ of $S^{-1}M$ is $(S^{-1}\mathfrak{p})$-primary. Moreover, if $s \in S$ and $m \in M$ are such that $sm \in N$, then $m \in N$, for the homothety with ratio s in M/N is injective, whence $N = (i_M^S)^{-1}(N')$.

Conversely, let N' be a submodule of $S^{-1}M$ which is $(S^{-1}\mathfrak{p})$-primary with respect to $S^{-1}M$. Let us write $N = (i_M^S)^{-1}(N')$, then $N' = S^{-1}N$ and

$$\mathrm{Ass}_{S^{-1}A}(S^{-1}(M/N)) = \mathrm{Ass}_{S^{-1}A}((S^{-1}M)/N') = \{S^{-1}\mathfrak{p}\}.$$

Since N is saturated, the canonical mapping $M/N \to S^{-1}(M/N)$ is injective, whence no prime ideal of A associated with M/N meets S (Proposition 12.1.13). It then follows that $\mathrm{Ass}(M/N) = \{\mathfrak{p}\}$, so that N is $\mathfrak{p}$-primary with respect to M. □

12.2.2 Primary decompositions

Let A be a Noetherian ring, M an A-module and N a submodule of M. A finite family $(Q_i)_{i\in I}$ of submodule of M which are primary with respect to M and such that $N = \bigcap_i Q_i$ is called a **primary decomposition** of N in M.

Example 12.2.5. Let us take $A = \mathbb{Z}$, $M = \mathbb{Z}$, $N = (n)$ for some integer $n > 0$. If $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ is the decomposition of n into prime factors, then

$$(n) = (p_1^{\alpha_1}) \cap \cdots \cap (p_k^{\alpha_k})$$

is a primary decomposition of (n) in $\mathbb{Z}$.

By an abuse of language, the relation $N = \bigcap_{i\in I} Q_i$ is called a primary decomposition of N in M. It amounts to the same to say that $\{0\} = \bigcap_{i\in I}(Q_i/N)$ is a primary decomposition of $\{0\}$

in M/N. If $(Q_i)_{i\in I}$ is a primary decomposition of N in M, the canonical mapping from M/N to $\bigcap_{i\in I}(M/Q_i)$ is injective. Conversely let N be a submodule of M and ϕ an injective homomorphism from M/N to a finite direct sum $P = \bigoplus_i P_i$, where each set $\mathrm{Ass}(P_i)$ is reduced to a single element $\mathfrak{p}_i$. Let ϕ_i be the homomorphism $M/N \to P_i$ obtained by taking the composition off with the projection $P \to P_i$, and let Q_i/N be the kernel of ϕ_i; then the Q_i distinct from M are primary with respect to M and $N = \bigcap_{i\in I} Q_i$. Moreover, $\mathrm{Ass}(M/N) \subseteq \bigcup_{i\in I}\{\mathfrak{p}_i\}$ by virtue of Proposition 12.1.7.

Theorem 12.2.6. *Let M be a finitely generated module over a Noetherian ring and let N be a submodule of M. Then there exists a primary decomposition of N of the form*

$$N = \bigcap_{\mathfrak{p}\in\mathrm{Ass}(M/N)} Q(\mathfrak{p}) \tag{2.2.1}$$

where for each $\mathfrak{p} \in \mathrm{Ass}(M/N)$, $Q(\mathfrak{p})$ is $\mathfrak{p}$-primary with respect to M.

Proof. We may replace M by M/N and therefore suppose that $N = 0$. By Corollary 12.1.19, $\mathrm{Ass}(M)$ is finite. By Proposition 12.1.10, there exists, for each $\mathfrak{p} \in \mathrm{Ass}(M)$, a submodule $Q(\mathfrak{p})$ of M such that $\mathrm{Ass}(M/Q(\mathfrak{p})) = \{\mathfrak{p}\}$ and $\mathrm{Ass}(Q(\mathfrak{p})) = \mathrm{Ass}(M) - \{\mathfrak{p}\}$. Let us write $P = \bigcap_{\mathfrak{p}\in\mathrm{Ass}(M)} Q(\mathfrak{p})$. For all $\mathfrak{p} \in \mathrm{Ass}(M)$, $\mathrm{Ass}(P) \subseteq \mathrm{Ass}(Q(\mathfrak{p}))$ and hence $\mathrm{Ass}(P) = \{\mathfrak{p}\}$, which implies $P = 0$ and therefore proves the theorem. □

Definition 12.2.7. *Let M be a module over a Noetherian ring and N a submodule of M. A primary decomposition $N = \bigcap_{i\in I} Q_i$ of N in M is called **reduced** if the following conditions are fulfilled:*

(a) there exists no index $i \in I$ such that $\bigcap_{j\neq i} Q_j \subseteq Q_i$;

(b) if $\mathrm{Ass}(M/Q_i) = \{\mathfrak{p}_i\}$, the $\mathfrak{p}_i$'s are distinct.

From every primary decomposition $N = \bigcap_{i\in I} Q_i$ of N in M a reduced primary decomposition of M in N can be deduced as follows: let J be a minimal element of the set of subsets I' of I such that $N = \bigcap_{i\in I'} Q_i$. Clearly $(Q_i)_{i\in J}$ satisfies condition (a). Then let Φ be the set of $\mathfrak{p}_i$ for $i \in J$. For all $\mathfrak{p} \in \Phi$, let $H(\mathfrak{p})$ be the set of $i \in J$ such that $\mathfrak{p}_i = \mathfrak{p}$ and let $Q(\mathfrak{p}) = \bigcap_{i\in H(\mathfrak{p})} Q_i$. It follows from Proposition 12.2.3 that $Q(\mathfrak{p})$ is $\mathfrak{p}$-primary with respect to M; further $N = \bigcap_{\mathfrak{p}\in\Phi} Q(\mathfrak{p})$ and the family $(Q(\mathfrak{p}))_{\mathfrak{p}\in\Phi}$ is therefore a reduced primary decomposition of N in M.

Proposition 12.2.8. *Let M be a module over a Noetherian ring, N a submodule of M, $N = \bigcap_{i\in I} Q_i$ a primary decomposition of N in M and, for all $i \in I$, let $\{\mathfrak{p}_i\} = \mathrm{Ass}(M/Q_i)$. For this decomposition to be reduced, it is necessary and sufficient that the $\mathfrak{p}_i$ be distinct and belong to $\mathrm{Ass}(M/N)$. In this case, we have*

$$\mathrm{Ass}(M/N) = \bigcup_{i\in I} \mathfrak{p}_i, \quad \mathrm{Ass}(Q_i/N) = \bigcup_{j\neq i}\{\mathfrak{p}_i\} \quad \textit{for all } i \in I. \tag{2.2.2}$$

Proof. If the condition of the statement is fulfilled, $N = \bigcap_{j\neq i} Q_j$ cannot hold, for we would deduce that $\mathrm{Ass}(M/N) \subseteq \bigcup_{j\neq i}\{\mathfrak{p}_j\}$ by Corollary 12.1.9, contrary to the hypothesis. The primary decomposition $(Q_i)_{i\in I}$ of N is then certainly reduced.

Conversely, assume that $(Q_i)_{i\in I}$ is reduced. Note that $\mathrm{Ass}(M/N) \subseteq \bigcup_{i\in I}\{\mathfrak{p}_i\}$ always holds by Corollary 12.1.9. On the other hand, for all $i \in I$, let us write $P_i = \bigcap_{j\neq i} Q_j$. Then $P_i \cap Q_i = N$

and $P_i \neq N$ if $(Q_i)_{i\in I}$ is reduced, hence P_i/N is non-zero and is isomorphic to the submodule $(P_i+Q_i)/Q_i$ of M/Q_i, whence $\{\mathfrak{p}_i\} = \mathrm{Ass}(P_i/N)$ by Proposition 12.1.7. As $P_i/N \subseteq M/N$, we get $\mathfrak{p}_i \in \mathrm{Ass}(M/N)$, which completes the proof of the necessity of the condition in the statement and the first formula of (2.2.2). Finally, for each $i \in I$, as $N = \bigcap_{j\neq i}(Q_i \cap Q_j)$, by Corollary 12.1.9 we have

$$\mathrm{Ass}(Q_i/N) \subseteq \bigcup_{j\neq i} \mathrm{Ass}(Q_i/(Q_i \cap Q_j)) = \bigcup_{j\neq i} \mathrm{Ass}((Q_i + Q_j)/Q_j) \subseteq \bigcup_{j\neq i}\{\mathfrak{p}_j\}.$$

Taking account of the first formula of (2.2.2) and Proposition 12.1.7, the second formula of (2.2.2) follows easily. □

Corollary 12.2.9. *Let A be a Noetherian ring, M an A-module, N a submodule of M and $(Q_i)_{i\in I}$ a primary decomposition of N in M. Then $|I| \geq |\mathrm{Ass}(M/N)|$, and the equality holds if and only if $(Q_i)_{i\in I}$ is reduced.*

Proof. It follows from the remarks preceding Proposition 12.2.8 that there exists a reduced primary decomposition $(R_i)_{i\in J}$ of N in M such that $\mathrm{Card}(J) \subseteq \mathrm{Card}(I)$. The first assertion then follows from the second and the latter is a consequence of Proposition 12.2.8. □

Proposition 12.2.10. *Let A be a Noetherian ring, M an A-module and N a submodule of M. Let $N = \bigcap_{i\in I} Q_i$ be a reduced primary decomposition of N where Q_i is $\mathfrak{p}_i$-primary. If $\mathfrak{p}_i$ is a minimal element of $\mathrm{Ass}(M/N)$, then Q_i is equal to the saturation on N with respect to $\mathfrak{p}_i$.*

Proof. We can obviously restrict our attention to the case where $N = 0$, replacing if need be M by M/N. If $\mathfrak{p}_i$ is minimal in $\mathrm{Ass}(M)$, then the set of elements of $\mathrm{Ass}(M)$ which do not meet $A - \mathfrak{p}_i$ reduces to $\mathfrak{p}_i$. The proposition then follows from the second formula of (2.2.2) above and Proposition 12.1.13, since the kernel of the canonical mapping $M \mapsto M_{\mathfrak{p}_i}$ equals to the saturation of 0 with respect to $\mathfrak{p}_i$. □

The minimal elements of $\mathrm{Ass}(M/N)$ are called the **minimal** or **isolated prime ideals** associated with M/N, and the prime ideals $\mathfrak{p} \in \mathrm{Ass}(M/N)$ which are not minimal are called the **embedded prime ideals** associated with M/N. If M/N is finitely generated, then by Corollary 12.1.15 we know the isolated ideals of M/N are just the minimal prime ideals containing $\mathrm{supp}(M/N) = V(\mathrm{Ann}(M/N))$, so for $\mathfrak{p} \in \mathrm{Ass}(M/N)$ to be embedded, it is necessary and sufficient that $V(\mathfrak{p})$ be not an irreducible component of $\mathrm{supp}(M/N)$.

If $(Q(\mathfrak{p}))$ and $(R(\mathfrak{p}))$ are two reduced primary decompositions of N in M, then by Proposition 12.2.10 we see $Q(\mathfrak{p}) = R(\mathfrak{p})$ if $\mathfrak{p}$ is an isolated prime associated with M/N, being the saturation of N with respect to $\mathfrak{p}$. However, it may happen that $Q(\mathfrak{p}) \neq R(\mathfrak{p})$ for $\mathfrak{p}$ an embedded prime, as the following example shows.

Example 12.2.11. Consider the ring $A = K[X, Y]$ where K is a field. Then for every positive integer n, a primary decomposition of the ideal $\mathfrak{a} = (X^2, XY)$ is

$$(X^2, XY) = (X) \cap (X^2, XY, Y^n)$$

where (X) is prime and (X^2, XY, Y^n) is (X, Y)-primary. Note that (X) is isolated and (X, Y) is embedded.

12.2.3 The localization of a primary decomposition

Given a submodule N of a module M over a Noetherian ring A, to simplify we shall denote by $D_I(M/N)$, in this part, the set of reduced primary decompositions of N in M whose indexing set is I.

Proposition 12.2.12. *Let A be a Noetherian ring, M an A-module, N a submodule of M and $I = \mathrm{Ass}(M/N)$. Let S be a multiplicative subset of A and I_S the subset I consisting of the indices i such that $S \cap \mathfrak{p}_i = \varnothing$. Let $\phi(N)$ be the saturation of N with respect to S in M. Then:*

(a) If $(Q_i)_{i\in I}$ is an element of $D_I(M/N)$, the family $(Q_i)_{i\in I_S}$ is an element of $D_{I_S}(M/\phi(N))$ and the family $(S^{-1}Q_i)_{i\in I_S}$ is an element of $D_{I_S}(S^{-1}M/S^{-1}N)$.

(b) The map $(Q_i)_{i\in I_S} \mapsto (S^{-1}Q_i)_{i\in I_S}$ is a bijection from $D_{I_S}(M/\phi(N))$ to $D_{I_S}(S^{-1}M/S^{-1}N)$.

(c) If $(Q_i)_{i\in I_S}$ is an element of $D_{I_S}(M/\phi(N))$ and $(R_i)_{i\in I}$ is an element of $D_I(M/N)$, then the family $(T_i)_{i\in I}$ defined by $T_i = Q_i$ when $i \in I_S$ and $T_i = R_i$ for $i \in I - I_S$ is an element of $D_I(M/N)$.

Proof. We know that for $i \in I_S$, $S^{-1}Q_i$ is $S^{-1}\mathfrak{p}_i$-primary and that for $i \in I - I_S$, $S^{-1}Q_i = S^{-1}M$. As $S^{-1}N = \bigcap_{i\in I} S^{-1}Q_i$, we see $S^{-1}N = \bigcap_{i\in I_S} S^{-1}Q_i$. The ideals $S^{-1}\mathfrak{p}_i$ for $i \in I_S$ are distinct and their set is $\mathrm{Ass}(S^{-1}M/S^{-1}N)$ by Proposition 12.1.11. Then by Proposition 12.2.8 $(S^{-1}Q_i)_{i\in I_S}$ is a reduced primary decomposition of $S^{-1}N$. Moreover, Q_i is saturated for $i \in I_S$, hence $\phi(N) = (i_M^S)^{-1}(S^{-1}N) = \bigcap_{i\in I_S} Q_i$, and $(Q_i)_{i\in I_S}$ is obviously a reduced primary decomposition of $\phi(N)$ in M.

As $S^{-1}\phi(N) = S^{-1}N$, we may replace N by $\phi(N)$ and suppose that $I = I_S$. Let $(P_i)_{i\in I}$ be a reduced primary decomposition Of $S^{-1}N$ in $S^{-1}M$ and let us write $Q_i = (i_M^S)^{-1}(P_i)$. It follows from Proposition 12.2.4 that Q_i is $\mathfrak{p}_i$-primary and $(Q_i)_{i\in I}$ then a reduced primary decomposition of N of M by virtue of Corollaries 12.2.9. Finally, since $I = I_S$, by Proposition 12.2.4 we see every $\mathfrak{p}_i$-primary submodule of M is saturated, so the two maps

$$D_I(M/N) \to D_I(S^{-1}M/S^{-1}N) \quad \text{and} \quad D_I(S^{-1}M/S^{-1}N) \to D_I(M/N)$$

are inverse of each other, which proves (b).

Finally, we prove (c). From (a) we have $\phi(N) = \bigcap_{i\in I_S} R_i$, whence

$$N = \phi(N) \cap \bigcap_{i\in I-I_S} R_i = \Big(\bigcap_{i\in I_S} Q_i\Big) \cap \Big(\bigcap_{i\in I-I_S} R_i\Big)$$

and it follows immediately from Corollary 12.2.9 that this primary decomposition is reduced. □

Corollary 12.2.13. *The maps*

$$D_I(M/N) \to D_{I_S}(M/\phi(N)) \quad \textit{and} \quad D_I(M/N) \to D_{I_S}(S^{-1}M/S^{-1}N)$$

defined in Proposition 12.2.12 are surjective.

Proof. Proposition 12.2.12(c) shows that the map $D_I(M/N) \to D_{I_S}(M/\phi(N))$ is suijective and Proposition 12.2.12(b) then shows that $D_I(M/N) \to D_{I_S}(M/N) \to D_{I_S}(S^{-1}M/S^{-1}N)$ is surjective. □

12.2.4 Module of finite length

If an A-module M is of finite length, we shall denote this length by $\ell_A(M)$ or $\ell(M)$. Recall that every Artinian ring is Noetherian and that every finitely generated module over an Artinian ring is of finite length.

Proposition 12.2.14. *Let M be a finitely generated module over a Noetherian ring A. The following properties are equivalent:*

(i) M is of finite length.

(ii) Every ideal $\mathfrak{p} \in \mathrm{Ass}(M)$ is a maximal ideal of A.

(iii) Every ideal $\mathfrak{p} \in \mathrm{supp}(M)$ is a maximal ideal of A.

Proof. Let (M_i) be a chain of submodules of M such that M_i/M_{i+1} is isomorphic to $A/\mathfrak{p}_i$ where $\mathfrak{p}_i$ is prime. If M is of finite length, so is each of the A-modules $A/\mathfrak{p}_i$, which implies that each of the rings $A/\mathfrak{p}_i$ is Artinian. But as $A/\mathfrak{p}_i$ is an integral domain, it is therefore a field, in other words $\mathfrak{p}_i$ is maximal; we conclude that (i) implies (ii). Condition (ii) implies (iii) by Proposition 12.1.14. Finally, if all the ideals of $\mathrm{supp}(M)$ are maximal, so are the $\mathfrak{p}_i$, hence the $A/\mathfrak{p}_i$ are simple A-modules and M is of finite length, which completes the proof. □

Corollary 12.2.15. *For every module of finite length M over a Noetherian ring A, $\mathrm{Ass}(M) = \mathrm{supp}(M)$.*

Proof. Every element of $\mathrm{supp}(M)$ is then minimal in $\mathrm{supp}(M)$ and the conclusion follows from Corollary 12.1.15. □

Corollary 12.2.16. *Let M be a finitely generated module over a Noetherian ring A and $\mathfrak{p}$ a prime ideal of A. For $M_\mathfrak{p}$ to be a non-zero $A_\mathfrak{p}$-module of finite length, it is necessary and sufficient that $\mathfrak{p}$ be a minimal element of $\mathrm{Ass}(M)$.*

Proof. By Proposition 12.1.11, $\mathrm{Ass}_{A_\mathfrak{p}}(M_\mathfrak{p})$ is the set of ideals $\mathfrak{q}_\mathfrak{p}$, where $\mathfrak{q}$ runs through the set of ideals of $\mathrm{Ass}(M)$ which are contained in $\mathfrak{p}$. Thus by Proposition 12.2.14, for $M_\mathfrak{p}$ to be an $A_\mathfrak{p}$-module of finite length, it is necessary and sufficient that no element of $\mathrm{Ass}(M)$ be strictly contained in $\mathfrak{p}$. On the other hand, for $M_\mathfrak{p} \neq 0$, it is necessary and sufficient by definition that $\mathfrak{p} \in \mathrm{supp}(M)$, that is that $\mathfrak{p}$ contain an element of $\mathrm{Ass}(M)$. This proves the corollary. □

Remark 12.2.2. Let M be a finitely generated module over a Noetherian ring A and let (M_i) be a chain of M such that M_i/M_{i+1} is isomorphic to $A/\mathfrak{p}_i$ where $\mathfrak{p}_i$ is a prime ideal of A. If $\mathfrak{p}$ is a minimal element of $\mathrm{Ass}(M)$, the modules $(M_i)_\mathfrak{p}$ then form a chain of $M_\mathfrak{p}$ and $(M_i)_\mathfrak{p}/(M_{i+1})_\mathfrak{p}$ is isomorphic to $(A/\mathfrak{p}_i)_\mathfrak{p}$ and hence to $\{0\}$ if $\mathfrak{p}_i \neq \mathfrak{p}$, and to $(A/\mathfrak{p})_\mathfrak{p}$ which is a field, if $\mathfrak{p}_i = \mathfrak{p}$.

Proposition 12.2.17. *Let M be a module of finite length over a Noetherian ring A.*

(a) There exists a unique primary decomposition $\{0\} = \bigcap_{\mathfrak{p}\in\mathrm{Ass}(M)} Q(\mathfrak{p})$ of $\{0\}$ with respect to M indexed by $\mathrm{Ass}(M)$, where $Q(\mathfrak{p})$ is $\mathfrak{p}$-primary with respect to M.

(b) There exists an integer n_0 such that, for all $n \geq n_0$ and all $\mathfrak{p} \in \mathrm{Ass}(M)$, $Q(\mathfrak{p}) = \mathfrak{p}^n M$.

(c) For all $\mathfrak{p} \in \mathrm{Ass}(M)$, the canonical mapping of M to $M_\mathfrak{p}$ is surjective and its kernel is $Q(\mathfrak{p})$. Therefore $M_\mathfrak{p}$ can be identified with $M/Q(\mathfrak{p})$.

(d) The canonical injection of M into $\bigoplus_{\mathfrak{p}\in\mathrm{Ass}(M)}(M/Q(\mathfrak{p}))$ is bijective.

Proof. Since each ideal of M is maximal, part (a) follows from Proposition 12.2.10. As $M/Q(\mathfrak{p})$ is finitely generated, by Proposition 12.1.21 there exists $n_0 > 0$ such that $\mathfrak{p}^n M \subseteq Q(\mathfrak{p})$ for all $n \geq n_0$. But as $\mathfrak{p}$ is a maximal ideal, $\mathfrak{p}^n M$ is $\mathfrak{p}$-primary with respect to M and, as $\bigcap_{\mathfrak{p}\in\mathrm{Ass}(M)} \mathfrak{p}^n M = \{0\}$, it follows from (a) that necessarily $\mathfrak{p}^n M = Q(\mathfrak{p})$ for all $\mathfrak{p} \in \mathrm{Ass}(M)$, whence (b) follows. As the $\mathfrak{p}^n$, for $\mathfrak{p} \in \mathrm{Ass}(M)$, are relatively prime in pairs, the canonical mapping $M \mapsto \bigoplus_{\mathfrak{p}\in\mathrm{Ass}(M)}(M/\mathfrak{p}^n M)$ is suijective, whence (d).

Now $\mathrm{Ass}(Q(\mathfrak{p})) = \mathrm{Ass}(M) - \{\mathfrak{p}\}$ and $\mathrm{Ass}(M/Q(\mathfrak{p})) = \{\mathfrak{p}\}$. As the elements of Ass(M) are maximal ideals, $\mathfrak{p}$ is the only element of $\mathrm{Ass}(M)$ which does not meet $A - \mathfrak{p}$. Then $Q(\mathfrak{p})$ is the kernel of the canonical mapping $i_{\mathfrak{p}} : M \to M_{\mathfrak{p}}$ by Proposition 12.1.10. If $s \in A - \mathfrak{p}$, the homothety of $M/Q(\mathfrak{p})$ with ratio s isinjective by virtue of the relation $\mathrm{Ass}(M/Q(\mathfrak{p})) = \{\mathfrak{p}\}$. Since $M/Q(\mathfrak{p})$ is Artinian, this homothety is bijective. Therefore, if $m \in M$ and $s \in A - \mathfrak{p}$, then there exists $n \in M$ such that $\bar{m} = s\bar{n}$ in $M/Q(\mathfrak{p})$, whence $m - ns \in Q(\mathfrak{p})$. By the characterization of $M_{\mathfrak{p}}$, we can then find $t \in A - \mathfrak{p}$ such that $t(m - ns) = 0$, that is, $m/s = n/1$ in $M_{\mathfrak{p}}$. This proves the canonical map $M \to M_{\mathfrak{p}}$ is surjective and finishes the proof. □

Corollary 12.2.18. *If M is a module of finite length over a Noetherian ring A, then*

$$\ell_A(M) = \sum_{\mathfrak{p}\in\mathrm{Ass}(M)} \ell_{A_{\mathfrak{p}}}(M_{\mathfrak{p}}).$$

Proof. This will follow from Proposition 12.2.17(d) if we prove that

$$\ell_A(M/Q(\mathfrak{p})) = \ell_{A_{\mathfrak{p}}}(M_{\mathfrak{p}}).$$

Now, since $\mathrm{Ass}(M/Q(\mathfrak{p})) = \{\mathfrak{p}\}$, for all $s \in A - \mathfrak{p}$ the homothety with ratio s on $M/Q(\mathfrak{p})$ is injective; the homothety with ratio s on every submodule N of $M/Q(\mathfrak{p})$ is therefore injective and, as N is Artinian, it is bijective. We conclude that the sub-A-modules of $M/Q(\mathfrak{p})$ are the images under the bijection $M_{\mathfrak{p}} \to M/Q(\mathfrak{p})$ of the sub-$A_{\mathfrak{p}}$-modules of $M_{\mathfrak{p}}$, whence our assertion. □

Proposition 12.2.19. *Let A be a Noetherian ring. The following conditions are equivalent:*

(i) A is Artinian.

(ii) All the prime ideals of A are maximal ideals.

(iii) All the prime ideals of $\mathrm{Ass}(A)$ *are maximal ideals.*

If these conditions are fulfilled, A has only a finite number prime ideals, which are all maximal and associated with the A-module A. Further, A is a semi-local ring and its Jacobson radical is nilpotent.

Proof. To say that A is Artinian is equivalent to saying that A is an A-module of finite length, hence (i) and (ii) are equivalent by Proposition 12.2.14. We already know that (i) and (ii) are equivalent by Proposition 6.3.7.

Suppose they hold. As every prime ideal of A belongs to $\mathrm{supp}(A)$ and every element of $\mathrm{supp}(A)$ contains an element of $\mathrm{Ass}(A)$, it follows from (iii) that $\mathrm{Ass}(A)$ is the set ofall prime ideals of A. Then A has only a finite number of prime ideals, all of them maximal and associated with the A-module A. Finally, we know that the Jacobson radical of an Artinian ring is nilpotent. □

Corollary 12.2.20. *Every Artinian ring A is isomorphic to the direct composition of a finite family of Artinian local rings.*

Proof. It follows from Proposition 12.2.19 and Proposition 12.2.17 (c) and (d) that, if $(\mathfrak{m}_i)$ is the family of maximal ideals of A, the canonical mapping $A \to \prod_i A_{\mathfrak{m}_i}$ is bijective. □

Corollary 12.2.21. *Let A be a Noetherian ring and $\mathfrak{a}$ an ideal of A. The following conditions are equivalent:*

(i) A is a semi-local ring and $\mathfrak{a}$ is a defining ideal of A.

(ii) A is a Zariski ring with the $\mathfrak{a}$-adic topology and $A/\mathfrak{a}$ is Artinian.

Proof. If (a) holds then by Example 11.4.26 we know A is a Zariski ring with the $\mathfrak{r}$-adic topology, where $\mathfrak{r}$ is the Jacobson radical of A. Moreover, as by hypothesis $\mathfrak{a}$ contains a power of $\mathfrak{r}$, every prime ideal of A which contains $\mathfrak{a}$ also contains $\mathfrak{r}$ and is therefore maximal, since $\mathfrak{r}$ is a finite intersection of maximal ideals. This shows that $A/\mathfrak{a}$ is Artinian.

Conversely, if (b) holds, then $\mathfrak{a} \subseteq \mathfrak{r}$, so every maximal ideal $\mathfrak{p}$ of A containing $\mathfrak{r}$ must contain $\mathfrak{a}$. As $A/\mathfrak{a}$ is Artinian, the ideals $\mathfrak{p}/\mathfrak{a}$ are finite in number (Proposition 12.2.19) and hence A has only a finite number of maximal ideals, which implies that it is semi-local. □

Corollary 12.2.22. *Let $\rho : A \to B$ be a ring homomorphism. Suppose that A is semi-local and Noetherian and that B is a finitely generated A-module. Then the ring B is semi-local and Noetherian. If $\mathfrak{a}$ is a defining ideal of A, then $\mathfrak{b} = \mathfrak{a}^e$ is a defining ideal of B.*

Proof. We know that B is a Zariski ring with the $\mathfrak{b}$-adic topology (Proposition 11.4.32). As $A/\mathfrak{a}$ is Artinian by Corollary 12.2.21 and $B/\mathfrak{b}$ is a finitely generated $(A/\mathfrak{a})$-module, it is an Artinian ring, hence B is semilocal and $\mathfrak{b}$ is a defining ideal of B by Corollary 12.2.21. □

Corollary 12.2.23. *Let A be a complete semi-local Noetherian ring, $\mathfrak{a}$ a defining ideal of A, M a finitely generated A-module and (N_n) a decreasing sequence of submodules of M such that $\bigcap_n N_n = 0$. Then, for all $p > 0$, there exists $n > 0$ such that $N_n \subseteq \mathfrak{m}^p M$.*

Proposition 12.2.24. *Let A be a Noetherian ring and $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ the prime ideals associated with the A-module A.*

(a) The set $S = \bigcap_{i=1}^n (A - \mathfrak{p}_i)$ is the set of elements which are not divisors of 0 in A.

(b) If all the $\mathfrak{p}_i$ are minimal elements of $\mathrm{Ass}(A)$, then the total ring of fractions $S^{-1}A$ of A is Artinian.

(c) If the ring A is reduced, then all the $\mathfrak{p}_i$ are minimal elements of $\mathrm{Ass}(A)$ (and therefore are the minimal prime ideals of A) and each of the $A_{\mathfrak{p}_i}$ is a field. For each index i, the canonical homomorphism $S^{-1}A \to A_{\mathfrak{p}_i}$ is surjective and its kernel is $S^{-1}\mathfrak{p}_i$. Finally the canonical homomorphism from $S^{-1}A$ to $\prod_{i=1}^n (S^{-1}A/S^{-1}\mathfrak{p}_i)$ is bijective.

Proof. The fact that S is the set of elements which are not divisors of 0 in A has already been seen in Proposition 12.1.3. The prime ideals of $S^{-1}A$ are of the form $S^{-1}\mathfrak{p}$, where $\mathfrak{p}$ is a prime ideal of A contained in $\bigcup_i \mathfrak{p}_i$, and hence is contained in one of the $\mathfrak{p}_i$. If $\mathfrak{p}_i$ is a minimal element of $\mathrm{Ass}(A)$, it is then a minimal element of $\mathrm{Spec}(A) = \mathrm{supp}(A)$. If each of the $\mathfrak{p}_i$ is a minimal element of $\mathrm{Ass}(A)$, we then see that the prime ideals of $S^{-1}A$ are the $S^{-1}\mathfrak{p}_i$ and they are therefore all maximal, which proves that $S^{-1}A$ is Artinian.

Suppose finally that the ring A is reduced. Then $\bigcap_i \mathfrak{p}_i = \{0\}$, and we deduce that $\{0\} = \bigcap_i \mathfrak{p}_i$ is a reduced primary decomposition of the ideal $\{0\}$ by Corollary 12.2.9. In particular, none of the $\mathfrak{p}_i$ can contain a $\mathfrak{p}_i$ of index $j \neq i$ and therefore the $\mathfrak{p}_i$ are all minimal elements of $\mathrm{Ass}(A)$. The ring $S^{-1}A$ is then Artinian by (b). The $S^{-1}\mathfrak{p}$ are prime ideals associated with the $S^{-1}A$-module $S^{-1}A$ and $\{0\} = S^{-1}(\bigcap_{i=1}^n \mathfrak{p}_i) = \bigcap_{i=1}^n S^{-1}\mathfrak{p}_i$. As the $S^{-1}\mathfrak{p}_i$ are distinct, $(S^{-1}\mathfrak{p}_i)$ is a reduced primary decomposition of $\{0\}$ in $S^{-1}A$ by Corollary 12.2.9. Proposition 12.2.17 then shows that the canonical homomorphism $\phi_i : S^{-1}A \to (S^{-1}A)_{\mathfrak{p}_i}$ is surjective and has kernel $S^{-1}\mathfrak{p}_i$, and the canonical homomorphism

$$S^{-1}A \to \prod_{i=1}^{n} (S^{-1}A/S^{-1}\mathfrak{p}_i)$$

is bijective. We know moreover that the canonical homomorphism $S^{-1}A \to A_{\mathfrak{p}_i}$ is given by

$$S^{-1}A \xrightarrow{\phi_i} (S^{-1}A)_{\mathfrak{p}_i} \xrightarrow{\cong} (S^{-1}A)_{S^{-1}\mathfrak{p}_i} \xrightarrow{\cong} A_{\mathfrak{p}_i}$$

Finally, it follows from Proposition 12.2.17 that $(S^{-1}A)_{S^{-1}\mathfrak{p}_i}$ is isomorphic to $S^{-1}A/S^{-1}\mathfrak{p}_i$, and hence is a field since $S^{-1}\mathfrak{p}_i$ is a maximal ideal. □

12.2.5 Extension of scalars

In this part, A and B will denote two rings and we shall consider a ring homomorphism $\rho : A \to B$ which makes B into an A-algebra. Recall that, for every B-module P, $\rho^*(P)$ is the A-module whose structure is defined by $a \cdot y = \rho(a)y$ for all $a \in A$, $y \in P$.

Lemma 12.2.25. *Let A be a Noetherian ring, $\mathfrak{p}$ a prime ideal of A, M an A-module whose annihilator contains a power of $\mathfrak{p}$ and such that $\mathrm{Ass}_A(M) = \{\mathfrak{p}\}$. Let P be a B-module such that $\rho^*(P)$ is a flat A-module. The condition $\mathfrak{P} \in \mathrm{Ass}_B(M \otimes_A P)$ then implies $\mathfrak{P}^c = \mathfrak{p}$.*

Proof. If n is such that $\mathfrak{p}^n M = 0$, then $\mathfrak{p}^n B \subseteq \mathrm{Ann}(M \otimes_A P)$, whence $\mathfrak{p}^n B \subseteq \mathfrak{P}$, which implics $\mathfrak{p}^n \subseteq \mathfrak{P}^c$ and therefore $\mathfrak{p} \subseteq \mathfrak{P}$ sincen $\mathfrak{P}^c$ is prime. Moreover, if $a \in A - \mathfrak{p}$, the homothety h_a with ratio a on M is injective. As $h_a \otimes 1_P$ is the homothety $h_{\rho(a)}$ with ratio $\rho(a)$ on $M \otimes_A P$ and $\rho^*(P)$ is flat, we see $h_{\rho(a)}$ is injective. This proves that $\rho(a) \notin \mathfrak{P}$, whence $\mathfrak{P}^c = \mathfrak{p}$. □

Proposition 12.2.26. *Let $\rho : A \to B$ be a ring homomorphism, M an A-module and P a B-module such that $\rho^*(P)$ is a flat A-module. Then*

$$\mathrm{Ass}_B(M \otimes_A P) \supseteq \bigcup_{\mathfrak{p} \in \mathrm{Ass}_A(M)} \mathrm{Ass}_B(P/\mathfrak{p}P) \tag{2.5.1}$$

and the equality holds if A is Noetherian.

Proof. Let $\mathfrak{p} \in \mathrm{Ass}_A(M)$. By definition there exists an injection $A/\mathfrak{p} \to M$, and by tensoring with P we get an injection $P/\mathfrak{p}P \to M \otimes_A P$, whence $\mathrm{Ass}_B(P/\mathfrak{p}P) \subseteq \mathrm{Ass}_B(M \otimes_A P)$ and (2.5.1) follows. Suppose now that A is Noetherian and let us prove the opposite inclusion.

Suppose first that M is a finitely generated A-module and that $\mathrm{Ass}_A(M)$ is reduced to a single element $\mathfrak{p}$. By Theorem 12.1.18 there exists a chain (M_i) of M such that M_i/M_{i+1} is

isomorphic to $A/\mathfrak{p}_i$ where $\mathfrak{p}_i$ is a prime ideal of A containing $\mathfrak{p}$. As P is a flat A-module, $(M_i \otimes_A P)$ is then a chain of $M \otimes_A P$ such that

$$(M_i \otimes_A P)/(M_{i+1} \otimes_A P) = (A/\mathfrak{p}_i) \otimes_A P = P/\mathfrak{p}_i P.$$

By Proposition 12.1.7, we get

$$\mathrm{Ass}_B(M \otimes_A P) \subseteq \bigcup_{i=0}^{n-1} \mathrm{Ass}_B(P/\mathfrak{p}_i P).$$

We know that M is annihilated by a power of $\mathfrak{p}$ by Proposition 12.1.21, so Lemma 12.2.25 shows that $\mathfrak{P}^c = \mathfrak{p}$ for all $\mathfrak{P} \in \mathrm{Ass}_B(M \otimes_A P)$. Also, since $P/\mathfrak{p}_i P$ is annihilated by $\mathfrak{p}_i$, by Lemma 12.2.25 we have $(\mathfrak{P}')^c = \mathfrak{p}_i$ for all $\mathfrak{P}' \in \mathrm{Ass}_B(P/\mathfrak{p}_i P)$. This then shows $\mathrm{Ass}_B(M \otimes_A P) \cap \mathrm{Ass}_B(P/\mathfrak{p}_i P) = \varnothing$ if $\mathfrak{p}_i \neq \mathfrak{p}$, which proves the claim in this case.

Next we drop the assumption $\mathrm{Ass}(M) = \{\mathfrak{p}\}$ and assume only that M is finitely generated. Let $\mathrm{Ass}_A(M) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ and let $\{0\} = \bigcap_i Q_i$ be a corresponding reduced primary decomposition of $\{0\}$. Then M is isomorphic to a submodule of the direct sum of the submodules $M_i = M/Q_i$ and, as $f^*(P)$ is a flat A-module, $M \otimes_A P$ is isomorphic to a submodule of the direct sum of the submodules $M_i \otimes_A P$. We deduce that

$$\mathrm{Ass}_B(M \otimes_A P) \subseteq \bigcup_{i=1}^{n} \mathrm{Ass}_B(M_i \otimes_A P).$$

But M_i is a finitely generated A-module such that $\mathrm{Ass}_A(M_i)$ is reduced to a single element $\mathfrak{p}_i$. By what we have proved, $\mathrm{Ass}_B(M_i \otimes_A P) = \mathrm{Ass}_B(P/\mathfrak{p}_i P)$, whence the claim in this case.

Now we turn to the general case. The B-module $M \otimes_A P$ is the union of the submodules $N \otimes_A P$, where N runs through the set of finitely generated submodules of the A-module M. If $\mathfrak{P}$ belongs to $\mathrm{Ass}_B(M \otimes_A P)$, then there exists a finitely generated submodule N of M such that $\mathfrak{P} \in \mathrm{Ass}_B(N \otimes_A P)$. By the preceeding argument, there exists $\mathfrak{p} \in \mathrm{Ass}_A(N)$ such that $\mathfrak{P} \in \mathrm{Ass}_B(P/\mathfrak{p}P)$. As $\mathrm{Ass}_A(N) \subseteq \mathrm{Ass}_A(M)$, this completes the proof. □

Corollary 12.2.27. *In the situation of Proposition 12.2.26, if A is Noetherian and $\mathfrak{P} \in \mathrm{Ass}_B(M \otimes_A P)$, then $\mathfrak{P}^c \in \mathrm{Ass}_A(M)$ and $\mathfrak{P}^c$ is the only prime ideal $\mathfrak{p}$ of A such that $\mathfrak{P} \in \mathrm{Ass}_B(P/\mathfrak{p}P)$.*

Proof. By Proposition 12.2.26 we see $\mathfrak{P} \in \mathrm{Ass}_B(P/\mathfrak{p}P) = \mathrm{Ass}_B((A/\mathfrak{p}) \otimes_A P)$ where $\mathfrak{p} \in \mathrm{Ass}_A(M)$. Then Lemma 12.2.25 says $\mathfrak{P}^c = \mathfrak{p}$. □

Corollary 12.2.28. *Suppose that A and B are Noetherian and that B is a flat A-module. Let $\mathfrak{p}$ be a prime ideal of A, Q a $\mathfrak{p}$-primary submodule of an A-module M and $\mathfrak{P}$ a prime ideal of B. For $Q \otimes_A B$ to be a $\mathfrak{P}$-primary submodule of $M \otimes_A B$, it is necessary and sufficient that $\mathfrak{p}B$ be a $\mathfrak{P}$-primary ideal of B.*

Proof. Let us apply Proposition 12.2.26 to the A-module M/Q and the B-module B. Then $\mathrm{Ass}_A(M/Q) = \{\mathfrak{p}\}$ and $(M/Q) \otimes_A B$ is isomorphic to $(M \otimes_A B)/(Q \otimes_A B)$ and hence $\mathrm{Ass}_B((E \otimes_A B)/(Q \otimes_A B)) = \mathrm{Ass}_B(B/\mathfrak{p}B)$. To say that $Q \otimes_A B$ is $\mathfrak{P}$-primary in $M \otimes_A B$ therefore means that $\mathrm{Ass}_B(B/\mathfrak{p}B)$ is reduced to $\{\mathfrak{P}\}$, whence the corollary. □

Proposition 12.2.29. *Suppose that A and B are Noetherian and that B is a flat A-module. Let M be an A-module and N a submodule of M such that, for every prime ideal $\mathfrak{p} \in \mathrm{Ass}_A(M/N)$, $\mathfrak{p}B$ is a prime*

ideal of B or equal to B. Let $N = \bigcap_{\mathfrak{p}\in \mathrm{Ass}_A(M/N)} Q(\mathfrak{p})$ be a reduced primary decomposition of N in M, $Q(\mathfrak{p})$ being $\mathfrak{p}$-primary for all $\mathfrak{p} \in \mathrm{Ass}(M/N)$.

(a) If $\mathfrak{p} \in \mathrm{Ass}(M/N)$ and $\mathfrak{p}B = B$, then $Q(\mathfrak{p}) \otimes_A B = M \otimes_A B$.

(b) If $\mathfrak{p} \in \mathrm{Ass}(M/N)$ and $\mathfrak{p}B$ is prime, then $Q(\mathfrak{p}) \otimes_A B$ is $\mathfrak{p}B$-primary in $M \otimes_A B$.

(c) If Φ is the set of $\mathfrak{p} \in \mathrm{Ass}(M/N)$ such that $\mathfrak{p}B$ is prime, then

$$N \otimes_A B = \bigcap_{\mathfrak{p}\in\Phi}(Q(\mathfrak{p}) \otimes_A B)$$

and this relation is a reduced primary decomposition of $N \otimes_A B$ in $M \otimes_A B$.

Proof. If $\mathfrak{p}B = B$, Proposition 12.2.26 applied to $M/Q(\mathfrak{p})$ and B shows that

$$\mathrm{Ass}_B((M/Q(\mathfrak{p})) \otimes_A B) = \varnothing$$

and, as B is Noetherian and is a flat A-module, we conclude that $Q(\mathfrak{p})\otimes_A B = M\otimes_A B$. Assertion (b) follows from Corollary 12.2.28, taking $\mathfrak{P} = \mathfrak{p}B$. Finally the relation $N\otimes_A B = \bigcap_{\mathfrak{p}\in\Phi}(Q(\mathfrak{p})\otimes_A B)$ follows from the fact that B is a flat A-module. Also, for each $\mathfrak{p} \in \Phi$ we have $\mathrm{Ass}_B((M/Q(\mathfrak{p})) \otimes B) = \{\mathfrak{p}B\}$, whence $\mathfrak{p} = (\mathfrak{p}B)^c$ by Lemma 12.2.25, and $\mathfrak{p}B \neq \mathfrak{q}B$ for two distinct ideals $\mathfrak{p}, \mathfrak{q}$ of Φ. On the other hand, by Proposition 12.2.26,

$$\mathrm{Ass}((M \otimes_A B)/(N \otimes_A B)) = \Phi$$

we conclude from Corollary 12.2.9 that

$$N \otimes_A B = \bigcap_{\mathfrak{p}\in\Phi}(Q(\mathfrak{p}) \otimes_A B)$$

is a reduced primary decomposition. □

Corollary 12.2.30. *In the situation of Proposition 12.2.29, suppose that $\mathfrak{p}B$ is prime for all $\mathfrak{p} \in \mathrm{Ass}_A(M/N)$. Then, if $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are the minimal elements of $\mathrm{Ass}_A(M/N)$, the $\mathfrak{p}_iB$ are minimal elements of $\mathrm{Ass}_A((M \otimes_A B)/(N \otimes_A B))$.*

Proof. It is easy to see $\mathfrak{p}B$ is a minimal prime if $\mathfrak{p}$ is, and by Proposition 12.2.29 we see $\mathfrak{p}_iB \neq \mathfrak{p}_jB$ when $i \neq j$. □

Example 12.2.31.

(a) Let us take $B = S^{-1}A$, where S is a multiplicative subset of A. If A is Noetherian, the hypotheses of Proposition 12.2.29 are satisfied and we recover a part of Proposition 12.1.11.

(b) Let A be a Noetherian ring, $\mathfrak{a}$ an ideal of A and B the Hausdorff completion of A with respect to the $\mathfrak{a}$-adic topology. Then B is a flat A-module and Proposition 12.2.26 may be applied with $P = B$. But in general the hypotheses of Proposition 12.2.29 are not satisfied for the prime ideals of A.

(c) Let A be a Noetherian ring and B the polynomial algebra $A[X_1, \ldots, X_n]$. Then B is Noetherian and is a free A-module and therefore flat. Also, if $\mathfrak{p}$ is a prime ideal of A,

$B/\mathfrak{p}B$ is isomorphic to $(A/\mathfrak{p})[X_1, \dots, X_n]$, which is an integral domain, and hence $\mathfrak{p}B$ is prime. The hypotheses of Proposition 12.2.29 are therefore satisfied for every A-module M and every submodule N of M.

12.2.6 Primary decomposition of graded modules

Proposition 12.2.32. *Let Δ be a torsion free commutative group, A a graded ring of type Δ and M a graded A-module of type Δ. Every prime ideal associated with M is graded and is the annihilator of a homogeneous element of M.*

Proof. We know that Δ can be given a total order structure compatible with its group structure. Let $\mathfrak{p}$ be a prime ideal associated with M, the annihilator of an element $x \in M$, and let $(x_i)_{i\in\Delta}$ be the family of homogeneous components of x; let $i(1) < i(2) < \cdots < i(r)$ be the values of i for which $x_i \neq 0$. Consider an element $a \in \mathfrak{p}$ and let $(a_i)_{i\in\Delta}$ be the family of its homogeneous components; we shall prove that $a_i \in \mathfrak{p}$ for all $i \in \Delta$, which will show that $\mathfrak{p}$ is a homogeneous ideal.

We argue by induction on the number of indices i such that $a_i \neq 0$. Our assertion is obvious if this number is 0; if not, let m be the gratest of the indices i for which $a_i \neq 0$; if we prove that $a_m \in \mathfrak{p}$, the induction hypothesis applied to $a - a_m$ will give the conclusion. Now, $ax = 0$; for all $j \in \Delta$, using the fact that the homogeneous component of degree $m + j$ of ax is 0, we obtain $\sum_{i\in\Delta} a_{m-i}x_{j+i} = 0$; we conclude that $a_m x_j$ is a linear combination of the x_i of indices $i > j$. In particular, $a_m x_{i(r)} = 0$, whence, by descending induction on $k < r$, $a_m^{r-k+1} x_{i(k)} = 0$. Then $a_m^r x = 0$, whence $a_m^r \in \mathfrak{p}$ and, as $\mathfrak{p}$ is prime, $a_m \in \mathfrak{p}$.

We now show that $\mathfrak{p}$ is the annihilator of a homogeneous element of M. Let us write $\mathfrak{b}_n = \mathrm{Ann}(x_{i(n)})$ for $1 \leq n \leq r$. For every homogeneous element b of $\mathfrak{p}$ and all n the homogeneous component of bx of degree $i(n) + \deg(b)$ is $bx_{i(n)}$, hence $bx_{i(n)} = 0$ and therefore $b \in \mathfrak{b}_n$; as $\mathfrak{p}$ is generated by its homogeneous elements, $\mathfrak{p} \subseteq \mathfrak{b}_n$. On the other hand, clearly $\bigcap_{n=1}^r \mathfrak{b}_n = \mathfrak{p}$; as $\mathfrak{p}$ is prime, there exists an n such that $\mathfrak{b}_n \subseteq \mathfrak{p}$ (Proposition 10.1.4), whence $b_n = \mathfrak{p} = \mathrm{Ann}(x_{i(n)})$, which completes the proof. □

Corollary 12.2.33. *For every (necessarily homogeneous) prime ideal $\mathfrak{p}$ associated with a graded A-module M, there exists an index $k \in \Delta$ such that the shifted graded A-module $(A/\mathfrak{p})(k)$ is isomorphic to a graded submodule of M.*

Proof. With the notation of the proof of Proposition 12.2.32, consider the homomorphism obtained, by taking quotients, from the homomorphism $a \mapsto ax_{i(n)}$ of A to M; the latter is a graded homomorphism of degree $i(n)$ and hence it gives on taking quotients a graded bijective homomorphism of degree $i(n)$ of $A/\mathfrak{p}$ onto a graded submodule of M. □

Proposition 12.2.34. *Let Δ be a torsion-free commutative group, A a graded Noetherian ring of type Δ and M a graded finitely generated A-module of type Δ. There exists a composition series $(M_i)_{0\leq i\leq n}$ consisting of graded submodules of M such that the graded module M_i/M_{i+1} is isomorphic to a shifted graded module $(A/\mathfrak{p}_i)(k_i)$, where $\mathfrak{p}_i$ is a homogeneous prime ideal of A and $k_i \in \Delta$.*

Proof. It is sufficient to retrace the argument of Theorem 12.1.18 taking on this occasion $\mathcal{M}$ to be the set of graded submodules of M with a composition series with the properties of the statement; we conclude using Corollary 12.2.33. □

Proposition 12.2.35. *Let Δ be a torsion-free commutative group, A a graded Noetherian ring of type Δ, $\mathfrak{p}$ a homogeneous ideal of A and M a graded A-module of type Δ not reduced to 0. Suppose that for every homogeneous element a of $\mathfrak{p}$ the homothety of ratio a on M is almost nilpotent and that for every homogeneous element b of $A - \mathfrak{p}$ the homothety of ratio b on M is infective. Then $\mathfrak{p}$ is prime and the submodule $\{0\}$ of M is $\mathfrak{p}$-primary.*

Proof. It suffices to show that $\mathrm{Ass}(M) = \{p\}$ (Proposition 12.2.1). Let $\mathfrak{q}$ be a prime ideal associated with M; it is a homogeneous ideal and it is the annihilator of a homogeneous element $x \neq 0$ of M by Proposition 12.2.32. For every homogcneous element a of $\mathfrak{q}$, $ax = 0$ and hence the homothety of ratio a on M is not injective, whence $a \in \mathfrak{p}$. Conversely, let b be a homogeneous element of $\mathfrak{p}$; there exists an integer $n > 0$ such that $b^n x = 0$, whence $b^n \in \mathrm{Ann}(x) = \mathfrak{q}$ and, as $\mathfrak{q}$ is prime, $b \in \mathfrak{q}$. As $\mathfrak{p}$ and $\mathfrak{q}$ are generated by their respective homogeneous element, $\mathfrak{p} = \mathfrak{q}$, which proves that $\mathrm{Ass}(M) \subseteq \{p\}$. As $M \neq \{0\}$, $\mathrm{Ass}(M) \neq \varnothing$ (Corollary 12.1.4), whence $\mathrm{Ass}(M) = \{\mathfrak{p}\}$. □

Proposition 12.2.36. *Let Δ be a torsion-free commutative group, A a graded Noetherian ring of type Δ and M a graded A-module of type Δ. Let $\mathfrak{p}$ be a prime ideal of A and N a submodule of M which is $\mathfrak{p}$-primary with respect to M.*

(a) The homogeneous ideal $\mathfrak{p}^h$ of A is prime.

(b) The graded submodule N^h of N is $\mathfrak{p}^h$-primary with respect to M.

Proof. We know that the homogeneous elements of $\mathfrak{p}^h$ (resp. N^h) are just the homogeneous elements of $\mathfrak{p}$ (resp. N). Let a be a homogeneous element of $\mathfrak{p}$; if x is a homogeneous element of M, there exists an integer $n > 0$ such that $a^n x \in N$; as $a^n x$ is homogeneous, $a^n x \in N^h$; as every $y \in M$ is the direct sum of a finite number of homogeneous elements, we conclude that there exists an integer $m > 0$ such that $a^m y \in N^h$, so that the homothety with ratio a in M/N^h is almost nilpotent.

Consider now a homogeneous element b of $A - \mathfrak{p}^h$; then $b \notin \mathfrak{p}$ since b is homogeneous. Let x be an element of M such that $bx \in N^h$ and let $(x_i)_{i\in\Delta}$ be the family of homogeneous components of x. As N^h is graded, $bx_i \in N^h$ for all i, hence $bx_i \in N$ and, as $b \notin \mathfrak{p}$, we conclude that $x_i \in N$; as x_i is homogeneous, $x_i \in N^h$, whence $x \in N^h$ and the homothety with ratio b on M/N^h is injective. The proposition then follows from Proposition 12.2.35 applied to $\mathfrak{p}^h$ and M/N^h. □

Proposition 12.2.37. *Let Δ be a torsion-free commutative group, A a graded Noetherian ring of type Δ, M a graded A-module of type M, N a graded submodule of M and $N = \bigcap_{i\in I} Q_i$ a primary decomposition of N in M.*

(a) Let Q_i^h be the graded submodule of Q_i, then the Q_i^h are primary and $N = \bigcap_{i\in I} Q_i^h$.

(b) If the primary decomposition $N = \bigcap_{i\in I} Q_i$ is reduced, so is the primary decomposition $N = \bigcap_{i\in I} Q_i^h$, and for all $i \in I$ the prime ideals corresponding to Q_i and Q_i^h are equal.

(c) If Q_i corresponds to a prime ideal $\mathfrak{p}_i$ which is a minimal element $\mathrm{Ass}(M/N)$, Q_i is a graded submodule of M.

Proof. We have seen (Proposition 12.2.36) that the Q_i^h are primary with respect to M and $N \subseteq Q_i^h \subseteq Q_i$, which proves (a). Proposition 12.2.36 also shows that the prime ideal $\mathfrak{p})i^h$ corresponding to Q_i^h is the largest homogeneous ideal contained in the prime ideal $\mathfrak{p}_i$ corresponding to Q_i. If the decomposition $N = \bigcap_{i \in I} Q_i$ is reduced, $\mathfrak{p}_i \in \operatorname{Ass}(M/N)$ for all i (Proposition 12.2.8), hence $\mathfrak{p}_i$ is a graded ideal (Proposition 12.2.32) and therefore $\mathfrak{p}_i = \mathfrak{p}_i^h$; then $\operatorname{Ass}(M/N) = \bigcup_{i \in I} \{\mathfrak{p}_i\}$ (Proposition 12.2.8), which proves that the decomposition $N = \bigcap_{i \in I} Q_i^h$ is reduced (Proposition 12.2.8). Finally, if $\mathfrak{p}_i$ is a minimal element of $\operatorname{Ass}(M/N)$, then $\mathfrak{p}_i^h = \mathfrak{p}_i$ since $\mathfrak{p}_i$ is homogeneous (Proposition 12.2.32), whence $Q_i^h = Q_i$, by virtue of Proposition 12.2.10. $\square$

Chapter 13

Integral dependence

13.1 Integral elements

Proposition 13.1.1. *Let A be a ring, R an algebra over A and x an element of R. The following properties are equivalent:*

(i) x is a root of a monic polynomial in the polynomial ring $A[X]$.

(ii) The subalgebra $A[x]$ of R is a finitely generated A-module.

(iii) There exists a faithful $A[x]$-module which is a finitely generated A-module.

Proof. The implications (i)⇒(ii)⇒(iii) are clear. Now assume that there exists a faithful $A[x]$-module M which is finitely generated as an A-module. Let ϕ to be multiplication by x and $I = A$ (we have $xM \subseteq M$ since M is an $A[x]$-module). Since M is faithful, we have $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ for suitable $a_i \in A$ in view of Proposition 7.1.1, whence (i) holds. □

An element $x \in R$ is called integral over A if it satisfies the equivalent properties of Proposition 13.1.1. A relation of the form $P(x) = 0$, where P is a monic polynomial in $A[X]$ is also called an equation of integral dependence with coefficients in A.

Example 13.1.2.

(a) Let K be a field and R a K-algebra; to say that an element $x \in R$ is integral over K is equivalent to saying that x is a root of a non-constant polynomial in the ring $K[X]$. Generalizing the terminology introduced when R is an extension of K, the elements $x \in R$ which are integral over K are also called the **algebraic elements** of R over K.

(b) The elements of $\mathbb{Q}(i)$ which are integral over $\mathbb{Z}$ are the elements of the form $a + ib$ where $a \in \mathbb{Z}$ and $b \in \mathbb{Z}$ ("Gaussian integers"); the elements of $\mathbb{Q}(\sqrt{5})$ which are integral over $\mathbb{Z}$ are the elements of the form $(a + b\sqrt{5})/2$ where a and b belong to $\mathbb{Z}$.

Proposition 13.1.3. *Let A be a ring, R an algebra over A and x an element of R. For x to be integral over A, it is necessary and sufficient that $A[x]$ be contained in a subalgebra R' of R which is a finitely generated A-module.*

Proof. The condition is obviously necessary by virtue of Proposition 13.1.1. It is also sufficient by virtue of Proposition 13.1.1, for R' is a faithful $A[x]$-module (since it contains the unit element of R). □

Corollary 13.1.4. *Let A be a Noetherian ring, R an A-algebra and x an element of R. For x to be integral over A, it is necessary and sufficient that there exist a finitely generated submodule of R containing $A[x]$.*

Proof. The condition is necessary by virtue of Proposition 13.1.1. It is sufficient for if $A[x]$ is a sub-A-module of a finitely generated A-module, it is itself a finitely generated A-module. □

Let A be a ring. An A-algebra R is called **integral over A** if every element of R is integral over A. Recall that R is called finite over A if R is a finitely generated *A-module*, and finite type if a finitely generated *A-algebra*. It follows from Proposition 13.1.3 that every finite A-algebra is integral.

Example 13.1.5. If M is a finitely generated A-module, the algebra $\mathrm{End}_A(M)$ of endomorphisms of M is integral over A by virtue of Proposition 13.1.1. In particular, for every integer n, the matrix algebra $\mathcal{M}_n(A) = \mathrm{End}_A(A^n)$ is integral (and even finite) over A.

Proposition 13.1.6. *Let A, B be two rings, R an A-algebra, S an B-algebra, and $\rho : A \longrightarrow B$ and $\tau : R \longrightarrow S$ two ring homomorphisms such that the diagram*

$$\begin{tikzcd} A \arrow[r, "\rho"] \arrow[d] & B \arrow[d] \\ R \arrow[r, "\tau"] & S \end{tikzcd}$$

is commutative. If an element $x \in R$ is integral over A, then $\tau(x)$ is integral over B.

Proof. If $P(x) = 0$ where $P \in A[X]$, then $\tau(x)$ is a zero of $\rho(P)$, hence $\tau(x)$ is integral over B. □

Corollary 13.1.7. *Let A be a ring, B an A-algebra and C a B-algebra. Then every element $x \in C$ which is integral over A is integral over B.*

Corollary 13.1.8. *Let K be a field, L an extension of K and x, y two elements of L which are conjugate over K. If A is a subring of K and x is integral over A, then y is also integral over A.*

Proof. There exists a K-isomorphism σ of $K(x)$ onto $K(y)$ such that $\sigma(x) = y$ and the elements of A are invariant under σ. □

Proposition 13.1.9. *Let $(R_i)_{1\leq i\leq n}$ be a finite family of A-algebras and let $R = \prod_{i=1}^n R_i$ be their product. For an element $x = (x_i)$ of R to be integral over A, it is necessary and sufficient that each of the x_i be integral over A. For R to be integral over A, it is necessary and sufficient that each of the R_i be integral over A.*

Proof. It is obviously sufficient to prove the first assertion. The condition is necessary by Proposition 13.1.6. Conversely, if each of the x_i is integral over A, the subalgebra $A[x_i]$ of R_i is a finitely generated A-module and hence so is the subalgebra $\prod_{i=1}^n A[x_i]$ of R. As $A[x]$ is contained in this subalgebra, x is integral over A. □

Proposition 13.1.10. *Let A be a ring, B an A-algebra and let $x_1, \ldots, x_n$ be integral over A. Then the ring $A[x_1, \ldots, x_n]$ is a finitely generated A-module.*

Proof. Proof by induction. For $n = 1$, this is a part of Proposition 13.1.1. Assume $n > 1$, let $A_{n-1} = A[x_1, \dots, x_{n-1}]$; then by the induction hypothesis A_{n-1} is a finitely generated A-module. Moreover, $A_n = A_{n-1}[x_n]$ is a finitely generated A_{n-1}-module by the case $n = 1$, since x_n is integral over A_{n-1}. Hence A_n is finitely generated as an A-module. □

Corollary 13.1.11. *Let A be a ring, R an A-algebra and E a set of elements of R which are integral over A. Then the sub-A-algebra of R generated by E is integral over A.*

Proof. Let B be the A-algebra generated by E in R. Then every element of B belongs to a sub-A-algebra of B generated by a finite subset of E, whence is integral over A by Proposition 13.1.10. □

Corollary 13.1.12. *The set $\overline{A}$ of elements of B which are integral over A is a subring of B containing A.*

Proof. If $x, y \in \overline{A}$ then $A[x, y]$ is a finitely generated A-module by Proposition 13.1.10. Hence $x \pm y$ and xy are integral over A, by (c) of Proposition 13.1.1. □

Proposition 13.1.13. *Let A be a ring and B and R two A-algebras. If R is integral over A, then $R \otimes_A B$ is integral over B.*

Proof. Consider any element $y = \sum_i \otimes b_i$ of $R \otimes_A B$, where the x, belong to R and the b_i to B. As $x_i \otimes a_i = (x_i \otimes 1)a_i$ and the $x_i \otimes 1$ are integral over B by Proposition 13.1.6, so is x. □

Corollary 13.1.14. *Let R be a ring and A, B, C subrings of R such that $A \subseteq B$. If B is integral over A, then $C[B]$ is integral over $C[A]$.*

Proof. The rng $B \otimes_A C[A]$ is integral over $C[A]$ by Proposition 13.1.13 and hence so is the canonical image $C[B]$ of $B \otimes_A C[A]$ in R (considered as an A-algebra) by Proposition 13.1.6. □

Proposition 13.1.15. *Let A be a ring and B an A-algebra. If B integral over A, $\mathfrak{b}$ is an ideal of B and $\mathfrak{a} = \mathfrak{b}^c$, then $B/\mathfrak{b}$ is integral over $A/\mathfrak{a}$.*

Proof. The follows by reducing an integral equation of an element of B mod $\mathfrak{b}$. □

Proposition 13.1.16. *Let A be a ring, B an A-algebra and C a B-algebra. If B is integral over A and C is integral over B, then C is integral over A.*

Proof. It is sufficient to verify that every $x \in C$ is integral over A. Then we have an equation

$$x^n + b_{n-1}x^{n-1} + \cdots + b_0, \quad b_i \in B.$$

The ring $B' = A[b_1, \dots, b_n]$ is a finitely generated A-module by Proposition 13.1.10, and $B'[X]$ is a finitely generated B'-module (since x is integral over B'). Hence $B'[X]$ is a finitely generated A-module and therefore x is integral over A by (c) of Proposition 13.1.1. □

Corollary 13.1.17. *Let A be a ring and R, S two A-algebras integral over A. Then $R \otimes_A S$ is integral over A.*

Proof. The ring $R \otimes_A S$ is integral over S by Proposition 13.1.13 and hence the conclusion follows from Proposition 13.1.16. □

13.1.1 The integral closure of a ring

Let A be a ring and R a A-algebra. The sub-A-algebra $\overline{A}$ of R consisting of the elements of R integral over A is called the integral closure of A in R. If $\overline{A}$ is equal to the canonical image of A in R, A is called integrally closed in R.

Remark 13.1.1. If A is a field, the integral closure $\overline{A}$ of A in R consists of the elements of R which are algebraic over A. Generalizing the terminology used for field extensions, $\overline{A}$ is then also called the algebraic closure of the field A in the algebra R and A is called algebraically closed in R if $\overline{A} = A$.

If A is an integral domain, the integral closure of A in its field of fractions is called the **integral closure of A**. An integral domain is called **integrally closed** if it is equal to its integral closure.

Proposition 13.1.18. *Let A be a ring and R an A-algebra. The integral closure $\overline{A}$ of A in R is a subring integrally closed in R.*

Proof. The integral closure of $\overline{A}$ in R is integral over A. It is therefore equal to $\overline{A}$. □

Corollary 13.1.19. *The integral closure of an integral domain A is an integrally closed domain.*

Proof. Let K be the field of fractions of A and B the integral closure of A. Clearly K is the field of fractions of B and it is sufficient to apply Proposition 13.1.18 to $R = K$. □

Proposition 13.1.20. *Let R be a ring, $(B_i)_{i\in I}$ a family of subrings of R and for each $i \in I$ let A_i be a subring of B_i. If each A_i is integrally closed in B_i, then $A = \bigcap_i A_i$ is integrally closed in $B = \bigcap_i B_i$.*

Proof. This follows from Corollary 13.1.7. □

Corollary 13.1.21. *Every intersection of a non-empty family of integrally closed subdomains of an integral domain A is an integrally closed domain.*

Proof. It is sufficient to apply Proposition 13.1.20: taking R and the B_i equal to the field of fractions K of A and noting that a subring of K integrally closed in K is a fortiori an integrally closed domain since its field of fractions is contained in K. □

Proposition 13.1.22. *Let A be a ring, $(R_i)_{1\le i\le n}$ a finite family of A-algebras and $\overline{A}_i$ the integral closure of A in R_i. Then the integral closure of A in $R = \prod_{i=1}^n R_i$ is $\prod_{i=1}^n \overline{A}_i$.*

Proof. This is an immediate consequence of Proposition 13.1.9. □

Corollary 13.1.23. *Let A be a reduced Noetherian ring, $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ its distinct minimal prime ideals, K_i the field of fractions of the integral domain $A/\mathfrak{p}_i$ and $\overline{A}_i$ the integral closure of A in K_i. Then the canonical isomorphism of the total ring of fractions $Q(A)$ of A onto $\prod_{i=1}^n K_i$ maps the integral closure of A in $Q(A)$ onto the product ring $\prod_{i=1}^n \overline{A}_i$.*

Proof. This follows from Proposition 12.2.24 and Proposition 13.1.22. □

Corollary 13.1.24. *For a reduced Noetherian ring to be integrally closed in its total ring of fractions, it is necessary and sufficient that it be a direct product of integrally closed (Noetherian) domains.*

13.1.2 Examples of integrally closed domains

Proposition 13.1.25. *A UFD is integrally closed.*

Proof. Let A be a UFD and K be its fraction field. Then an element $x = a/b \in K$ (where a, b are coprime) is integral over A if and only if $x \in A$. In fact, if there is an equation

$$a^n/b^n + c_{n-1}a^{n-1}/b^{n-1} + \cdots + c_1 a/b + c_0 = 0$$

then multiplying b^n on both sides we see $b \mid a$, which is a contradiction. □

Example 13.1.26. Let k be a field and X an indeterminate over k; set $A = k[X^2, X^3] \subseteq B = k[X]$. Then A and B both have the same field of fractions $K = k(X)$. Since B is a UFD, it is integrally closed; but X is integral over A, so that B is the integral closure of A in K.

Note that in this example $A \cong k[X, Y]/(Y^2 - X^3)$. Thus A is the coordinate ring of the plane curve $Y^2 = X^3$, which has a singularity at the origin. The fact that A is not integrally closed is related to the existence of this singularity.

Proposition 13.1.27. *Let A be a ring, R an A-algebra and P and Q monic polynomials in $R[X]$. If the cofficients of PQ are integral over A, then the coefficients of P and Q are integral over A.*

Proof. There exists a ring R' containing R and families of elements (a_i), (b_j) of R' such that in $R'[X]$ we have

$$P(X) = \prod_{i=1}^{n}(X - a_i), \quad Q(X) = \prod_{j=1}^{m}(X - b_j)$$

The coefficients of PQ are integral over A and so belong to the integral closure A' of A in R'. Thus the elements a_i and b_j are integral over A' and hence belong to A'. It the follows that the coefficients of P and Q are integral over A. □

Let A be an integral domain, K its field of fractions and L a K-algebra. Given an element $x \in L$ algebraic over K, the polynomials $P \in K[X]$ such that $P(x) = 0$ form a nonzero ideal a of $K[X]$, necessarily principal. There exists a unique monic polynomial which generates $\mathfrak{a}$. Generalizing the tenninology, this monic polynomial will be called the **minimal polynomial** of x over K.

Corollary 13.1.28. *Let A be an integral domain, K its field of fractions and x an element of a K-algebra L. Then x is integral over A if and only if the coefficients of the minimal polynomial P of x over K are integral over A.*

Proof. If all coefficients of the minimal polynomial of x are integral over A, then by Proposition 13.1.16 we see x is integral over A. Conversely, assume that x is integral over A. Then there exists by hypothesis a monic polynomial $Q \in A[X]$ such that $Q(x) = 0$. As P divides Q in $K[X]$, it follows from Proposition 13.1.27 that the coefficients of P are integral over A. □

Example 13.1.29. Let A be a UFD in which 2 is a unit and $a \in A$. Then $A[\sqrt{a}]$ is an integrally closed domain if and only if a is squre-free. In fact, let α be a square root of a. Let K be the field of fractions of A; then A is integrally closed in K, so that if $\alpha \in K$ we have $\alpha \in A$ and $A[\alpha] = A$, and the assertion is trivial. If $\alpha \notin K$ then the field of fractions of $A[\alpha]$ is $K(\alpha)$, and

every element $\xi \in K(\alpha)$ can be written in a unique way as $\xi = x + y\alpha$ with $x, y \in K$. The minimal polynomial of ξ over K is

$$X^2 - 2xX + (x^2 - y^2 a)$$

Since α is integral over A, $\xi \in K(\alpha)$ is integral over $A[\alpha]$ if and only if it is integral over A, and by Corollary 13.1.28, if and only if $2x \in A$ and $x^2 - y^2 a \in A$.

If so, then by assumption, $2x \in A$ implies $x \in A$. Hence $y^2 a \in A$. From this, if some prime p of A divides the denominator of y, we must have $p^2 \mid a$, which is impossible if a is square-free. Thus $y \in A$ and $A[\alpha]$ is integrally closed in this case.

Note that if a is not squre-free then we can choose y such that $y^2 a \in A$ and $y \notin A$. Thus, in this case $A[\alpha]$ is not integrally closed.

Example 13.1.30. If A is an integrally closed domain and $\mathfrak{p}$ is a prime ideal in A, then the residue ring $A/\mathfrak{p}$ is not integrally closed in general. In fact, any finite integral domain $k[x_1, \dots, x_n]$ over a field k is of the form $A/\mathfrak{p}$, where A is the polynomial ring $k[X_1, \dots, X_n]$. But finite integral domains are not in general integrally closed. In the case $n = 2$ the simplest example is the one in which $\mathfrak{p}$ is the principal ideal $(X_1^2 - X_2^3)$. In that case, x_1/x_2 does not belong to the ring $k[x_1, x_2]$, but x_1/x_2 is integral over that ring since $(x_1/x_2)^2 = x_2$.

Let A be a ring and R an A-algebra. The homomorphism $A \to R$ defining the A-algebra structure on R can be extended uniquely to a homomorphism $A[X] \to R[X]$ of polynomial rings over A and R, leaving X invariant and hence $R[X]$ is given a canonical $A[X]$-algebra structure.

Proposition 13.1.31. *Let A be a ring, R an A-algebra and P a polynomial in $R[X_1, \dots, X_n]$. For P to be integral over $A[X_1, \dots, X_n]$, it is necessary and sufficient that the coefficients of P be integral over A.*

Proof. By considering the polynomials of $R[X_1, \dots, X_n]$ as polynomials in X_n with coefficients in $R[X_1, \dots, X_{n-1}]$, we see immediatelythat it is reduced to proving the proposition for $n = 1$. Then let P be a polynomial in $R[X]$. It follows immediately from Proposition 13.1.13 that, if the coefficients of P are in the integral closure B of A in R, the element P, which belongs to $B[X] = B \otimes_A A[X]$, is integral over $A[X]$. Conversely, suppose that P is integral over $A[X]$ and let

$$Q(Y) = Y^m + F_{m-1}Y^{m-1} + \cdots + F_0$$

be a monic polynomial with coefficients $F_i \in A[X]$ with P as a root. Let r be an integer strictly greater than all the degrees of the polynomials P and F_i and let us write $P_1(X) = P(X) - X^r$. Then P_1 is a root of the polynomial

$$Q_1(Y) = Q(Y + X^r) = Y^m + G_{m-1}Y^{m-1} + \cdots + G_0$$

with coefficients in $A[X]$. We may therefore write

$$G_0 = -P_1(P_1^{m-1} + G_{m-1}P_1^{m-2} + \cdots + G_1).$$

Now the choice of r implies that $-P_1$ is a manic polynomial of $R[X]$ and so is $G_0(X) = Q(X^r)$, the degrees of the polynomials $F_i(X)X^{r(m-i)}$ being all smaller than rm for $i \geq 1$. We conclude

first of all that the polynomial

$$P_1^{m-1} + G_{m-1}P_1^{m-2} + \cdots + G_1$$

of $R[X]$ is also monic. Moreover, as the coefficients of G_0 belong to A, Proposition 13.1.27 shows that P_1 has coefficients integral over A and the coefficients of P are therefore certainly integral over A. □

Corollary 13.1.32. *Let A be a ring, R an A-algebra and $\overline{A}$ the integral closure of A in R. Then the integral closure of $A[X_1, \ldots, X_n]$ in $R[X_1, \ldots, X_n]$ is equal to $\overline{A}[X_1, \ldots, X_n]$.*

Corollary 13.1.33. *Let A be an integral domain and $\overline{A}$ its integral closure. Then the integral closure of the polynomial ring $A[X_1, \ldots, X_n]$ is $\overline{A}[X_1, \ldots, X_n]$.*

Proof. Arguing by induction on n, the problem is immediately reduced to the case $n = 1$. Let K be the field of fractions of A, which is also that of $\overline{A}$. If an element P of the field of fractions $K(X)$ of $A[X]$ is integral over $A[X]$, it belongs to the polynomial ring $K[X]$, for the latter is a principal ideal domain and hence integrally closed. The corollary then follows from Corollary 13.1.32 applied to $R = K$. □

Corollary 13.1.34. *Let A be an integral domain. For the polynomial ring $A[X_1, \ldots, X_n]$ to be integrally closed, it is necessary and sufiicient that A be integrally closed.*

13.1.3 Completely integrally closed domains

Proposition 13.1.35. *Let A be a ring, K the filed of fraction of A and x an element of K. The following properties are equivalent:*

(i) There exists nonzero $a \in A$ such that $ax^n \in A$.

(ii) All the powers x^n (with $n \geq 0$) are contained in a finitely generated sub-A-module of K.

(iii) The subalgebra $A[X]$ of K is a fractional ideal of K.

Proof. It is clear that (i) and (iii) are equivalent and (iii) implies (ii). Also, if all powers x^n is contained in a finitely generated sub-A-module M of K, then it can be easily seen that there exists $s \in A$ such that $sM \subseteq A$, whence (i) holds. □

An element x of K is called almost integral over A if it satisfies the conditions of Proposition 13.1.35. An integral domain A is called **completely integrally closed** if every almost integral element of K belongs to A. Clearly a completely integrally closed domain is integrally closed. Conversely, Corollary 13.1.4 shows that an integrally closed Noetherian domain is completely integrally closed. If (A_i) is a family of completely integrally closed domains with the same field of fractions K, then $A = \bigcap_i A_i$ is completely integrally closed. For if $x \in K$ is such that for somc non-zero d in A, $dA[x]$ belongs to A, the hypothesis implies that $x \in A_i$ for all i and hence $x \in A$.

Proposition 13.1.36. *Let A be a completely integrally closed domain. Then every polynomial ring $A[X_1, \ldots, X_n]$ (resp. every ring of formal power series $A[\![X_1, \ldots, X_n]\!]$) is completely integrally closed.*

Proof. By induction on n, it is sufficient to prove that $A[X]$ (resp. $A[\![X]\!]$) is completely integrally closed. Then let P be an element of the field of fractions of $A[X]$ (resp. $A[\![X]\!]$) and suppose that there exists a non-zero, element $Q \in A[X]$ (resp. $Q \in A[\![X]\!]$) such that, $QP^m \in A[X]$ (resp. $QP^m \in A[\![X]\!]$) for every integer $m \geq 0$. If K is the field of fractions of A, then $A[X]$ (resp. $A[\![X]\!]$) is a subring of $K[X]$ (resp. $K[\![X]\!]$) and $K[X]$ (resp. $K[\![X]\!]$) is a principal ideal domain and hence integrally closed and Noetherian and therefore completely integrally closed, therefore we have already seen that $P \in K[X]$ (resp. $P \in K[\![X]\!]$). Write

$$P = \sum_{k=0}^{\infty} a_k X^k, \quad Q = \sum_{k=0}^{\infty} b_k X^k$$

where $a_k \in K$ and $b_k \in A$, and we argue by reductio ad absurdum by supposing that the a_k do not all belong to A. Then there is a least index i such that $a_i \notin A$. If we write $P_1 = \sum_{k=0}^{i-1} a_k X^k \in A[X]$, it follows immediately from the hypothesis that also $Q(P - P_1)^m \in A[X]$ (resp. $Q(P - P_1)^m \in A[\![X]\!]$) for all $m \geq 0$. Let j be the least integer such that $b_j \neq 0$. Then in $Q(P-P_1)^m$ the term of least degree with a nonzero coefficient is $b_j a_i^m X^{j+mi}$ and hence $b_j a_i^m \in A$ for all $m \geq 0$. But as A is completely integrally closed this implies $a_i \in A$, contrary to the hypothesis. □

Proposition 13.1.37. *Let A be a filtered ring whose filtration is exhaustive and such that every principal ideal of A is closed under the topology defined by the filtration. If the associated graded ring* $\mathrm{gr}(A)$ *is a completely integrally closed domain, then A is a completely integrally closed domain.*

Proof. Let $(A_n)_{n\in\mathbb{Z}}$ be the filtration defined on A. As $\bigcap_n A_n$ is the closure of the ideal (0), the hypothesis implies first that the filtration (A_n) is separated and, as $\mathrm{gr}(A)$ is an integral domain, so then is A (Corollary 11.2.13). Let $x = a/b$ be an element of the field of fractions K of A for which there exists a nonzero element d of A such that $dx^n \in A$ for all n. We must prove that $a \in Ab$ and, as by hypothesis the ideal Ab is closed, it is sufficient to show that, for all $n \in \mathbb{Z}$, $a \in A_b + A_n$. As the filtration of A is exhaustive, there exists an integer $p \in \mathbb{Z}$ such that $a \in Ab + A_p$. It will therefore suffice to prove that the relation $a \in Ab + A_m$ implies $a \in Ab + A_{m+1}$ for any $m \in \mathbb{N}$.

Suppose then $a = by + z$ where $y \in A$ and $z \in A_m$. Since by hypothesis $dx^n \in A$ for all n, we have $d(x-y)^n \in A$ for all n. In other words, $dz^n = b^n t_n$ where $t_n \in A$ for all n. We may assume that $z \neq 0$. Let v denote the order function on A and let us write $v(z) = n_0$. If $\bar{x}$ denote the canonical image of an element $x \in A$ in $\mathrm{gr}(A)$, then since $b \neq 0$, we deduce that $\bar{d}(\bar{z}/\bar{b})^n \in \mathrm{gr}(A)$ for all $n \in \mathbb{N}$. Since $\mathrm{gr}(A)$ is completely integrally closed, there exists an element $\bar{s} \in \mathrm{gr}(A)$ such that $\bar{z} = \bar{b}\bar{s}$. Decomposing $\bar{s}$ into a sum of homogeneous elements, it is further seen (since $\bar{z}$ and $\bar{b}$ are homogeneous) that $\bar{s}$ may be assumed to be homogeneous and that is the image of an element $s \in A$. Then $v(bs) = v(z) = n_0$ and $z \equiv bs \bmod A_{n_0+1}$. As we have $n_0 \geq m$, a fortiori $z \equiv bs \bmod A_{m+1}$, hence $a \equiv b(y+s) \bmod A_{m+1}$ and the claim follows. □

13.1.4 The integral closure of a ring of fractions

Proposition 13.1.38. *Let A be a ring, R an A-algebra, $\overline{A}$ the integral closure of A in R and S a multiplicative subset of A. Then $S^{-1}\overline{A}$ is the integral closure of $S^{-1}A$ in $S^{-1}B$.*

Proof. Let $b/s \in S^{-1}\overline{A}$, where b is integral over A, say

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0, \quad a_i \in A.$$

Then the equation of b gives an equation

$$(b/s)^n + (a_{n-1}/s)(b/s)^{n-1} + \cdots + a_0/s^n = 0$$

Hence $S^{-1}\overline{A}$ is integral over $S^{-1}A$. Conversely, if $b/s \in S^{-1}B$ is integral over $S^{-1}A$, then we have an equation of the form

$$(b/s)^n + (a_{n-1}/s_{n-1})(b/s)^{n-1} + \cdots + a_0/s_0 = 0$$

where $a_i \in A$, $s_i \in S$. Let $t = s_1 \cdots s_n$, and multiply this equation by $(st)^n$ throughout. Then it becomes an equation of integral dependence for bt over A. Hence $bt \in \overline{A}$ and therefore $b/s = bt/st \in S^{-1}\overline{A}$. □

Corollary 13.1.39. *Let A be an integral domain, $\overline{A}$ its integral closure and S a multiplicative subset such that $0 \notin S$. Then the integral closure of $S^{-1}A$ is $S^{-1}\overline{A}$.*

Proof. The field of fractions K of A is also the field of fractions of $S^{-1}A$ since $0 \notin S$, so Proposition 13.1.38 is then applied to K. □

Corollary 13.1.40. *Let A be an integral domain, K its field of fractions, R an algebra over K and B the integral closure of A in R. The elements of R which are algebraic over K are the elements of the form $a^{-1}b$ where $b \in B$ and $a \in A$. If L is the algebraic closure of K in R, then there exists a basis of L over K contained in B.*

Proof. The first assertion follows from Proposition 13.1.38 applied in the case $S = A - \{0\}$. If $(x_i)_{i\in I}$ is a basis of L over K, then there exists for all $i \in I$ an element a_i of A such that $a_i x_i \in B$. Then $(a_i x_i)_{i\in I}$ is also a basis of L over K. □

Proposition 13.1.41. *Let A be an integral domain. Then the following are equivalent:*

(i) A is integrally closed.

(ii) $A_\mathfrak{p}$ is integrally closed for each prime ideal $\mathfrak{p}$.

(iii) $A_\mathfrak{m}$ is integrally closed for each maximal ideal $\mathfrak{m}$.

Proof. It follows from Proposition 13.1.38 that the condition (iii) is necessary. The condition is sufficient, for $A = \bigcap_\mathfrak{m} A_\mathfrak{m}$ by Proposition 10.3.25 and it is sufficient to apply the Proposition 13.1.20. □

Corollary 13.1.42. *Let A be an integral domain, K its field of fractions and S a multiplicative subset of A such that $0 \notin S$.*

*(a) Let B be a subring of K which is integral over A and let $\mathfrak{f}$ be the annihilator of the A-module B/A (called the **conductor of A in B**). Then $S^{-1}\mathfrak{f}$ is contained in the conductor of $S^{-1}A$ in $S^{-1}B$ and is equal to it if B is a finitely generated A-module.*

(b) *Let $\overline{A}$ be the integral closure of A. For $S^{-1}A$ to be integrally closed, it is sufficient that the conductor $\mathfrak{f}$ of A in $\overline{A}$ meet S. This condition is also necessary if $\overline{A}$ is a finitely generated A-module.*

Proof. As $\mathfrak{f}B \subseteq A$, $(S^{-1}\mathfrak{f})(S^{-1}B) \subseteq S^{-1}A$ and hence $S^{-1}\mathfrak{f}$ is contained in $\mathrm{Ann}(S^{-1}B/S^{-1}A)$. If B is a finitely generated A-module, the equation $S^{-1}\mathfrak{f} = \mathrm{Ann}(S^{-1}B/S^{-1}A)$ is a special case of Proposition 10.2.32, $S^{-1}B/S^{-1}A$ being canonically identified with $S^{-1}(B/A)$. This proves (a).

By Proposition 13.1.38, $S^{-1}\overline{A}$ is the integral closure of $S^{-1}A$. As the relations $\mathfrak{f} \cap S \neq \varnothing$ and $S^{-1}\mathfrak{f} = S^{-1}A$ are equivalent, (b) is an immediate consequence of (a). □

Corollary 13.1.43. *Let A be an integral domain, $\overline{A}$ its integral closure and $\mathfrak{f}$ the conductor of A in $\overline{A}$. Suppose that $\overline{A}$ is a finitely generated A-module. Then the prime ideals $\mathfrak{p}$ of A such that $A_{\mathfrak{p}}$ is not integrally closed are those which contain $\mathfrak{f}$.*

13.1.5 Norms and traces of integral elements

Proposition 13.1.44. *Let A be a ring, B be an A-algebra, and T be a square matrix of order n over B. The following properties are equivalent:*

(i) *T is integral over A;*

(ii) *There exists a finitely generated sub-A-module M of B^n such that $T(M) \subseteq M$ and M is a system of generators of the B-module B^n.*

(iii) *The coefficients of the characteristic polynomial of T are integral over A.*

Proof. If $\chi(X)$ is the characteristic polynomial of X, the Cayley-Hamilton Theorem shows that $\chi(T) = 0$ and, as $\chi(X)$ is a monic polynomial, (iii) implies (i) by the transitivity of integrality. Suppose in the second place that (i) holds. If $e_1, \dots, e_n$ is the canonical basis of B^n, the sub-A-module M of B generated by the $T^k e_i$ is a finitely generated A-module, since the A-algebra $A[T]$ is a finitely generated A-module. As M contains the e_i, it is seen that (i) implies (ii). The converse is a consequence of Proposition 13.1.1.

Finally let us prove that (i) implies (iii). As T is integral over A and a fortiori over the polynomial ring $A[X]$, the polynomial $X - T$ is integral over $A[X]$ by Proposition 13.1.31. By Proposition 13.1.31, the problem is seen to reduce (by replacing T by $X - T$ and A by $A[X]$) to proving that, if T is integral over A, then $\det(T)$ is an element of B which is integral over A. Now, we have seen above that the endomorphism ϕ of B^n defined by the matrix T preserves a finitely generated sub-A-module M containing the e_i. Then $\bigwedge^n M$ is a finitely generated sub-A-module in $\bigwedge^n B^n$ containing $e_1 \wedge \cdots \wedge e_n$ and which is stable under $\wedge^n \phi$, in other words under the homothety of ratio $\det(T)$. As $e_1 \wedge \cdots \wedge e_n$ generates $\bigwedge^n B^n$, Proposition 7.1.1 then proves that $\det(T)$ is integral over A. □

Corollary 13.1.45. *Let A be an integral domain, K its field of fractions and L a finite dimensional K-algebra. If $x \in L$ is integral over A, then the coefieients of the characteristic polynomial of x over K are integral over A.*

Proof. Let h_x be the homothety of ratio x on L. Then by definition h_x is integral over A, and the characteristic polynomial of h_x is that of x over K. □

Corollary 13.1.46. *Let A be an integral domain, K its field of fractions and L a finite dimensional K-algebra. If $x \in L$ is integral over A, then $N_{L/K}(x)$ and $\mathrm{tr}_{L/K}(x)$ are integral over A.*

Proposition 13.1.47. *If L/K is a finite separable extension, then $(x, y) = \mathrm{tr}_{L/K}(xy)$ is a nondegenerate bilinear form on L.*

Proof. Let θ be a primitive element for L, so that $L = K(\theta)$. Then the bilinear form $(x, y) \mapsto \mathrm{tr}_{L/K}(xy)$ has matrix $G = (\mathrm{tr}_{L/K}(\theta^{i-1}\theta^{j-1}))$ under the basis $1, \theta, \dots, \theta^{n-1}$, . It is nondegenerate because, if $\theta_1 = \theta, \dots, \theta_n$ are the K-conjugates of θ, then

$$\det(G) = \prod_{i<j}(\theta_i - \theta_j) \neq 0.$$

This proves the claim. □

Theorem 13.1.48. *Let A be an integrally closed domain, K its quotient field, L a finite-dimensional separable K-algebra, and B the integral closure of A in L. There exists a basis $\{x_1, \dots, x_n\}$ of L over K such that B is contained in the A-module $\sum_i Ax_i$.*

The proposition will follow from the following more precise lemma:

Lemma 13.1.49. *Under the hypotheses of Theorem 13.1.48, let $(w_1, \dots, w_n)$ be a basis of L over K contained in B (Corollary 13.1.40); then there is a unique dual basis $(w_1^*, \dots, w_n^*)$ of L over K with respect to the trace form $\mathrm{tr}_{L/K}$; if $d = D_{L/K}(w_1, \dots, w_n)$ is the discriminant of the basis $(w_1, \dots, w_n)$, then $d \neq 0$ and*

$$\sum_{i=1}^{n} Aw_i \subseteq B \subseteq \sum_{i=1}^{n} Aw_i^* \subseteq d^{-1}\Big(\sum_{i=1}^{n} Aw_i\Big). \tag{1.5.1}$$

In particular, if d is invertible in A, B is a free A-module with basis $(w_1, \dots, w_n)$.

Proof. As L is a separable K-algebra, $d \neq 0$ by **??** and the K-bilinear form $\mathrm{tr}_{L/K}$ is non-degenerate. This shows the existence and uniqueness of the dual basis (w_i^*). This being so, the first inclusion of (1.5.1) is obvious. Let x be an element of B; let us write $x = \sum_{i=1}^n \xi_i w_i^*$ where $\xi_i \in K$; for all i, we have $\xi_i = \mathrm{tr}_{L/K}(xw_i)$, so ξ_i is integral over A (Corollary 13.1.46) and, as A is integrally closed, $\xi_i \in A$ for all i; this shows the second inclusion in (1.5.1). Finally, let us write $w_j^* = \sum_{i=1}^n \alpha_{ji} w_i$ where $\alpha_{ji} \in K$; then $\sum_{i=1}^n \alpha_{ji}\mathrm{tr}_{L/K}(w_i w_k) = \delta_{jk}$ for all j and k; Cramer's formulae show that the α_{ji} belong to $d^{-1}A$, whence the third inclusion (1.5.1). The last assertion follows immediate from (1.5.1), which in this case gives $B = \sum_{i=1}^n Aw_i$. □

Proof. We first notice that $L = S^{-1}B$, where $S = A - \{0\}$; that is, given any element x of L there exists a non-zero element s of A such that $sx \in B$: in fact, if $p(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ is the minimal polynomial of x over K, and if we take a common denominator s in A such that $sc_i = a_i \in A$, then we have

$$(sx)^n + a_{n-1}(sx)^{n-1} + \cdots + s^{n-1}a_0 = 0$$

and sx is integral over A. It follows from this observation that there exists a basis $\{u_1, \dots, u_n\}$ of L over K such that $u \in B$ for every i. Let $\{v_1, \dots, v_n\}$ be the dual basis of $\{u_1, \dots, u_n\}$ under the bilinear form $\mathrm{tr}(xy)$. If an element $x = \sum_j a_j x_j$ is in B, we have $xu_i \in B$ for every

i, whence $\mathrm{tr}(xu_i) \in A$ (A is integrally closed). Since $\mathrm{tr}(xu_i) = \sum_i a_i \mathrm{tr}(u_i v_j) = a_i$, we then have $B \subseteq \sum_j Av_j$. □

Corollary 13.1.50. *The assumptions being the same as in Theorem 13.1.48, let us furthermore assume that the ring A is Noetherian. Then B is a finite A-module and is a Noetherian ring.*

Proof. In fact, B is a submodule of the finite A-module $\sum_i Ax_i$, and is therefore a finite A-module. Thus B satisfies the a.c.c. as an A-module, and a fortiori satisfies the a.c.c. as an B-module. That is, B is Noetherian. □

Corollary 13.1.51. *The assumptions being the same as in Theorem 13.1.48, let us furthermore assume that A is a PID. Then there exists a basis $\{y_i\}$ of L over K such that $B = \sum_i Ay_i$.*

Proof. It was just shown that B is contained in an A-module generated by n elements x. Hence B has a basis consisting of n elements $\{y_i\}$, Since $L = S^{-1}B$, the set $\{y_i\}$ is necessarily also a basis of L over K. □

Corollary 13.1.51 is of particular importance for the case in which A is either the ring $\mathbb{Z}$ of rational integers, L being then an algebraic number field, or a polynomial ring $k[X]$ in one variable over a field k, L being then a field of algebraic functions of one variable. In the first case, the elements of L which are integral over $\mathbb{Z}$ are called the **algebraic integers** of the number field L; in the second case, the elements of L which are integral over $k[X]$ are called the **integral functions** of the function field L (with respect to the element X). Corollary 13.1.51 shows that these algebraic integers (or integral functions) are the linear combinations, with ordinary integral coefficients (or with coefficients in $k[X]$), of $n = [L : K]$ linearly independent algebraic integers y_i. Such a basis $\{y_i\}$ of L over the rational field (or over the rational function field $k(X)$) is called an **integral basis** of L.

Example 13.1.52. Let X be an indeterminate over a field k of characteristic $\neq 2$, and p an irreducible polynomial over k. Let $A = k[X]$ and $K = k(X)$, then the function field $L = k(X, Y)$ admits $\{1, Y\}$ as an integral basis (with respect to A). In fact, in the first place 1 and Y are integral over A. Furthermore, let f be an element of L which is integral over A. We write $f = a(X) + b(X)Y$ with $a, b \in k(X)$. Then the trace $2a(X)$ and the norm $a(X)^2 - b(X)^2 p(X)$ of f over $k(X)$ belong to $k[X]$, whence both $a(X)$ and $b(X)$ are polynomials, since otherwise $p(X)$ would be divisible by the square of the denominator of $b(X)$. Consequently, the integral closure of $A = k[X]$ in $L = k(X, Y)$ is the ring $k[X, Y]$.

Proposition 13.1.53. *Let k be a field, L a separable extension of k and A an integrally closed k-algebra. If the ring $L \otimes_k A$ is an integral domain, it is integrally closed.*

Proof. Let K be the field of fractions of A; as k is a field, $L \otimes_k A$ is canonically identified with a sub-k-algebra of $L \otimes_k K$ and L and A with sub-k-algebras of $L \otimes_k A$. Moreover, since an element $s \neq 0$ of A is not a divisor of 0 in A, $1 \otimes s$ is not a divisor of zero in $L \otimes_k A$ since L is flat over k; identifying s with $1 \otimes s$, it is therefore seen that, if $S = A \setminus \{0\}$, $L \otimes_k K$ is identified with $S^{-1}(L \otimes_k K)$; as $L \otimes_k A$ is assumed to be an integral domain, $L \otimes_k K$ is thus identified with a subring of the field of fractions Ω of $L \otimes_k A$.

First suppose that L is a *finite* extension of k; then $L \otimes_k K$ is an algebra of finite rank over K and by hypothesis has no divisor of 0; hence it is a field (it is sandwiched by K and Ω)

and it is in this case the field of fraction Ω of $L \otimes A$. Let $(w_1, \dots, w_n)$ be a basis of L over k, which is therefore also a basis of $L \otimes_k K$ over K. There exists a basis $(w_1^*, \dots, w_n^*)$ of L such that $\mathrm{tr}_{L/k}(w_i w_j^*) = \delta_{ij}$ (Lemma 13.1.49); every $z \in L \otimes_k K$ may be written uniquely $z = \sum_{i=1}^n a_i w_i$ where $a_i \in K$; then

$$\mathrm{tr}_{(L\otimes K)/K}(zw_j^*) = \sum_{i=1}^n a_i \mathrm{tr}_{(L\otimes K)/K}(w_i w_j^*)$$

and as in L the traces $\mathrm{tr}_{(L\otimes K)/K}$ and $\mathrm{tr}_{L/K}$ coincide, finally $\mathrm{tr}_{(L\otimes K)/K}(zw_j^*) = a_j$ for each j. Note on the other hand that the elements of L are integral over k and hence also over A; therefore $L \otimes_k A$ is integral over A (Corollary 13.1.17). This being so, suppose that $z \in L \otimes_k K$ is integral over $L \otimes_k A$; then z is integral over A, hence so is zw_j^* and therefore also $a_j = \mathrm{tr}_{L/K}(zw_j^*)$ for all j (Corollary 13.1.46). As A is integrally closed, $a_j \in A$ for all j and hence $z \in L \otimes_k A$, which proves the proposition in this case.

Suppose now that L is a finitely generated separable extension of k; then there exists a separating transcendence basis $(x_1, \dots, x_d)$ of L over k; as L and K are algebraically disjoint over k in the field Ω, the x_i are algebraically independent over K; hence $A[x_1, \dots, x_d]$ is integrally closed (Corollary 13.1.33). Let T be the set of nonzero elements of the ring $R = k[x_1, \dots, x_d] \subseteq L$, so that the field $k_1 = k(x_1, \dots, x_d) \subseteq L$ is equal to $T^{-1}R$; then

$$k_1 \otimes_k A = (T^{-1}R) \otimes_k A = T^{-1}R \otimes_R (R \otimes_k A) = T^{-1}(R \otimes_k A) = T^{-1}A[x_1, \dots, x_d]$$

by the associativity of the tensor product, hence this domain is integrally closed (Proposition 13.1.38). But $L \otimes_k A$ is identified with $L \otimes_{k_1} (k_1 \otimes_k A)$ and by definition L is a finite separable extension of k_1; it follows therefore from the preceding argument that $L \otimes_k A$ is integrally closed.

In the general case, if z is an element of Ω which is integral over $L \otimes_k A$, it satisfies a relation ofthe form $z^n + b_{n-1}z^{n-1} + \cdots + b_0 = 0$, where the b_i belong to $L \otimes_k A$; then there exists a finitely generated sub-extension L' of L over k such that the b_i belong to $L' \otimes_k A$ for all i and z to $L' \otimes_k K$. Then it follows from the previous argument that $z \in L' \otimes_k A$ and hence $L \otimes_k A$ is integrally closed. □

Remark 13.1.2. Let V be an affine irreducible algebraic variety over a field k and A the ring of functions regular on V defined over k; if A is integrally closed, V is called normal over k; Proposition 13.1.53 shows that, if V is normal over k, it remains normal over every separable extension L of k.

Corollary 13.1.54. *Let k be a field and A and B two integrally closed k-algebras. Suppose that the ring $A \otimes_k B$ is an integral domain and that the fields of fractions K and L of A and B respectively are separable over k. Then the ring $A \otimes_k B$ is an integrally closed domain.*

Proof. As A and B are identified with subalgebras of $A \otimes_k B$, K and L are identified with subfields of the field of fractions Ω of $A \otimes_k B$ which are linearly disjoint over k (**??**). It then follows from Proposition 13.1.53 that $A \otimes_k L$ and $K \otimes_k B$ are integrally closed domains; as their intersection is $A \otimes_k B$ (Proposition 7.2.17), $A \otimes_k B$ is an integrally closed domain (Proposition 13.1.20). □

13.1.6 Integers over a graded ring

All the graduations considered in this part are of type $\mathbb{Z}$; if A is a graded ring and $i \in \mathbb{Z}$, A_i denotes the set of homogeneous elements of degree i of the ring A. Let A be a graded ring and B a graded A-algebra. Let x be a homogeneous element of B which is integral over A; then there is a relation

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0 \quad a_i \in A.$$

Let $m = \deg(x)$ and let a'_i be the homogeneous componenet of degree $m(n-i)$ of a_i for each i; then obviously

$$x^n + a'_{n-1}x^{n-1} + \cdots + a'_0 = 0 \tag{1.6.1}$$

in other words x satisfies an equation of integral dependence with homogeneous coefficients.

Let $A[X, X^{-1}]$ denote the ring of fractions $S^{-1}A[X]$ of the polynomial ring $A[X]$ in one indeterminate, S being the multiplicative subset of $A[X]$ consisting of the powers X^n of X; as X is not a divisor of 0 in $A[X]$ it is immediate that the X^i's form a basis over A of the A-module $A[X, X^{-1}]$. For every element $a \in A$ with homogeneous components $(a_i)_{i\in\mathbb{Z}}$, we write

$$j_A(a) = \sum_{i\in\mathbb{Z}} a_i X^i \in A[X, X^{-1}]$$

it is immediate that $j_A : A \to A[X, X^{-1}]$ is an injective ring homomorphism.

Proposition 13.1.55. *Let $A = \bigoplus_{i\in\mathbb{Z}} A_i$ be a graded ring and B a graded A-algebra. Then the set R of elements of B integral over A is a graded subalgebra of B. Moreover, if $A_i = 0$ for $i < 0$ and R is a reduced ring, then $R_i = 0$ for $i < 0$.*

Proof. The diagram

$$\begin{tikzcd} A \arrow[r, "\rho"] \arrow[d, "j_A"] & B \arrow[d, "j_B"] \\ A[X, X^{-1}] \arrow[r, "\tilde{\rho}"] & B[X, X^{-1}] \end{tikzcd}$$

(where ρ is the homomorphism defining the A-algebra structure on B and $\tilde{\rho}$ the homomorphism canonically derived from it) is commutative, as is immediately verified from the definition. Let x be an element of B integral over A; then $j_B(x)$ is integral over $A[X, X^{-1}]$ (Proposition 13.1.6) and it therefore follows from Proposition 13.1.38 that there exists an integer $m > 0$ such that $X^m j_B(x)$ is an element of $B[X]$ integral over $A[X]$. We then deduce from Proposition 13.1.31 that the coefficients of the polynomial $X^m j_B(x)$ are integral over A; as these coefficients are by definition the homogeneous components of x, it is seen that these are integral over A, which proves that R is a graded subalgebra of B.

Suppose now that $x \in R_i$ where $i < 0$; the remark at the beginning of this part shows that x satisfies an equation of the form (1.6.1) where $a'_k \in A_{ki}$ for $1 \le k \le n$. If $A_j = 0$ for $j < 0$, then $x^n = 0$ and if B is a reduced ring we conclude that $x = 0$ and hence $R_i = 0$ for all $i < 0$ in this case. □

Recall that, if $A = \bigoplus_{i\in\mathbb{Z}} A_i$ is a graded ring and S is a multiplicative subset of A consisting of homogeneous elements, a graded ring structure is defined on $S^{-1}A$ by taking the set $(S^{-1}A)_i$

of homogeneous elements of degree i to be the set of elements of the form a/s, where $a \in A$ and $s \in S$ are homogeneous and such that $\deg(a) - \deg(s) = i$.

Lemma 13.1.56. *Let $A = \bigoplus_{i\in\mathbb{Z}} A_i$ be a graded integral domain and S the set of nonzero homogeneous elements of A.*

(a) Every nonzero homogeneous element of $S^{-1}A$ is invertible, the ring $K = (S^{-1}A)_0$ is a field and the set of $i \in \mathbb{Z}$ such that $(S^{-1}A)_i \neq 0$ is a subgroup $q\mathbb{Z}$ of $\mathbb{Z}$ (where $q \neq 0$).

(b) Suppose that $q \geq 1$ and let t be a non-zero element of $(S^{-1}A)_q$. Then the K-homomorphism f of the polynomial ring $K[X]$ to $S^{-1}A$ which maps X to t extends to an isomorphism of $K[X, X^{-1}]$ onto $S^{-1}A$ and $S^{-1}A$ is integrally closed.

Proof. The assertions in (a) follow immediately from the definitions and the hypothesis that A is an integral domain, for if a/s and b/t are two nonzero homogeneous elements of $S^{-1}A$ of degrees i and j, ab/st is a nonzero homogeneous element and of degree $i + j$. To show (b), we note that since t is invertible in $S^{-1}A$ the homomorphism f extends in a unique way to a homomorphism $\tilde{f} : K[X, X^{-1}] \to S^{-1}A$ and necessarily $\tilde{f}(X^{-1}) = t^{-1}$. On the other hand, by definition of q, every nonzero homogeneous element of $S^{-1}A$ is of degree qn ($n \in \mathbb{Z}$) and hence can be written uniquely in the form λt^n where $\lambda \in K$ (since $S^{-1}A$ is an integral domain); hence $\tilde{f}$ is bijective. Finally, we know that $K[X]$ is integrally closed and hence so is $K[X, X^{-1}]$ (Proposition 13.1.38), which completes the proof of the Lemma. □

Proposition 13.1.57. *Let $A = \bigoplus_{i\in\mathbb{Z}} A_i$ be a graded integral domain and S the set of nonzero homogeneous elements of A. The integral closure B of A is then a graded subring of $S^{-1}A$. If further $A_i = 0$ for $i < 0$, then $B_i = 0$ for $i < 0$.*

Proof. If $A = A_0$, the proposition is trivial. Otherwise we may apply Lemma 13.1.56; the ring $S^{-1}A$ is an integrally closed domain and therefore $B \subseteq S^{-1}A$; as $S^{-1}A$ is graded, so is B by Proposition 13.1.55; the latter assertion also follows from Proposition 13.1.55. □

Corollary 13.1.58. *With the hypotheses and notation of Proposition 13.1.57, if every homogeneous element of $S^{-1}A$ which is integral over A belongs to A, then A is integrally closed.*

Proof. Then $B_i \subseteq A$ for all $i \in \mathbb{Z}$, hence $B = A$. □

Corollary 13.1.59. *If $A = \bigoplus_{i\in\mathbb{Z}} A_i$ is an integrally closed graded domain, the domain A_0 is integrally closed.*

Proof. The field of fractions K_0 of A_0 is identified (in the notation of Proposition 13.1.57) with a subring of the ring of homogeneous elements of degree 0 of $S^{-1}A$; every element of K_0 integral over A_0 (and a fortiori over A) belongs therefore by hypothesis to A_0. □

Corollary 13.1.60. *Let $A = \bigoplus_{i\in\mathbb{Z}} A_i$ be an integrally closed graded domain. Then, for every integer $d > 0$, the ring $A^{(d)}$ is an integrally closed domain.*

Proof. Let U be the set of nonzero homogeneous elements of $A^{(d)}$ and let x be a homogencous element of $U^{-1}A^{(d)}$ integral over $A^{(d)}$ and hence over A; as $x \in S^{-1}A$, x belongs to A by hypothesis; as its degree is divisible by d, it belongs to $A^{(d)}$ and it then follows from Corollary 13.1.58 that $A^{(d)}$ is integrally closed. □

13.1.7 The lift of prime ideals

Let A, B be two rings and $\rho : A \to B$ a ring homomorphism. An ideal $\mathfrak{b}$ of B is said to **lie over** an ideal $\mathfrak{a}$ of A if $\mathfrak{a} = \rho^{-1}(\mathfrak{b})$.

To say that a prime ideal $\mathfrak{P}$ of B lies over an ideal $\mathfrak{p}$ of A therefore means that $\mathfrak{p}$ is the image of $\mathfrak{P}$ under the continuous mapping $f^* : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ associated with f. Note that for there to exist an ideal of B lying over the ideal (0) of A, it is necessary and sufficient that $\rho : A \to B$ be injective.

Let $\mathfrak{a}$ be an ideal of A. By taking quotients the homomorphism ρ gives a homomorphism $\bar{\rho} : A/\mathfrak{a} \to B/\mathfrak{b}$. To say that $\mathfrak{b}$ is an ideal of B lying over $\mathfrak{a}$ is equivalent to saying that $\mathfrak{a}B \subseteq \mathfrak{b}$ and that $\mathfrak{b}/\mathfrak{a}A$ is an ideal of $B/\mathfrak{a}B$ lying over (0).

Lemma 13.1.61. *Let $\rho : A \to B$ be a ring homomorphism, S a multiplicative subset of A, i_A^S and i_B^S the canonical homomorphisms, so that there is a commutative diagram*

$$\begin{tikzcd} A \arrow[r, "\rho"] \arrow[d, "i_A^S"] & B \arrow[d, "i_B^S"] \\ S^{-1}A \arrow[r, "S^{-1}\rho"] & S^{-1}B \end{tikzcd}$$

Let $\mathfrak{p}$ be a prime ideal of A such that $\mathfrak{p} \cap S = \varnothing$. Then $\mathfrak{b} \mapsto S^{-1}\mathfrak{b}$ is a bijective map of the set of ideals of B lying over $\mathfrak{p}$ and saturated with S onto the set of ideals of $S^{-1}B$ lying over $S^{-1}\mathfrak{p}$. In particular $\mathfrak{P} \mapsto S^{-1}\mathfrak{P}$ is a bijection on the set of prime ideals of B lying over $\mathfrak{p}$ onto the set of prime ideals of $S^{-1}B$ lying over $S^{-1}\mathfrak{p}$.

Proof. This follows from Proposition 10.2.36 and Proposition 10.2.27. □

Proposition 13.1.62. *Let $A \subseteq B$ be integral domains, B integral over A. Then B is a field if and only if A is a field.*

Proof. IfA is a field, then, for all nonzero y in B, $A[y]$ is by hypothesis a finitely generated A-module. As $A[y]$ is an integral domain, it is a field and a fortiori y is invertible in B and hence B is a field. Conversely, suppose that B is a field and let x be nonzero in A. As $x^{-1} \in B$ and B is integral over A, there is an equation of integral dependence

$$x^{-n} + a_{n-1}z^{-(n-1)} + \cdots + a_0 = 0$$

where the $a_i \in A$; now this relation shows that

$$-z^{-1} = a_{n-1} + a_{n-2}z + \cdots + a_0 z^{n-1} \in A,$$

hence A is a field. □

Corollary 13.1.63. *Let $\rho : A \to B$ be a ring homomorphism such that B is integral over A, $\mathfrak{P}$ a prime ideal of B and $\mathfrak{p} = f^{-1}(\mathfrak{P})$. For $\mathfrak{p}$ to be maximal, it is necessary and sufficient that $\mathfrak{P}$ be so.*

Proof. Let $\bar{\rho} : A/\mathfrak{p} \to B/\mathfrak{P}$ be the homomorphism derived from f by taking quotients. Then $A/\mathfrak{p}$ and $B/\mathfrak{P}$ are integral domains and $B/\mathfrak{P}$ is integral over $A/\mathfrak{p}$. To say that $\mathfrak{p}$ (resp. $\mathfrak{P}$) is maximal means that $A/\mathfrak{p}$ (resp. $B/\mathfrak{P}$) is a field. The corollary then follows from Proposition 13.1.62. □

Corollary 13.1.64. *Let $\rho : A \to B$ a ring homomorphism such that B is integral over A, $\mathfrak{p}$ a prime ideal of A and $\mathfrak{P}_1$ and $\mathfrak{P}_2$ two ideals of B lying over $\mathfrak{p}$ such that $\mathfrak{P}_1 \subseteq \mathfrak{P}_2$. If $\mathfrak{P}_1$ is prime, then $\mathfrak{P}_1 = \mathfrak{P}_2$.*

Proof. Let us write $S = A - \mathfrak{p}$. Then $S^{-1}B$ is integral over $S^{-1}A$ by Proposition 13.1.38, $S^{-1}\mathfrak{p}$ is a maximal ideal of $S^{-1}A$, $S^{-1}\mathfrak{P}_1$ and $S^{-1}\mathfrak{P}_2$ are ideals of $S^{-}B$ lying over $S^{-1}\mathfrak{p}$ and $S^{-1}\mathfrak{P}_1 \subseteq S^{-1}\mathfrak{P}_2$. As $S^{-1}\mathfrak{P}_1$ and $S^{-1}\mathfrak{P}_2$ are prime, they are maximal by Corollary 13.1.63 and hence $S^{-1}\mathfrak{P}_1 = S^{-1}\mathfrak{P}_2$. Therefore $\mathfrak{P}_1 = \mathfrak{P}_2$. □

Corollary 13.1.65. *Let B be an integral domain, A a subring of B such that B is integral over A and f a homomorphism from B to a ring C. If the restriction of f to A is injective, then f is injective.*

Proof. If $\mathfrak{b}$ is the kernel of f, the hypothesis means that $\mathfrak{b} \cap A = (0)$. As B is an integral domain, Corollary 13.1.64 may be applied taking $\mathfrak{p}$ and $\mathfrak{P}_1$ to be the ideal (0) of A and the ideal (0) of B respectively, whence $\mathfrak{b} = (0)$. □

Corollary 13.1.66. *Let $A \subseteq B$ be rings, B integral over A and $\mathfrak{m}$ a maximal ideal of A. Suppose that there are only finitely many distinct maximal ideals $\mathfrak{M}_1, \dots, \mathfrak{M}_s$ in B lying over $\mathfrak{m}$. Let $\mathfrak{Q}_i$ be the saturation of $\mathfrak{m}B$ with respect to $\mathfrak{M}_i$. Then:*

(a) In the ring $B/\mathfrak{Q}_i$, the zero divisors are the elements of $\mathfrak{M}_i/\mathfrak{Q}_i$, and they are nilpotent.

(b) $\mathfrak{m}B = \bigcap_{i=1}^{s} \mathfrak{Q}_i = \prod_{i=1}^{s} \mathfrak{Q}_i$.

(c) The canonical homomorphism $B/\mathfrak{m}B \to \prod_{i=1}^{s} B/\mathfrak{Q}_i$ is an isomorphism.

Proof. For a prime ideal of B to contain $\mathfrak{m}B$, it is necessary and sufficient that its intersection with A contains $\mathfrak{m}$, and hence that it lies over $\mathfrak{m}$, since $\mathfrak{m}$ is maximal in A. Therefore $\mathfrak{M}_i$ are therefore the only prime ideals of B containing $\mathfrak{m}B$ and therefore $\sqrt{\mathfrak{m}B} = \bigcap_{i=1}^{s} \mathfrak{M}_i$. By definition of $\mathfrak{Q}_i$, the image of an element of $B - \mathfrak{M}_i$ in $B/\mathfrak{Q}_i$ is not a divisor of 0. On the other hand, as the $\mathfrak{M}_i$ are distinct maximal ideals, for every index i there exists an element a_i belonging to $\bigcap_{j \neq i} \mathfrak{M}_j$ and not to $\mathfrak{M}_i$. Then for all $x \in \mathfrak{M}_i$ we have $a_i x \in \sqrt{\mathfrak{m}B}$, hence the image of $a_i x$ in $B/\mathfrak{Q}_i$ is nilpotent, and, as that of a_i is not a divisor of 0, we conclude that the image of x is nilpotent. In other words $\mathfrak{M}_i$ is the radical of $\mathfrak{Q}_i$ and proves (a).

It follows that $\mathfrak{Q}_i$ are relatively coprime in pair, and (c) will be a concequence of (b). To establish (b), we note that in the ring $B/\mathfrak{m}B$ the $\mathfrak{M}_j/\mathfrak{m}B$ are the only maximal ideals and $\mathfrak{Q}_j/\mathfrak{m}B$ is the saturation of (0) with respect to $\mathfrak{M}_j/\mathfrak{m}B$. We may therefore restrict our attention to the case $\mathfrak{m}B = (0)$. The assertion of (b) then follows from Proposition 10.3.19, by the definition of a saturation of (0). □

Theorem 13.1.67. *Let $\rho : A \to B$ be a ring homomorphism such that B is integral over A and let $\mathfrak{p}$ be a prime ideal of A containing* $\ker \rho$. *Then there exists a prime ideal $\mathfrak{P}$ of B such that $\mathfrak{P} \cap A = \mathfrak{p}$.*

Proof. By consider the image $\rho(A)$ in B, we may assume that ρ is injective. Suppose first that A is a local ring and $\mathfrak{p}$ the maximal ideal of A. Then, for every maximal ideal $\mathfrak{M}$ of B, $\mathfrak{M}^c$ is a maximal ideal of A and hence equal to $\mathfrak{p}$, which proves the theorem in this case (since B contains A by hypothesis and is therefore not reduced to 0). In the general case, let us write $S = A - \mathfrak{p}$, then $S^{-1}A$ is a local ring whose maximal ideal is $S^{-1}\mathfrak{p}$, $S^{-1}f : S^{-1}A \to S^{-1}A$ is injective and $S^{-1}B$ is integral over $S^{-1}A$. Then there exists a prime ideal $\mathfrak{P}'$ of $S^{-1}B$ lying over $S^{-1}\mathfrak{p}$ and we know that $\mathfrak{P}' = S^{-1}\mathfrak{P}$ where $\mathfrak{P}$ is a prime ideal of B lying over $\mathfrak{p}$ by Lemma 13.1.61. □

Corollary 13.1.68. *Let $\rho : A \to B$ be a ring homomorphism such that B is integral over A, $\mathfrak{a}$ and $\mathfrak{p}$ two ideals of A such that $\mathfrak{a} \subseteq \mathfrak{P}$ and $\mathfrak{b}$ an ideal of B lying over $\mathfrak{a}$. Suppose that $\mathfrak{p}$ is prime, then there exists a prime ideal $\mathfrak{P}$ of B lying over $\mathfrak{p}$ and containing $\mathfrak{b}$.*

Proof. If $\bar{\rho} : A/\mathfrak{a} \to B/\mathfrak{b}$ is the homomorphism derived from f by taking quotients, then $\bar{\rho}$ is injective by hypothesis and $B/\mathfrak{b}$ is integral over $A/\mathfrak{a}$, so the claim follows from Theorem 13.1.67. □

Corollary 13.1.69. *Let A be a ring and B a ring containing A and integral over A. Then there exists one-to-one correspondence between maximal ideals of A and maximal ideals of B.*

Proof. This follows from Corollary 13.1.63 and Theorem 13.1.67. □

Corollary 13.1.70. *Let A be a ring and B a ring containing A and integral over A. If $\mathfrak{R}$ is the Jacobson radical of B, then $\mathfrak{R} \cap A$ is the Jacobson radical of A.*

Corollary 13.1.71 (Going-up theorem). *Let A be a ring and B a ring containing A and integral over A. Let $\mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n$ be a chain of prime ideals of A and $\mathfrak{P}_1 \subset \cdots \subset \mathfrak{P}_m$ a chain of prime ideals of B such that $\mathfrak{P}_i \cap A = \mathfrak{p}_i$ for $1 \leq i \leq m$ and $m < n$. Then the chain $\mathfrak{P}_1 \subset \cdots \subset \mathfrak{P}_m$ can be extended to a chain $\mathfrak{P}_1 \subset \cdots \subset \mathfrak{P}_n$ such that $\mathfrak{P}_i \cap A = \mathfrak{p}_i$ for $1 \leq i \leq n$.*

Proof. By induction we reduce immediately to the case $m = 1$, $n = 2$, and this follows from Corollary 13.1.68. □

Corollary 13.1.72. *Let $\rho : A \to B$ be a ring homomorphism such that B is integral over A. Then the associated continuous mapping $\rho^* : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is closed.*

Proof. For every ideal $\mathfrak{b}$ of B, $B/\mathfrak{b}$ is integral over B, hence also over A and $\mathrm{Spec}(B/\mathfrak{b})$ is identified with the closed subspace $V(\mathfrak{b})$ of $\mathrm{Spec}(B)$. To show that ρ^* is closed, we see then (replacing B by $B/\mathfrak{b}$) that it is sufficient to prove that the image of $\mathrm{Spec}(B)$ under ρ^* is a closed subset of $\mathrm{Spec}(A)$. Now it follows from Theorem 13.1.67 that this image is just the set of prime ideals of A containing the ideal $\ker \rho$ and this set is closed by definition of the topology on $\mathrm{Spec}(A)$. □

Corollary 13.1.73. *Let A be a ring, B a ring containing A and integral over A and ϕ a homomorphism from A to an algebraically closed field Ω. Then ϕ can be extended to a homomorphism from B to Ω.*

Proof. Let $\mathfrak{p}$ be the kernel of ϕ, which is a prime ideal since $\phi(A) \subseteq \Omega$ is an integral domain. Let $\mathfrak{P}$ be a prime ideal of B lying over $\mathfrak{p}$. Then $A/\mathfrak{p}$ is canonically identified with a subring of $B/\mathfrak{P}$ and $B/\mathfrak{P}$ is integral over $A/\mathfrak{p}$. The homomorphism ϕ defines, by taking the quotient, an isomorphism of $A/\mathfrak{p}$ onto the subring $\phi(A)$ of Ω, which can be extended to an isomorphism ψ of the field of fractions K of $A/\mathfrak{p}$ onto a subfield of Ω. As the field of fractions L of $B/\mathfrak{P}$ is algebraic over K, ψ can be extended to an isomorphism ψ' of L onto a subfield of Ω. If $\pi : B \to B/\mathfrak{P}$ is thc canonical homomorphism, $\psi' \circ \pi$ is a homomorphism from B to Ω extending ϕ. □

Proposition 13.1.74. *Let $\rho : A \to B$ be a ring homomorphism such that B is integral over A, $\mathfrak{p}$ a prime ideal of A, and $S = A - \mathfrak{p}$. If $(\mathfrak{P}_i)_{i \in I}$ is the family of all the prime ideals of B lying over $\mathfrak{p}$ and $T = \bigcap_{i \in I}(B - \mathfrak{P}_i)$, then $S^{-1}B = T^{-1}B$.*

Proof. By definition $\rho(S) \subseteq T$ and, as $\rho(S)^{-1}B = S^{-1}B$, it suffices to prove, by virtue of Proposition 10.2.23, that, if a prime ideal $\mathfrak{Q}$ of B does not meet $\rho(S)$, it does not meet T either. Now, suppose that $\mathfrak{Q} \cap \rho(S) = \varnothing$ and let $\mathfrak{q} = \rho^{-1}(\mathfrak{Q})$. Then $\mathfrak{q} \cap S = \varnothing$, in other words $\mathfrak{q} \subseteq \mathfrak{p}$. As $\mathfrak{Q}$ lies over $\mathfrak{q}$ by definition, it follows from Corollary 13.1.68 that there is an index i such that $\mathfrak{Q}_i \subseteq \mathfrak{p}_i$ and hence $\mathfrak{Q} \cap T = \varnothing$, which completes the proof. □

Corollary 13.1.75. *Let A be an integral domain, $\overline{A}$ its integral closure, and $\mathfrak{p}$ a prime ideal of A. If $(\mathfrak{P}_i)_{i\in I}$ is the family of all prime ideals of $\overline{A}$ lying over $\mathfrak{p}$ and $T = \bigcap_{i\in I}(\overline{A} - \mathfrak{P}_i)$, then $T^{-1}\overline{A}$ is the integral closure of $A_\mathfrak{p}$.*

Proof. By Proposition 13.1.38, the integral closure of $A_\mathfrak{p}$ is $\overline{A}_\mathfrak{p}$, which equals to $T^{-1}\overline{A}$ by Proposition 13.1.74. □

Proposition 13.1.76. *Let $\rho : A \to B$ be a ring homomorphism sueh that B is a finitely generated A-module. Then, for every prime ideal $\mathfrak{p}$ of A, the set of prime ideals of B lying over $\mathfrak{p}$ is finite.*

Proof. By taking localization and quotient, we may reduce the problem to $\mathfrak{p} = (0)$ and A is a field. The ring B is then an A-algebra of finite rank and therefore Artinian and we know that in such an algebra there is only a finite number of prime ideals. □

Proposition 13.1.77. *Let A be an integrally closed domain and B a ring containing A and integral over A. Suppose that B is a torsion-free A-module. Let $\mathfrak{p} \subseteq \mathfrak{q}$ be two prime ideals of A and $\mathfrak{Q}$ a prime ideal of A lying over $\mathfrak{q}$. Then there exists a prime ideal $\mathfrak{P}$ of B lying over $\mathfrak{p}$ and such that $\mathfrak{P} \subseteq \mathfrak{Q}$.*

Proof. Suppose first that B is an integral domain. Let K, L be the fields of fractions of A and B respectively. Let Ω be the algebraic closure of L and $\overline{A}$ the integral closure of A in Ω, so that $A \subseteq B \subseteq \overline{A}$. Let $\mathcal{P}$ be a prime ideal of $\overline{A}$ lying over $\mathfrak{p}$, then by Corollary 13.1.68 there is a prime ideal $\mathcal{Q}$ of $\overline{A}$ lying over $\mathfrak{q}$ and such that $\mathcal{P} \subseteq \mathcal{Q}$. Finally let $\mathcal{Q}_1$ be a prime ideal of $\overline{A}$ lying over $\mathfrak{Q}$. By Proposition 13.2.14, there exists a K-automorphism σ of Ω such that $\sigma(\mathcal{Q}) = \mathcal{Q}_1$. Then $\sigma(\mathcal{P})$ is a prime ideal of $\overline{A}$ lying over $\mathfrak{p}$ such that $\sigma(\mathcal{P}) \subseteq \mathcal{Q}_1$ and hence $\mathfrak{P} = B \cap \sigma(\mathcal{P})$ is a prime ideal of B lying over $\mathfrak{p}$ and contained in $\mathfrak{Q}$.

$$\begin{tikzcd}
\sigma(\mathcal{P}) \arrow[rr, hook] \arrow[dd, dash] & & \mathcal{Q}_1 \arrow[dd, dash] & \\
& \mathcal{P} \arrow[ul, "\sigma"'] \arrow[rr, hook] \arrow[dd, dash] & & \mathcal{Q} \arrow[ul, "\sigma"'] \arrow[dd, dash] \\
\mathfrak{P} \arrow[rr, hook] \arrow[dd, dash] & & \mathfrak{Q} \arrow[dd, dash] & \\
& & & \\
\mathfrak{p} \arrow[rr, hook] \arrow[dr, equal] & & \mathfrak{q} \arrow[dr, equal] & \\
& \mathfrak{p} \arrow[rr, hook] & & \mathfrak{q}
\end{tikzcd}$$

We pass to the general case. As A is an integral domain and $\mathfrak{Q}$ is prime, the subsets $A \setminus \{0\}$ and $B \setminus \mathfrak{Q}$ of B are multiplicative; then their product $S = (A \setminus \{0\})(B \setminus \mathfrak{Q})$ is a multiplicative subset of B which does not contain 0 since the non-zero elements of A are not divisors of 0 in B. Then there exists a prime ideal $\mathfrak{M}$ of B disjoint from S, in other words such that $\mathfrak{M} \subseteq \mathfrak{Q}$ and $\mathfrak{M} \cap A = 0$. Let π be the canonical homomorphism $B \to B/\mathfrak{M}$. Then the restriction of π to A is injective and hence $\pi(A)$ is integrally closed. Since $B/\mathfrak{M}$ is an integral domain, the first part of the proof proves that there exists a prime ideal $\mathfrak{N}$ of $B/\mathfrak{M}$ such that $\mathfrak{N} \cap \pi(A) = \pi(\mathfrak{p})$ and

$\mathfrak{N} \subseteq \pi(\mathfrak{Q})$. The ideal $\mathfrak{P} = \pi^{-1}(\mathfrak{N})$ is a prime ideal of B and $\mathfrak{P} \subseteq \mathfrak{Q}$, since $\mathfrak{Q}$ contains the kernel of π. As π is injective on A, we see $\mathfrak{P} \cap A = \mathfrak{p}$. □

Corollary 13.1.78 (Going-down theorem). *Let A be an integrally closed domain and B a ring containing A and integral over A. Suppose that B is a torsion-free A-module. Let $\mathfrak{p}_1 \supseteq \cdots \supseteq \mathfrak{p}_n$ be a chain of prime ideals of A and $\mathfrak{P}_1 \supseteq \cdots \supseteq \mathfrak{P}_m$ a chain of prime ideals of B such that $\mathfrak{P}_i \cap A = \mathfrak{p}_i$ for $1 \leq i \leq m$ and $m < n$. Then the chain $\mathfrak{P}_1 \supseteq \cdots \supseteq \mathfrak{P}_m$ can be extended to a chain $\mathfrak{P}_1 \supseteq \cdots \supseteq \mathfrak{P}_n$ such that $\mathfrak{P}_i \cap A = \mathfrak{p}_i$ for $1 \leq i \leq n$.*

Corollary 13.1.79. *let $\mathfrak{p}$ be a prime ideal of A. The prime ideals of B lying over $\mathfrak{p}$ are the minimal elements of the set $\mathcal{E}$ of prime ideals of B containing $\mathfrak{p}B$.*

Proof. A prime ideal of B lying over $\mathfrak{p}$ is minimal in $\mathcal{E}$ by virtue of Corollary 13.1.64. Conversely, let $\mathfrak{Q}$ be a minimal element of $\mathcal{E}$. As $\mathfrak{Q} \cap A \supseteq \mathfrak{p}$, the going down theorem shows that there exists a prime ideal $\mathfrak{P}$ of B lying over $\mathfrak{p}$ such that $\mathfrak{P} \subseteq \mathfrak{Q}$. As $\mathfrak{P}$ contains $\mathfrak{p}B$, the hypothesis made on $\mathfrak{Q}$ implies that $\mathfrak{P} = \mathfrak{Q}$ and hence $\mathfrak{Q}$ lies over $\mathfrak{p}$. □

Proposition 13.1.80. *Let $\rho : A \to B$ be a flat homomorphism of rings. Then ρ has the going-down property.*

Proof. Let $\mathfrak{p}_1 \subseteq \mathfrak{p}$ be prime ideals in A, $\mathfrak{P}$ a prime ideal in B such that $\mathfrak{P} \cap A = \mathfrak{p}$. Consider the localization $A_\mathfrak{p}$ and $B_\mathfrak{P}$. From Corollary 10.2.42 we know the map $\rho^* : \mathrm{Spec}(B_\mathfrak{P}) \to \mathrm{Spec}(A_\mathfrak{p})$ is surjective, hence there is a prime ideal $\mathfrak{P}_1'$ lying over $\mathfrak{p}_1$. Contracting $\mathfrak{P}_1'$ to B gives the desired prime ideal. □

Theorem 13.1.81. *Let $A \subseteq B$ be integral domains such that A is integrally closed and B is integral over A. Let $\phi : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ be the canonical map. For $b \in B$, let*

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$$

be a monic polynomial with coefficients in A having b as a root and of minimal degree. Then

$$\phi(D(b)) = \bigcup_{i=1}^{n} D(a_i).$$

In particular, ϕ is an open map.

Proof. By hypothesis, f is the minimal polynomial of b over the field of fraction of A. If we set $C = A[b]$ then $C \cong A[X]/(f(X))$ is a free A-module with basis $1, b, b^2, \ldots, b^{n-1}$ and is hence faithfully flat over A. Suppose that $\mathfrak{P} \in D(b)$, so that $\mathfrak{P} \in \mathrm{Spec}(B)$ with $b \notin \mathfrak{P}$, and set $\mathfrak{p} = \mathfrak{P} \cap A$. Then $\mathfrak{p} \in \bigcup_i D(a_i)$, since otherwise $a_i \in \mathfrak{p}$ for all i, and so $b^n \in \mathfrak{P}$, hence $b \in \mathfrak{P}$, which is a contradiction. So we have $\phi(D(b)) \subseteq \bigcup_{i=1}^n D(a_i)$.

Conversely, let $\mathfrak{p} \in \bigcup_i D(a_i)$ and let $\mathcal{P}$ be a prime of C lying over $\mathfrak{p}$ and $\mathfrak{P}$ a prime of B lying over $\mathcal{P}$. Suppose that $b \in \sqrt{\mathfrak{p}C}$, then for sufficiently large m we have

$$b^m = \sum_{i=1}^{n} p_i b^i, \quad p_i \in \mathfrak{p}.$$

By the assumption on $f(X)$ we must have $m \geq n$. Then $X^m - \sum_{i=1}^n p_i X^i$ is divisible by $f(X)$ in $A[X]$, which implies that X^m is divisible by $\overline{f}(X) = X^n + \sum_{i=1}^{n-1} \overline{a}_i X^i$ in $(A/\mathfrak{p})[X]$; since at least one of the $\overline{a}_i$ is nonzero, this is a contradiction.

Thus $b \notin \sqrt{\mathfrak{p}C}$ and there exists some $\mathcal{P}_1 \in \operatorname{Spec}(C)$ with $b \notin \mathcal{P}_1$ and $\mathfrak{p}C \subset \mathcal{P}_1$. By Corollary 13.1.79 we have $\mathcal{P} \subseteq \mathcal{P}_1$, so $\mathfrak{P} \in D(b)$ since otherwise $b \in \mathfrak{P} \cap C = \mathcal{P} \subseteq \mathcal{P}_1$, which is a contradiction. This proves $\phi(D(b)) = \bigcup_{i=1}^n D(a_i)$. Since any open set of $\operatorname{Spec}(B)$ is a union of open sets of the form $D(a)$, it follows that ϕ is open. □

Proposition 13.1.82. *A ring homomorphism $\rho : A \to B$ is said to have the **going-up property** (resp. the **going-down property**) if the conclusion of the going-up theorem (resp. the going-down theorem) holds for B and its subring $\rho(A)$. Let $\rho^* : \operatorname{Spec}(B) \to \operatorname{Spec}(A)$ be the mapping associated with ρ.*

(1) Consider the following three statements:

(a) ρ^* is a closed mapping.

(b) ρ has the going-up property.

(c) Let $\mathfrak{P}$ be any prime ideal of B and let $\mathfrak{p} = \mathfrak{P}^c$. Then $\rho^* : \operatorname{Spec}(B/\mathfrak{P}) \to \operatorname{Spec}(A/\mathfrak{p})$ is surjective.

Then we have (a)⇔(b)⇔(c).

(2) Consider the following three statements:

(a′) ρ^* is an open mapping.

(b′) ρ has the going-down property.

(c′) Let $\mathfrak{P}$ be any prime ideal of B and let $\mathfrak{p} = \mathfrak{P}^c$. Then $\rho^* : \operatorname{Spec}(B_{\mathfrak{P}}) \to \operatorname{Spec}(A_{\mathfrak{p}})$ is surjective.

Then we have (a′)⇒(b′)⇔(c′).

Proof. The equivalences (b)⇔(c) and (b′)⇔(c′) are clear. For (a)⇒(b), assume that ρ^* is closed, we claim that $\rho^*(V(\mathfrak{P})) = V(\mathfrak{p})$ if $\mathfrak{p} = \mathfrak{P}^c$. To see this, we note that since ρ^* is closed, $\rho^*(V(\mathfrak{P}))$ is closed and contains $\mathfrak{p}$, so $V(\mathfrak{p}) = \overline{\{\mathfrak{p}\}} \subseteq \rho^*(V(\mathfrak{P}))$. But $\mathfrak{P}' \supseteq \mathfrak{P}$ implies $(\mathfrak{P}')^c \supseteq \mathfrak{P}^c = \mathfrak{p}$, hence we also have $\rho^*(V(\mathfrak{P})) \subseteq V(\mathfrak{p}_1)$, and therefore $\rho^*(V(\mathfrak{P})) = V(\mathfrak{p})$. In particular, the map ρ^* is surjective on $V(\mathfrak{p})$, so if $\mathfrak{p} \subseteq \mathfrak{p}'$ then $\mathfrak{p}' \in V(\mathfrak{p})$ and there is a $\mathfrak{P}' \in V(\mathfrak{P})$ such that $(\mathfrak{P}')^c = \mathfrak{p}'$.

For (a′)⇒(c′), we first prove the following *downward property*: If $\mathfrak{p}' \subseteq \mathfrak{p}$ and $\mathfrak{p} \in U$ for open set U, then $\mathfrak{p}' \in U$. In fact, write $U = X \setminus C$ where C is closed, then $\mathfrak{p}' \in C$ would implies $V(\mathfrak{p}') = \overline{\{\mathfrak{p}'\}} \subseteq C$ since C is closed. But $\mathfrak{p} \in V(\mathfrak{p}')$ is not in C, contrdiction. By this property, if $\rho^*(U)$ is open, then for any $\mathfrak{p}' \supseteq \mathfrak{p}$ in A and $\mathfrak{P}$ in B such that $\mathfrak{P}^c = \mathfrak{p}$. Then let U be a neighborhood of $\mathfrak{P}$ in B, so $\rho^*(B)$ is a neighbrhood of $\mathfrak{p}_1$ in A. Now since $\mathfrak{p}' \subseteq \mathfrak{p}$, we conclude $\mathfrak{p}' \in f(U)$, so $\mathfrak{p}'$ has a preimage $\mathfrak{P}'$. This shows the map $\rho^* : \operatorname{Spec}(B_{\mathfrak{P}}) \to \operatorname{Spec}(A_{\mathfrak{p}})$ is surjective.

Now assume the going up property, we show that ρ^* is closed. To this end, let $V(\mathfrak{b})$ be a closed subset of $\operatorname{Spec}(B)$. Since $V(\mathfrak{b})$ is identified with $\operatorname{Spec}(B/\mathfrak{b})$ and the induced map $A/\mathfrak{a} \to B/\mathfrak{b}$ satisfies the going up property (where $\mathfrak{a} = \mathfrak{b}^c$), we only need to show the image of $\operatorname{Spec}(B)$ under ρ^* is closed. For this, let T be the image of ρ^*, and let $\mathfrak{p} \in \operatorname{Spec}(A)$ be in the closure of T. This means for every $f \in A - \mathfrak{p}$ we have $D(f) \cap T \neq \varnothing$. Note that $D(f) \cap T$ is the image of $\operatorname{Spec}(B_f)$ in $\operatorname{Spec}(A)$. Hence we conclude that $B_f \neq 0$. Since $B_{\mathfrak{p}}$ is the directed limit of the

rings B_f with $f \in A - \mathfrak{p}$, we conclude that $B_\mathfrak{p} \neq 0$ by Exercise 7.1.10. If $\mathcal{P}'$ is a prime ideal of $B_\mathfrak{p}$, then $\mathfrak{p}' = \mathcal{P}' \cap A$ is a prime ideal of A such that $\mathfrak{p}' \subseteq \mathfrak{p}$, and it is in the image of ρ^* since $\mathfrak{P}' \cap A = \mathfrak{p}'$, where $\mathfrak{P}' = (i_B^\mathfrak{p})^{-1}(\mathcal{P}')$. As we assumed that ρ satisfies the going up property, there exist a prime ideal $\mathfrak{P}$ of B lying over $\mathfrak{p}$, whence $\mathfrak{p} \in T$ and T is closed. □

13.2 Group action on algebras

13.2.1 Group acting on an algebra

Given a ring R, a R-algebra A and a group G acting on A, we shall say the action of G is ***R*-linear** or G is a R-action if for each $\sigma \in G$, the map $x \mapsto \sigma(x)$ is an endomorphism of the R-algebra A. We shall denote by A^G the set of elements of A which are invariant under G. Clearly it is a sub-R-algebra of A. We shall say that the **action is locally finite** if every orbit of G in A is finite.

Proposition 13.2.1. *Let A be a R-algebra and G a locally finite R-action on A. Then A is integral over the subalgebra A^G.*

Proof. For all $x \in A$, let $x_1, \dots, x_n$ be the distinct elements of the orbit of x under G. For all $\sigma \in G$, there exists a permutation $\pi_\sigma \in \mathfrak{S}_n$ such that $\sigma(x_i) = x_{\pi_\sigma(i)}$ for $1 \leq i \leq n$. Therefore the elementary symmetric functions of the x_i are elements of A which are invariant under G, in other words elements of A^G. As x is a root of the monic polynomial $\prod_i (X - x_i)$ and the coefficients of this polynomial belong to A^G, x is integral over A^G. □

Theorem 13.2.2. *Let A be a finitely generated R-algebra and G a locally finite R-action on A. Then A is a finitely generated A^G-module. If further R is Noetherian, A^G is a finitely generated R-algebra.*

Proof. Let $a_1, \dots, a_n$ generate the R-algebra A. Then we see $A = A^G[a_1, \dots, a_n]$ and the a_i are integral over A^G by Proposition 13.2.1, the first assertion follows. The second is a consequence of the following lemma:

Let A be a Noetherian ring, B a finitely generated A-algebra and C a sub-A-algebra of B such that B is integral over C. Then C is a finitely generated A-algebra. (2.1.1)

To prove the lemma, let $x_1, \dots, x_n$ be a finite system of generators of the A-algebra B. For all i, there exists by hypothesis a monic polynomial $P_i \in C[X]$ such that $P_i(x_i) = 0$. Let C' be the sub-A-algebra of C generated by the coefficients of the P_i. Clearly the x_i are integral over C' and $B = C'[x_1, \dots, x_n]$, hence B is a finitely generated C'-module. On the other hand C' is a Noetherian ring, hence C is a finitely generated C'-module, which proves that C is a finitely generated A-algebra. □

Let S be a multiplicative subset of a ring A and G a group acting on A and for which S is stable. Then, for all $\sigma \in G$, there exists a unique endomorphism $z \mapsto \sigma(z)$ of the ring $S^{-1}A$ such that $\sigma(a/1) = \sigma(a)/1$ for all $a \in A$, which is given by $\sigma(a/s) = \sigma(a)/\sigma(s)$. If τ is another element of G, then clearly $\sigma(\tau(z)) = \sigma\tau(z)$ for all $z \in S^{-1}A$, whence the group G operates on the ring $S^{-1}A$.

Proposition 13.2.3. *Let A be a R-algebra, G a locally finite R-action on A, S a multiplicative subset of A stable under G and S^G the set $S \cap A^G$. Then the canonical map $i_A^{S^G,S} : (S^G)^{-1}A \to S^{-1}A$ is an isomorphism which maps $(S^G)^{-1}A^G$ to $(S^{-1}A)^G$.*

Proof. For all $s \in S$, let $s_1 = s, s_2, \dots, s_n$ be the distinct elements of the orbit of s under G. As $\prod_{i=1}^n s_i \in S^G$, the first assertion follows from Proposition 10.2.23. Identifying canonically $(S^G)^{-1}A$ with $S^{-1}A$, clearly every element of $(S^G)^{-1}A^G$ is invariant under G. Conversely, let a/s be an element of $(S^G)^{-1}A$ which is invariant under G. If $a_1, \dots, a_m$ are the distinct elements of the orbit of a under G, then $a_j/s = a/s$ for $1 \le j \le m$ and therefore there exists $t \in S^G$ such that $t(a_j - a) = 0$ for $1 \le j \le m$. In other words, ta is invariant under G and, as $a/s = (ta)/(ts)$, certainly $a/s \in (S^G)^{-1}A^G$. □

Corollary 13.2.4. *Let A be an integral domain, K its field of fractions and G a locally finite R-action on A. Then G acts on K and K^G is the field of fractions of A^G.*

13.2.2 Decomposition group and inertial group

Let B be a ring and G a group acting on B. Given a prime ideal $\mathfrak{P}$ of B the subgroup of elements $\sigma \in G$ such that $\sigma(\mathfrak{P}) = \mathfrak{P}$ is called the **decomposition group** of $\mathfrak{P}$ (with respect to G) and is denoted by $G^Z(\mathfrak{P})$. The ring of elements of B invariant under $G^Z(\mathfrak{P})$ is called the **decomposition ring** of $\mathfrak{P}$ (with respect to G) and is denoted by $A^Z(\mathfrak{P})$.

We often write G^Z and A^Z instead of $G^Z(\mathfrak{P})$ and $A^Z(\mathfrak{P})$ respectively, when there is no ambiguity. For all $\sigma \in G^Z(\mathfrak{P})$, we also denote by $z \mapsto \sigma(z)$ the endomorphism of the ring $B/\mathfrak{P}$ derived from the endomorphism $x \mapsto \sigma(x)$ of B by taking quotients; clearly the group $G^Z(\mathfrak{P})$ operates in this way on the ring $B/\mathfrak{P}$. The subgroup of $G^Z(\mathfrak{P})$ consisting of those σ such that the endomorphism $z \mapsto \sigma(z)$ of $B/\mathfrak{P}$ is the identity is called the **inertia group** of $\mathfrak{P}$ (with respect to G) and denoted by $G^T(\mathfrak{P})$. Similarly, we write $A^T(\mathfrak{P})$ for the subring of B invariant under $G^T(\mathfrak{P})$.

If A is the subring of B consisting of the invariants of G (i.e., $A = B^G$), clearly we have

$$A \subseteq A^Z(\mathfrak{P}) \subseteq A^T(\mathfrak{P}) \subseteq B.$$

It follows from definition that, for $\rho \in G$,

$$G^Z(\rho(\mathfrak{P})) = \rho G^Z(\mathfrak{P})\rho^{-1}, \quad G^T(\rho(\mathfrak{P})) = \rho G^T(\mathfrak{P})\rho^{-1}. \tag{2.2.1}$$

We may also write $\mathfrak{P}^Z := \mathfrak{P} \cap A^Z$ and $\mathfrak{P}^T = \mathfrak{P} \cap A^T$.

If, for all $\sigma \in G^Z(\mathfrak{P})$, $\bar{\sigma}$ denotes the automorphism $z \mapsto \overline{\sigma(z)}$ of $B/\mathfrak{P}$, then the map $\sigma \mapsto \bar{\sigma}$ is a homomorphism (called canonical) of $G^Z(\mathfrak{P})$ to the group of automorphisms of $B/\mathfrak{P}$ leaving invariant the elements of $A^Z/(\mathfrak{P}^Z)$, and by definition $G^T(\mathfrak{P})$ is the kernel of this canonical homomorphism, so it is a normal subgroup of $G^Z(\mathfrak{P})$. If $\kappa(\mathfrak{P})$ is the field of fractions of $B/\mathfrak{P}$, every automorphism of $B/\mathfrak{P}$ can be extended uniquely to an automorphism of $\kappa(\mathfrak{P})$, so that $\sigma \mapsto \bar{\sigma}$ can be considered as a homomorphism from $G^Z(\mathfrak{P})$ to the group of automorphisms of $\kappa(\mathfrak{P})$. Note that, since $G^T(\mathfrak{P})$ is normal in $G^Z(\mathfrak{P})$, the ring $A^T(\mathfrak{P})$ is stable under G, in view of (2.2.1).

Proposition 13.2.5. *Let B be a ring, G a group acting on B, A the ring of invariants of G, $\mathfrak{P}$ a prime ideal of B and S a multiplicative subset of A not meeting $\mathfrak{P}$. Then*

$$G^Z(S^{-1}\mathfrak{P}) = G^Z(\mathfrak{P}), \quad G^T(S^{-1}\mathfrak{P}) = G^T(\mathfrak{P})$$

and, if the action of G is locally finite, then

$$S^{-1}A^Z(\mathfrak{P}) = A^Z(S^{-1}\mathfrak{P}), \quad S^{-1}A^T(\mathfrak{P}) = A^T(S^{-1}\mathfrak{P}).$$

Proof. As the elements of S are invariant under G, clearly, if $\sigma(\mathfrak{P}) = \mathfrak{P}$, also $\sigma(S^{-1}\mathfrak{P}) = S^{-1}\mathfrak{P}$. Conversely, suppose that $\sigma \in G$ is such that $\sigma(S^{-1}\mathfrak{P}) = S^{-1}\mathfrak{P}$, then, if $x \in \mathfrak{P}$, we have $\sigma(x/1) \in S^{-1}\mathfrak{P}$ and there therefore exists $s \in S$ such that $s\sigma(x) \in \mathfrak{P}$, whence $\sigma(x) \in \mathfrak{P}$ since $\mathfrak{P}$ is prime and $s \notin \mathfrak{P}$. This proves that $\sigma(\mathfrak{P}) \subseteq \mathfrak{P}$ and it can be similarly shown that $\sigma^{-1}(\mathfrak{P}) \subseteq \mathfrak{P}$, hence $\sigma(\mathfrak{P}) = \mathfrak{P}$ and $\sigma \in G^Z(\mathfrak{P})$. If $\sigma \in G^T(\mathfrak{P})$, then $\sigma(x) - x \in \mathfrak{P}$ for all $x \in B$, hence also, for all $s \in S$,

$$\sigma(x/s) - (x/s) = (\sigma(x) - x)/s \in S^{-1}\mathfrak{P}$$

and therefore $\sigma \in G^T(S^{-1}\mathfrak{P})$. Conversely, suppose that $\sigma \in G^T(S^{-1}\mathfrak{P})$. Then, for all $x \in B$, $\sigma(x/1) - (x/1) \in S^{-1}\mathfrak{P}$ and therefore there exists $s \in S$ such that $s(\sigma(x) - x) \in \mathfrak{P}$, whence as above $\sigma(x) - x \in \mathfrak{P}$, which proves that $\sigma \in G^T(\mathfrak{P})$. The last two assertions follow from Proposition 13.2.3. □

Proposition 13.2.6. *Let B be a ring, G a finite group acting on B and A the ring of invariants of G so that B is integral over A.*

(a) Given two prime ideals $\mathfrak{P}$, $\mathfrak{Q}$ of B lying over the same prime ideal $\mathfrak{p}$ of A, there exists $\sigma \in G$ such that $\sigma(\mathfrak{P}) = \mathfrak{Q}$. In other words, G operates transitively on the set of prime ideals of B lying over $\mathfrak{p}$.

(b) Let $\mathfrak{P}$ be a prime ideal of B and $\mathfrak{p} = \mathfrak{P} \cap A$. Then $\kappa(\mathfrak{P})$ is a normal extension of $\kappa(\mathfrak{p})$ and the canonical homomorphism $\sigma \mapsto \bar{\sigma}$ defines by taking the quotient an isomorphism of $G^Z(\mathfrak{P})/G^T(\mathfrak{P})$ onto $\mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$. In other words, we get the following exact sequence

$$1 \longrightarrow G^T(\mathfrak{P}) \longrightarrow G^Z(\mathfrak{P}) \longrightarrow \mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})) \longrightarrow 1$$

Proof. If $x \in \mathfrak{Q}$, then $\prod_{\sigma\in G} \sigma(x) \in \mathfrak{Q} \cap A = \mathfrak{p} \subseteq \mathfrak{P}$. Hence there exists $\sigma \in G$ such that $\sigma(x) \in \mathfrak{P}$, that is $x \in \sigma^{-1}(\mathfrak{P})$. We then conclude that $\mathfrak{Q} \subseteq \bigcup_{\sigma\in H} \sigma(\mathfrak{P})$, and hence ($G$ is finite) $\mathfrak{Q} \subseteq \sigma(\mathfrak{P})$ for some $\sigma \in G$. Since $\mathfrak{Q}$ and $\sigma(\mathfrak{P})$ both lie over $\mathfrak{p}$, we see $\mathfrak{Q} = \sigma(\mathfrak{P})$.

To see that $\kappa(\mathfrak{P})$ is a normal extension of $\kappa(\mathfrak{p})$, it suffices to prove that every element $\bar{x} \in B/\mathfrak{P}$ is a root of a polynomial P in $\kappa(\mathfrak{p})[X]$ all of whose roots are in $B/\mathfrak{P}$. Now, let $x \in B$ be a representative of the class $\bar{x}$. Then the polynomial $P(X) = \prod_{\sigma\in G}(X - \sigma(x))$ has all its coefficients in A. Let $\bar{P}(X)$ be the polynomial in $(A/\mathfrak{p})[X]$ which is the image of $P(X)$, then we see $\bar{P}(X) = \prod_{\sigma\in G}(X - \overline{\sigma(x)})$ and therefore solves the problem.

Clearly, for all $\sigma \in G^Z$, $\bar{\sigma}$ is a $\kappa(\mathfrak{p})$-automorphism of $\kappa(\mathfrak{P})$. It remains to verify that $\sigma \mapsto \bar{\sigma}$ maps G^Z onto the group of all $\kappa(\mathfrak{p})$-automorphisms of $\kappa(\mathfrak{P})$. Since $\kappa(\mathfrak{p})$ and $\kappa(\mathfrak{P})$ are not changed under localization and by Proposition 13.2.5 neither G^Z nor its operation on $\kappa(\mathfrak{P})$ is changed, we may therefore restrict our attention to the case where $\mathfrak{p}$ is maximal, in which case

we know that so is $\mathfrak{P}$ and every element of $\kappa(\mathfrak{P})$ is therefore of the form $\bar{x}$ for some x in B. It has been seen above that such an element is a root of a polynomial in $\kappa(\mathfrak{p})[X]$ of degree smaller than $|G|$. As every finite separable extension of $\kappa(\mathfrak{p})$ admits a primitive element, it is seen that every finite separable extension of $\kappa(\mathfrak{p})$ contained in $\kappa(\mathfrak{P})$ is of degree smaller than $|G|$, whence the separable closure $\kappa(\mathfrak{p})^{\mathrm{sep}}$ in $\kappa(\mathfrak{P})$ is of degree smaller than $|G|$. Let $y \in B$ be an element such that $\bar{y}$ is a primitive element of $\kappa(\mathfrak{p})^{\mathrm{sep}}$. The ideals $\sigma(\mathfrak{P})$ for $\sigma \in G - G^Z$ are maximal and distinct from $\mathfrak{P}$ by definition. By Chinese remainder therorem there then exists $x \in B$ such that $x \equiv y$ mod $\mathfrak{P}$ and $x \in \sigma(\mathfrak{P})$ for all $\sigma \in G - G^Z$. Now let θ be a $\kappa(\mathfrak{p})$-automorphism of $\kappa(\mathfrak{P})$ and let $P(X) = \prod_{\sigma \in G}(X - \overline{\sigma(x)})$. As $\bar{x}$ is a root of P and $P \in \kappa(\mathfrak{p})[X]$, $\theta(\bar{x})$ is also a root of P in $\kappa(\mathfrak{P})$ and hence there exists $\tau \in G$ such that

$$\theta(\bar{x}) = \tau(\bar{x}).$$

Since $\sigma(\bar{x}) = 0$ for all $\sigma \in G - G^Z$ and $\theta(\bar{x}) \neq 0$, we conclude that necessarily $\tau \in G^Z$. As θ and τ have the same value for the primitive element $\bar{x} = \bar{y}$ of $\kappa(\mathfrak{p})^{\mathrm{sep}}$, they coincide on $\kappa(\mathfrak{p})^{\mathrm{sep}}$ and, as $\kappa(\mathfrak{P})$ is an inseparable extension of $\kappa(\mathfrak{p})^{\mathrm{sep}}$, they coincide on $\kappa(\mathfrak{P})$. □

Corollary 13.2.7. *With the hypotheses and notation of Proposition 13.2.6, let f_1 and f_2 be two homomorphism of B to a field Ω with the same restriction to A. Then there exists a $\sigma \in G$ such that $f_2 = f_1 \circ \sigma$.*

Proof. Let $\mathfrak{P}_i$ be the kernel of f_i, which is a prime ideal of B. By hypothesis $\mathfrak{P}_1 \cap A = \mathfrak{P}_2 \cap A$ and this intersection is a prime ideal $\mathfrak{p}$ of A. There therefore exists $\tau \in G$ such that $\tau(\mathfrak{P}_2) = \mathfrak{P}_1$. Replacing f_1 by the homomorphism $f_1 \circ \tau$, we may then assume that $\mathfrak{P}_1 = \mathfrak{P}_2$ (an ideal which we shall denote by $\mathfrak{P}$). By taking the quotient and localization we then derive from f_1 and f_2 two injective homomorphisms $\tilde{f}_1$, $\tilde{f}_2$ from $\kappa(\mathfrak{P})$ to Ω. As $\kappa(\mathfrak{P})$ is a normal extension of $\kappa(\mathfrak{p})$, we see $\tilde{f}_2 \circ \tilde{f}_1^{-1}$ is a $\kappa(\mathfrak{p})$-automorphism of $\kappa(\mathfrak{P})$ (Theorem 9.1.43) and it follows from Proposition 13.2.6 that $\tilde{f}_2 \circ \tilde{f}_1^{-1} = \bar{\sigma}$ for some $\sigma \in G$. In particular, for all $x \in B$ the elements $f_2(x)$ and $f_1(\sigma(x))$ are equal. □

Proposition 13.2.8. *Let B be a ring, G a finite group acting on B and H a subgroup of G. Let A^G and A^H be the rings of invariants of G and H respectively, so that $A^G \subseteq A^H$. For a prime ideal $\mathfrak{P}$ of B, set $\mathfrak{p}^G = \mathfrak{P} \cap A^G$ and $\mathfrak{p}^H = \mathfrak{P} \cap A^H$.*

(a) For H to be contained in the decomposition group $G^Z(\mathfrak{P})$, it is necessary and sufficient that $\mathfrak{P}$ be the only prime ideal of A lying over $\mathfrak{p}^H$.

(b) If H contains $G^Z(\mathfrak{P})$, then

(α) The rings $A^G/\mathfrak{p}^G$ and $A^H/\mathfrak{p}^H$ have the same field of fractions;

(β) The maximal ideal of the local ring $(A^H)_{\mathfrak{p}^H}$ is generated by $\mathfrak{p}^G$.

(c) Suppose further that B is an integral domain and that $\bigcap_{n=1}^{\infty}(\mathfrak{p}^G)^n B_{\mathfrak{P}} = 0$, then conditions ($\alpha$) and ($\beta$) of (b) imply that $G^Z(\mathfrak{P})$ preserves the elements of A^H.

Proof. It follows from Proposition 13.2.6(a) that the prime ideals of B lying over $\mathfrak{p}^H$ are the ideals of the form $\sigma(\mathfrak{P})$ where $\sigma \in H$; whence immediately (a).

Now we prove (b). By localization, we may assume that $\mathfrak{p}^G$ is maximal. To establish (α) it will be sufficient to prove that

$$A^H = A^G + \mathfrak{p}^H. \tag{2.2.2}$$

for this will show that the fields $(A^G/\mathfrak{p}^G)$ and $(A^H)/(\mathfrak{p}^H)$ are canonically isomorphic. By Proposition 13.2.6 there is only a finite number of primes of B lying over $\mathfrak{p}^G$, therefore there is only a finite number of prime ideals of A^H lying over $\mathfrak{p}^G$, let $\mathfrak{n}_1, \dots, \mathfrak{n}_r$ denote those of these ideals that are different from $\mathfrak{p}^H$. Let x be an element of A^H, as the ideals $\mathfrak{p}^H$ and $\mathfrak{n}_i$ are maximal, there exists $y \in A^H$ such that $y \equiv x \bmod \mathfrak{p}^H$ and $y \in \mathfrak{n}_i$ for $1 \le j \le r$. Let $y_1 = y, y_2, \dots, y_s$ be distinct elements of the orbit of y under G. Clearly

$$z = y_1 + y_2 + \cdots + y_s \in A^G$$

and to establish (2.2.2) it will be sufficient to show that $y_i \in \mathfrak{P}$ for $i \ge 2$, for then we shall deduce that $z - y \in \mathfrak{P} \cap A^H = \mathfrak{p}^H$, whence $x \in A^G + \mathfrak{p}^H$ since $x \equiv y \bmod \mathfrak{p}^H$. Now let $i \ge 2$ and $\sigma \in G$ be such that $\sigma(y) = y_i$. Then $\sigma^{-1}(\mathfrak{P})$ does not lie over $\mathfrak{p}^H$, for otherwise there would exist $\tau \in G$ such that $\sigma^{-1}(\mathfrak{P}) = \tau(\mathfrak{P})$, whence $\sigma\tau \in G^Z \subseteq H$. But as $y \in A^H$ and $\sigma(y) \ne y$, this is a contradiction. We conclude that $\sigma^{-1}(\mathfrak{P})$ lies over one of the ideals $\mathfrak{n}_j$ and as $y \in \mathfrak{n}_j$ by construction, we see $y \in \sigma^{-1}(\mathfrak{P})$ or $y_i = \sigma(y) \in \mathfrak{P}$.

To prove (β) we show that $\mathfrak{p}^H$ is contained in the saturation $\mathfrak{q}$ of the ideal $(\mathfrak{p}^G)A^H$ with respect to $\mathfrak{p}^H$. As $\mathfrak{p}^H$ is contained in none of the $\mathfrak{n}_i$, by Proposition 10.1.4 it will suflice even to prove that

$$\mathfrak{p}^H \subseteq \mathfrak{q} \cup \mathfrak{n}_1 \cup \cdots \cup \mathfrak{n}_r. \tag{2.2.3}$$

For this, we consider an element $x \in \mathfrak{p}^H$ belonging to none of the $\mathfrak{n}_i$. Let $x_1 = x, x_2, \dots, x_m$ be the distinct elements of the orbit of x under G. Write $u = x_1 x_2 \cdots x_m$ and $v = x_2 \cdots x_m$, then $u \in A^G$. On the other hand, if $\tau \in H$ then $\tau(x) = x$ and hence necessarily $\tau(x_i) \ne x$ for $i \ge 2$, which shows that $\tau(v) = v$ and hence $v \in A^H$. It can be shown as in the proof of (α) that, if $\sigma \in G$ is such that $\sigma(x) = x_i$ where $i \ge 2$, then $\sigma^{-1}(\mathfrak{P})$ lies over one of the $\mathfrak{n}_j$ and, as $x \notin \mathfrak{n}_j$, we have $x \notin \sigma^{-1}(\mathfrak{P})$ whence $x_i \notin \mathfrak{P}$. We conclude that $v \notin \mathfrak{P}$ and therefore $v \notin \mathfrak{p}^H$. On the other hand clearly $u \in \mathfrak{P} \cap A^G = \mathfrak{p}^G$ and the relation $u = xv$ then shows that x is in the saturation of $\mathfrak{p}^G(A^H)$ with respect to $\mathfrak{p}^H$ and hence establishes (2.2.3).

Suppose that B is an integral domain, that $\bigcap_{n=0}^{\infty}(\mathfrak{p}^G)^n B\mathfrak{P} = 0$ and that conditions (α) and (β) of (b) hold. With the same notation as in (b), by localization we may assume also that the ideal $\mathfrak{p}^G$ is maximal. The hypotheses (α) and (β) then imply that for all $n > 0$ we have (by induction)

$$(A^H)_{\mathfrak{p}^H} = A^G + (\mathfrak{p}^G)^n (A^H)_{\mathfrak{p}^H}.$$

Then let σ be an element of G^Z and x be an element of A^H. For all $n > 0$, there exists $a_n \in A^G$ such that $x - a_n \in (\mathfrak{p}^G)^n (A^H)_{\mathfrak{p}^H} \subseteq (\mathfrak{p}^G)^n B_{\mathfrak{P}}$. As $\sigma(a_n) = a_n$ and $\sigma(\mathfrak{P}) = \mathfrak{P}$, we deduce that $\sigma(x) - x \in (\mathfrak{p}^G)^n B_{\mathfrak{P}}$. Since this relation holds for all n, we conclude from the hypothesis that $\sigma(x) = x$. □

Corollary 13.2.9. *Under the hypotheses of Proposition 13.2.8 the rings $(A^G)/(\mathfrak{p}^G)$ and $A^Z/(\mathfrak{P}^Z)$ have the same field of fractions and the maximal ideal of the local ring $(A^Z)_{\mathfrak{P}^Z}$ is generated by $\mathfrak{p}^G$.*

Proof. This follows from Proposition 13.2.8 by taking $H = G^Z$. □

Corollary 13.2.10. *Let B be an integral domain, G a finite group acting on B, A the ring of invariants of G and $\mathfrak{P}$ a prime ideal of B. Let K, K^Z and L be the fields of fractions of A, A^Z and L respectively.*

Then L is a Galois extension of K with Galois group G and the subfields E of L containing K and such that $\mathfrak{P}$ is the only prime ideal of B lying over the ideal $\mathfrak{P} \cap E$ of $B \cap E$ are just those which contain K^Z.

Proof. By Proposition 13.2.3 applied to $S = A - \{0\}$, we see K is the field of invariants of G in L and similarly K^Z is the field of invariants of G^Z. By **??** we see L is a Galois extension of K with Galois group G. By Galois correspondence, we see the condition "E contains K^Z" is equivalent to "H is contained in G^Z", where H is the fixed group of E. As E is then the field of invariants of H in L, $B \cap E$ is the ring of invariants of H in B. The second assertion then follows from Proposition 13.2.8. □

Proposition 13.2.11. *Let B be an integral domain, G a finite group acting on B, A the ring of invariants of G, $\mathfrak{p}$ a prime ideal of A and $\mathfrak{P}$ a prime of B lying over A. Then*

(a) The residue field of $\mathfrak{P}^T$ is the separable closure of $\kappa(\mathfrak{p})$ in $\kappa(\mathfrak{P})$.

(b) The extension K^T/K is Galois and $\mathrm{Gal}(K^T/K)$ is isomorphic to $\mathrm{Gal}(\kappa(\mathfrak{P}^T)/\kappa(\mathfrak{p}))$.

(c) There exists a correspondence between the set of all intermediate extensions of $K^T/E/K$ and the set of all separable extensions $\kappa(\mathfrak{P}^T)/\kappa/\kappa(\mathfrak{p})$. The extension $\kappa/\kappa(\mathfrak{p})$ is a Galois extension if and only if E/K is Galois. Moreover, κ is the residue field of $\mathfrak{P} \cap E$.

Proof. By localization this may be reduced to the case where $\mathfrak{p}$ is a maximal ideal of A, which implies that $\mathfrak{P}$, $\mathfrak{P}^Z$ and $\mathfrak{P}^T$ are maximal in B, A^Z and A^T respectively. Since G^T is a normal subgroup of G, we know K^T/K is Galois with Galois group G/G^T. Since K^T/K is normal, by Proposition 13.2.6 we see $\kappa(\mathfrak{P}^T)$ is a normal extension of $\kappa(\mathfrak{p})$, and Proposition 13.2.6 shows that $\mathrm{Gal}(K^T/K)$ is isomorphic to $\mathrm{Gal}(\kappa(\mathfrak{P}^T)/\kappa(\mathfrak{p}))$, hence the correspondence between the sets of intermediate fields $K \subseteq E \subseteq K^T$ and $\kappa(\mathfrak{p}) \subseteq \kappa \subseteq \kappa(\mathfrak{P}^T)$ follows from Galois correspondence as well as the statement concerning normality. To see the last statement of (c), observe that K^T is also the inertial field of $\mathfrak{P} \cap E$ for any intermediate extension $K \subseteq E \subseteq K^T$, therefore if $\kappa(E)$ is the residue field of $\mathfrak{P} \cap E$, then $\mathrm{Gal}(K^T/E) \cong \mathrm{Gal}(\kappa(\mathfrak{P}^T)/\kappa(E))$, by what we have just seen.

For all $x \in B$, the polynomial $P(X) = \prod_{\sigma \in G^T}(X - \sigma(x))$ has its coefficients in the inertia ring A^T and, by definition of G^T, all its roots in B are congruent mod $\mathfrak{P}$. The polynomial $\pi(P)(X)$ over $A^T/\mathfrak{P}^T$ whose coefficients are the canonical images of those of P under the homomorphism $\pi : B \to B/\mathfrak{P}$ therefore has all its roots in $B/\mathfrak{P}$ equal $\pi(x)$, which shows that $\kappa(\mathfrak{P})$ is purely inseparable over $\kappa(\mathfrak{P}^T)$; whence $\kappa(\mathfrak{p})^{\mathrm{sep}} \subseteq \kappa(\mathfrak{P}^T)$.

We know that $\kappa(\mathfrak{p})^{\mathrm{sep}}/\kappa(\mathfrak{p})$ is a Galois extension and it follows from Proposition 13.2.6 that its Galois group is isomorphic to $G' = G^Z/G^T$. As $\kappa(\mathfrak{P}^T)$ is a purely inseparable extension of $\kappa(\mathfrak{p})^{\mathrm{sep}}$, $\kappa(\mathfrak{P}^T)$ is a normal extension of $\kappa(\mathfrak{p})$ and the separable degree of $\kappa(\mathfrak{P}^T)$ over $\kappa(\mathfrak{p})$ is

$$[\kappa(\mathfrak{P}^T) : \kappa(\mathfrak{p})]_s = [\kappa(\mathfrak{p})^{\mathrm{sep}} : \kappa(\mathfrak{p})] = [G^Z : G^T] =: q.$$

It remains to see that $\kappa(\mathfrak{P}^T)$ is a separable extension of $\kappa(\mathfrak{p})$. We have seen above that G' is identified with an automorphism group of A^T and that A^Z is the ring of invariants of G'. If $x \in A^T$, the polynomial $Q(X) = \prod_{\sigma' \in G'}(X - \sigma'(x))$ therefore has its coefficients in A^Z. The polynomial $\pi(Q)$ over $A^Z/\mathfrak{p}^Z$ whose coefficients are the images of those of Q under the homomorphism π is of degree q and has a root $\pi(x) \in A^T/\mathfrak{p}^T$. As $A^Z/\mathfrak{p}^Z = \kappa(\mathfrak{p})$ by Proposition 13.2.8(b), we see that every element of $\kappa(\mathfrak{P}^T)$ is of degree $\leq q$ over $\kappa(\mathfrak{p})$.

This being so, let κ be the field of invariants of the Galois group $\mathrm{Gal}(\kappa(\mathfrak{P}^T)/\kappa(\mathfrak{p}))$; then $[\kappa(\mathfrak{P}^T) : \kappa] = q$ by Proposition 9.1.89. Let ξ be a primitive element of $\kappa(\mathfrak{P}^T)$ over κ; as it is of degree q over κ and of degree $\leq q$ over $\kappa(\mathfrak{p})$, it is of degree q over $\kappa(\mathfrak{p})$ and its minimal polynomial over κ has coefficients in $\kappa(\mathfrak{p})$; this shows that ξ is separable over $\kappa(\mathfrak{p})$. On the other hand, for all $\zeta \in \kappa$, there exists a power p^f of the characteristic p such that $\zeta^{p^f} \in \kappa(\mathfrak{p})$. We conclude that $\kappa(\mathfrak{p})(\xi - \zeta)$, which contains

$$(\xi - \zeta)^{p^f} = \xi^{p^f} - \zeta^{p^f}$$

contains ξ^{p^f} and consequently $\kappa(\mathfrak{p})(\xi^{p^f})$. But as ξ is separable over $\kappa(\mathfrak{p})$, $\kappa(\mathfrak{p})(\xi) = \kappa(\mathfrak{p})(\xi^{p^f})$ by Proposition 9.1.64, whence $\kappa(\mathfrak{p})(\xi) \subseteq \kappa(\mathfrak{p})(\xi - \zeta)$. As ξ is of degree q over $\kappa(\mathfrak{p})$ and $\xi - \zeta$ of degree $\leq q$, it follows that $\kappa(\mathfrak{p})(\xi) = \kappa(\mathfrak{p})(\xi - \zeta)$, whence $\zeta \in \kappa(\mathfrak{p})(\xi)$. This shows that ζ is separable over $\kappa(\mathfrak{p})$, hence $\kappa = \kappa(\mathfrak{p})$ and $\kappa(\mathfrak{P}^T)$ is separable over $\kappa(\mathfrak{p})$. □

Corollary 13.2.12. *If the order of the inertia group $G^T(\mathfrak{P})$ is relatively prime to the characteristic p of $\kappa(\mathfrak{p})$, then $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ is a Galois extension.*

Proof. With the notation of the proof of Proposition 13.2.11, the polynomial $\pi(P)$ has coefficients in $\kappa(\mathfrak{P}^T) = \kappa(\mathfrak{p})^{\mathrm{sep}}$; and all its roots equal to the image $\bar{x}$ of x in $B/\mathfrak{P}$. We immediately deduce that $\pi(P)$ is a power of a minimal polynomial of $\bar{x}$ over $\kappa(\mathfrak{p})^{\mathrm{sep}}$. But the latter has degree equal to a power of p and hence, as the degree of $\pi(P)$ is equal to the order of G^T, the hypothesis implies that $\pi(P)$ has degree zero, in other words $\bar{x} \in \kappa(\mathfrak{p})^{\mathrm{sep}}$. Thus $\kappa(\mathfrak{P}^T) = \kappa(\mathfrak{p})^{\mathrm{sep}}$ and $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ is a Galois extension. □

13.2.3 Applications for integrally closed domains

Lemma 13.2.13. *Let A be an integrally closed domain, K its field of fractions, p the characteristic of K, L a radicial extension of K and B a subring of L containing A and integral over A. For every prime ideal $\mathfrak{p}$ of A, there exists a unique prime ideal $\mathfrak{P}$ of B lying over $\mathfrak{p}$ and $\mathfrak{P}$ is the set of $x \in B$ such that there exists an integer $n > 0$ for which $x^{p^n} \in \mathfrak{p}$.*

Proof. The existence of $\mathfrak{P}$ follows from Theorem 13.1.67. If $x \in \mathfrak{P}$, there exists $n > 0$ such that $x^{p^n} \in K$, whence $x^{p^n} \in A$ since A is integrally closed, hence $x^{p^n} \in A \cap \mathfrak{P} = \mathfrak{p}$. Conversely, if $x \in B$ is such that $x^{p^n} \in \mathfrak{p} \subseteq \mathfrak{P}$ then $x \in \mathfrak{p}$ since $\mathfrak{P}$ is prime. □

Proposition 13.2.14. *Let A be an integrally closed domain, K its field of fractions, L a normal extension of K and B the integral closure of A in L. Then*

(a) For every prime ideal $\mathfrak{p}$ of A, the group G of K-automorphisms of L acts transitively on the set of prime ideals of B lying over $\mathfrak{p}$.

(b) For every prime ideal $\mathfrak{P}$ of B and $\mathfrak{p} = \mathfrak{P} \cap A$, the residue field $\kappa(\mathfrak{P})$ is a nromal extension of $\kappa(\mathfrak{p})$ and the canonical homomorphism $\sigma \mapsto \bar{\sigma}$ defines by taking the quotient an isomorphism of $G^Z(\mathfrak{P})/G^T(\mathfrak{P})$ onto $\mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$.

Proof. Suppose first that L is a finite Galois extension of K. Then $A = B \cap K$ since A is integrally closed and A is therefore the ring of invariants of G in B. As G is finite, the proposition follows in this case from Proposition 13.2.6.

Suppose secondly that L is any Galois extension of K. Then L is the union of a right directed family $(K_\alpha)_{\alpha\in I}$ of finite Galois extensions of K. To show (a), consider two prime ideals $\mathfrak{P}$, $\mathfrak{Q}$ of B lying over $\mathfrak{p}$. For all $\alpha \in I$, $\mathfrak{P} \cap K_\alpha$ and $\mathfrak{Q} \cap K_\alpha$ are two prime ideals of $B \cap K_\alpha$ lying over $\mathfrak{p}$. Since $B \cap K_\alpha$ is the integral closure of A in K_α and the restrictions to K_α of the elements of G form the group of K-automorphisms of K_α, it follows from the finite case that there exists $\sigma \in G$ such that $\sigma(\mathfrak{P} \cap K_\alpha) = \mathfrak{Q} \cap K_\alpha$. Let $\mathcal{E}_\alpha$ be the set of $\sigma \in G$ which have the above property. Let $\sigma \in G - \mathcal{E}_\alpha$, then for all $\tau \in G$ leaving invariant the elements of K_α, we have

$$(\sigma\tau)(\mathfrak{P} \cap K_\alpha) = \sigma(\mathfrak{P} \cap K_\alpha) \neq \mathfrak{Q} \cap K_\alpha$$

and hence $\sigma\tau \in G - \mathcal{E}_\alpha$. It follows that $\mathcal{E}_\alpha$ is closed in the topological Galois group G and clearly the family $\mathcal{E}_\alpha$ is directed. As G is compact and the $\mathcal{E}_\alpha$ are non-empty, the intersection $\mathcal{E}$ of the family $(\mathcal{E}_\alpha)$ is non-empty and $\sigma(\mathfrak{P}) = \mathfrak{Q}$ for all $\sigma \in \mathcal{E}$, whence (a).

To show (b), note that $\kappa(\mathfrak{P})$ is the union of the right directed family $(\kappa_\alpha)_{\alpha\in I}$ where κ_α is the residue field of $\mathfrak{P} \cap K_\alpha$. As each κ_α is a normal extension of $\kappa(\mathfrak{p})$ by Proposition 13.2.6, so is $\kappa(\mathfrak{P})$. On the other hand, let θ be a $\kappa(\mathfrak{p})$-automorphism of $\kappa(\mathfrak{P})$. By virtue of Proposition 13.2.6 applied to $B \cap K_\alpha$, there exists for all α a non-empty set $\mathcal{F}_\alpha$ of elements $\sigma \in G$ such that $\sigma(\mathfrak{P} \cap K_\alpha) = \mathfrak{P} \cap K_\alpha$ and $\theta(\bar{x}) = \overline{\sigma(x)}$ for all $x \in B \cap K_\alpha$. As above it is seen that $\mathcal{F}_\alpha$ is closed in G and, as $(\mathcal{F}_\alpha)$ is a left directed set, its intersection $\mathcal{F}$ is non-empty. Clearly for $\sigma \in G$ we have $\sigma \in G^Z$ and $\bar{\sigma} = \theta$, which completes the proof of (b) in this case.

Finally we deal with the general case. The field of invariants K_1 of G is a purely inseparable extension of K. There therefore exists a single prime ideal $\mathfrak{p}_1$ of $A_1 = B \cap K_1$ lying over $\mathfrak{p}$ (Lemma 13.2.13). If $\mathfrak{P}$ and $\mathfrak{Q}$ are two prime ideals of B lying over $\mathfrak{p}$, then they lie over $\mathfrak{p}_1$. As L is a Galois extension of K_1 and $B \cap K_1$ is integrally closed by Proposition 13.1.20, it follows from the Galois case that there exists a $\sigma \in G$ such that $\sigma(\mathfrak{P}) = \mathfrak{Q}$, whence (a). On the other hand, clearly the residue field of $\mathfrak{p}_1$ is a purely inseparable extension of $\kappa(\mathfrak{p})$. As $\kappa(\mathfrak{P})$ is a normal extension of κ_1 by the Galois case, we then see $\kappa(\mathfrak{P})$ is a normal extension of $\kappa(\mathfrak{p})$ (since every $\kappa(\mathfrak{p})$-isomorphism of $\kappa(\mathfrak{P})$ is a κ_1-isomorphism). This last remark shows also, taking account of the Galois case, that every $\kappa(\mathfrak{p})$-automorphism of $\kappa(\mathfrak{P})$ is of the form $\bar{\sigma}$ where $\sigma \in G^Z(\mathfrak{P})$, which completes the proof of (b). □

Corollary 13.2.15. *Let A be an integrally closed domain, K its field of fractions, L a normal extension of K and B the integral closure of A in L. Let θ_1 and θ_2 be two homomorphisms of B to a field Ω with the same restriction on A. Then there exists a K-automorphism σ of L such that $\theta_1 = \theta_2 \circ \sigma$.*

Proof. This can be proved as Corollary 13.2.7. □

Proposition 13.2.16. *Let A be an integrally closed domain, K its field of fractions, L a finite algebraic extension of K and B a subring of L containing A and integral over A.*

(a) For every prime ideal $\mathfrak{p}$ of A the set of prime ideals of B lying over $\mathfrak{p}$ is at most $[L : K]_s$.

(b) If $\mathfrak{P}$ is a prime ideal of B lying over $\mathfrak{p}$, every element of $\kappa(\mathfrak{P})$ is of degree smaller than $[L : K]$ over $\kappa(\mathfrak{p})$.

Proof. We may first restrict our attention to the case where L is a separable extension of K, for in general L is a purely inseparable extension of the separable closure K_0 of K contained in L,

and $[L : K]_s = [K_0 : K]$ by definition and, if $A_0 = B \cap K_0$, the prime ideals of A_0 and B are in one-to-one correspondence (Lemma 13.2.13).

Suppose therefore that L is separable over K and let N be the Galois extension of K generated by L in an algebraic closure of K, G its Galois group, $\bar{A}$ the integral closure of A in N and $\mathcal{P}$ a prime ideal of $\bar{A}$ lying over $\mathfrak{p}$. Let H be the Galois group of N over L and G^Z the decomposition group of $\mathcal{P}$. The prime ideals of $\bar{A}$ lying over $\mathfrak{p}$ are the $\sigma(\mathcal{P})$ where $\sigma \in G$ (Proposition 13.2.6) and the relation $\sigma(\mathcal{P}) = \sigma'(\mathcal{P})$ means that $\sigma' = \sigma\tau$ where $\tau \in G^Z$. On the other hand, in order that $\sigma(\mathcal{P}) \cap L = \sigma'(\mathcal{P}) \cap L$, it is necessary and sufficient that $\sigma(\mathcal{P}) = \theta\sigma(\mathcal{P})$, where $\theta \in H$ (Proposition 13.2.6), whence finally $\sigma' = \theta\sigma\tau$ where $\theta \in H$ and $\tau \in G^Z$. The number of prime ideals of B lying over $\mathfrak{p}$ is therefore equal to the cardinality of the double coset $H\backslash G/G^Z$, and this number is smaller than $[G : H] = [L : K]$ be Galois theory.

The coefficients of the minimal polynomial (over K) of any element $x \in B$ belong to A (Corollary 13.1.28). Applying the canonical homomorphism $B \to B/\mathfrak{P}$ to the coefficients of this polynomial, an equation of integral dependence with coefficients in $A/\mathfrak{p}$ and of degree $\leq [L : K]$ is obtained for the class mod $\mathfrak{P}$ of x, whence the conclusion. □

Proposition 13.2.17. *Let A be an integrally closed domain, K its field of fractions, L a Galois extension of K, B the integral closure of A in L, $\mathfrak{P}$ a prime ideal of B, $\mathfrak{p} = A \cap \mathfrak{P}$. For a subfield E of L containing K, set $A(E) = B \cap E$ and $\mathfrak{p}(E) = \mathfrak{P} \cap E$.*

(a) If E is contained in K^Z, then $\mathfrak{p}$ and $\mathfrak{p}(E)$ have the same residue field and the maximal ideal of $(A(E))_{\mathfrak{p}(E)}$ is generated by $\mathfrak{p}$.

(b) Conversely, if these two conditions in (a) hold and $\bigcap_{n=0}^{\infty} \mathfrak{p}^n B_{\mathfrak{P}} = 0$, then E is contained in K^Z.

Proof. Let G be the Galois group of L over K and H the Galois group of L over E. Then to say that $E \subseteq K^Z$ means that $G^Z \subseteq H$ and the assertions are therefore special cases of Proposition 13.2.8 when $[L : K]$ is finite. In the general case the argument is as in the proof of Proposition 13.2.14. □

Proposition 13.2.18. *Let A be an integrally closed domain, K its field of fractions, L a Galois extension of K, B the integral closure of A in L, $\mathfrak{P}$ a prime ideal of B, $\mathfrak{p} = A \cap \mathfrak{P}$.*

(a) The residue field $\kappa(\mathfrak{P}^T)$ is the separable closure of $\kappa(\mathfrak{p})$ in $\kappa(\mathfrak{P})$.

(b) The extension K^T/K is Galois and $\mathrm{Gal}(K^T/K)$ is isomorphic to $\mathrm{Gal}(\kappa(\mathfrak{P}^T)/\kappa(\mathfrak{p}))$.

(c) There exists an inclusion-preserving bijective correspondence between the set of all intermediate extensions $K \subseteq E \subseteq K^T$ and the set of all separable extensions $\kappa(\mathfrak{p}) \subseteq \kappa \subseteq \kappa(\mathfrak{P}^T)$. The extension $\kappa/\kappa(\mathfrak{p})$ is a Galois extension if and only if E/K is Galois. Moreover, in this case κ is the residue field of $\mathfrak{P} \cap E$.

Proof. The ring A is the ring of invariants in B of the Galois group of L over K. If L is of finite degree over K, the corollary then follows from Proposition 13.2.8 and Proposition 13.2.11. Consider now the general case, L therefore being the union of a right directed set (K_α) of finite Galois extensions of K.

Suppose now that $x \in A^T$. There exists α such that $x \in A^T(\mathfrak{P} \cap K_\alpha)$ and Proposition 13.2.11 shows that the class $\bar{x}$ of x mod $\mathfrak{P}^T \cap K_\alpha$ is algebraic and separable over $\kappa(\mathfrak{p})$. A fortiori the class mod $\mathfrak{P}^T$ of x is separable over $\kappa(\mathfrak{p})$. To complete the proof of the corollary, it is sufficient to

show that $\kappa(\mathfrak{P})$ is a purely inseparable extension of $\kappa(\mathfrak{P}^T)$. Now, $\kappa(\mathfrak{P})$ is the union of the right directed family of residue fields κ_α of $\mathfrak{P} \cap K_\alpha$. It follows therefore from Proposition 13.2.11 that, if an element of $\kappa(\mathfrak{P})$ belongs to κ_α, it is purely inseparable over the residue field of $\mathfrak{P}^T \cap K_\alpha$, and a fortiori over $\kappa(\mathfrak{P}^T)$. □

Let A be an integrally closed domain, K its field of fractions, L a normal extension of K and B the integral closure of A in L. The field of invariants $K^Z(\mathfrak{P})$ (resp. $K^T(\mathfrak{P})$) of the group $G^Z(\mathfrak{P})$ (resp. $G^T(\mathfrak{P})$) in the field L is called the **decomposition field** (resp. inertia field) of $\mathfrak{P}$ with respect to K. We also write K^z (resp. K^T) in place of $K^Z(\mathfrak{P})$ (resp. $K^T(\mathfrak{P})$). It follows from Proposition 13.2.3 that K^Z (resp. K^T) is the field of fractions of the ring A^Z (resp. A^T), and by Proposition 13.1.20 A^Z (resp. A^T) is the integral closure of A in K^Z (resp. K^T).

Proposition 13.2.19. *Let A be an integrally closed domain, K its field of fractions, L a Galois extension of K, B the integral closure of A in L, $\mathfrak{P}$ a prime ideal of B. For a subfield E of L containing K, set $A(E) = B \cap E$ and $\mathfrak{p}(E) = \mathfrak{P} \cap E$. Then the decomposition field (resp. inertia field) of $\mathfrak{P}$ with respect to E is EK^Z (resp. EK^T). If further E is a Galois extension of K, the decomposition field of $\mathfrak{p}(E)$ with respect to K is $E \cap K^Z$.*

Proof. If H is the Galois group of L over E, clearly the decomposition group (resp. inertia group) of $\mathfrak{P}$ with respect to E is $H \cap G^Z$ (resp. $H \cap G^T$) and the first assertion follows from Galois theory if L is a finite Galois extension of K. In the general case it follows from the fact that A^Z (resp. A^T) is the union of the $A^Z(\mathfrak{P} \cap K_\alpha)$ (resp. $A^T(\mathfrak{P} \cap K_\alpha)$): every element $x \in L$ belongs to some K_α and if it is invariant under $G^Z(\mathfrak{P}) \cap H$ (resp. $G^T(\mathfrak{P}) \cap H$) it is also invariant under $G^Z(\mathfrak{P} \cap K_\beta) \cap H$ (resp. $G^T(\mathfrak{P} \cap K_\beta) \cap H$) for some suitable β; hence it belongs by the beginning of the argument to $EK^Z(\mathfrak{P} \cap K_\alpha) \subseteq EK^Z$ (resp. $EK^T(\mathfrak{P} \cap K_\alpha) \subseteq EK^T$).

Suppose now that E is a Galois extension of K. The restriction to E of every $\sigma \in G^Z$ then preserves $\mathfrak{p}(E)$ and hence belongs to the decomposition group of $\mathfrak{p}(E)$ with respect to K. Conversely, let τ be an automorphism of E belonging to this group and let σ be an extension of τ to a K-automorphism of L. We write $\mathfrak{Q} = \sigma(\mathfrak{P})$. As $\mathfrak{P}$ and $\mathfrak{Q}$ both lie over $\mathfrak{p}(E)$, there exists an automorphism $\rho \in H$ such that $\mathfrak{Q} = \rho(\mathfrak{P})$, whence $\rho^{-1}\sigma \in G^Z$ and τ is the restriction of $\rho^{-1}\sigma$ to E. In other words, the decomposition group of $\mathfrak{p}(E)$ with respect to K is identical with the group of restrictions to E of the automorphisms $\sigma \in G^Z$ which proves the second assertion. □

13.3 Finite generated algebras over a field

In this part, k will be a field. Recall that, if A is a ring, by a finite generated A-algebra we mean an A-algebra B that is isomorphic to a quotient of some polynomial algebra $A[X_1, \dots, X_n]$.

Theorem 13.3.1 (Normalization Lemma). *Let A be a finitely generated k-algebra and let $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subset \cdots \subset \mathfrak{a}_p$ be an increasing finite sequence of peroper ideals of A. Then there exists a sequence $(x_i)_{1 \le i \le n}$ of elements of A which are algebraically independent over k and such that:*

(a) A is integral over the ring $B = k[x_1, \dots, x_n]$.

(b) There exists an increasing sequence $(h_j)_{1 \le j \le n}$ of integers such that for all j the ideal $\mathfrak{a}_j \cap B$ of B is generated $x_1, \dots, x_{h_j}$.

Proof. It is sufficient to prove the theorem when A is a polynomial algebra $k[Y_1, \dots, Y_m]$. In fact, assume the theorem for this case. In the general case, A is isomorphic to a quotient of such an algebra $\tilde{A}$ by an ideal $\tilde{\mathfrak{a}}_0$. Let $\tilde{\mathfrak{a}}_j$ denote the inverse image of $\mathfrak{a}_j$ in $\tilde{A}$ and let $(\tilde{x}_i)_{1\le i\le r}$ be elements of $\tilde{A}$ satisfying the conditions of the statement for the ring $\tilde{A}$ and the increasing sequence of ideals of $\tilde{\mathfrak{a}}_0 \subset \cdots \subset \tilde{\mathfrak{a}}_p$. Then the images x_i of the $\tilde{x}_i$ in A for $i > h_0$ satisfy the desired conditions. In fact, condition (b) is obvious and condition (a) follows from Proposition 13.1.6. Finally, if the x_i for $i > h_0$ were not algebraically independent over k, there would be a non-zero polynomial $Q \in k[X_{h_0+1}, \dots, X_r]$ such that $Q(x_{h_0+1}, \dots, x_r) \in \tilde{\mathfrak{a}}_0 \cap \tilde{B}$, where $\tilde{B} = k[\tilde{x}_1, \dots, \tilde{x}_r]$. But by hypothesis, the ideal $\mathfrak{a}_0 \cap \tilde{B}$ is generated by $x_1, \dots, x_{h_0}$, a contradiction which proves our assertion.

We shall therefore suppose in the rest of the proof that $A = k[Y_1, \dots, Y_m]$ and we shall argue by induction on p. First assume $p = 1$, and we may further assume that $\mathfrak{a}_i$ is a principal ideal generated by an element $x_1 \notin k$. Then $x_1 = P(Y_1, \dots, Y_m)$, where P is a non-constant polynomial. We shall see that, for a suitable choice of integers $r_i > 0$, the ring A is integral over $B = k[x_1, x_2, \dots, x_m]$, where

$$x_i = Y_i - Y_1^{r_1} \quad \text{for } 2 \le i \le m. \tag{3.0.1}$$

For this it is sufficient to choose the r_i such that Y_1 is integral over B (Proposition 13.1.10). Now, there is the relation

$$P(Y_1, x_2 + Y_1^{r_2}, \dots, x_m + Y_1^{r_m}) - x_1 = 0 \tag{3.0.2}$$

Write $P = \sum_\alpha a_\alpha Y^\alpha$, where $\alpha \in \mathbb{N}^m$ and $a_\alpha \in k$ are nonzero elements of k. Then (3.0.2) becomes

$$\sum_\alpha a_\alpha Y_1^{\alpha_1}(x_2 + Y_1^{r_2})^{\alpha_2} \cdots (x_m + Y_1^{r_m})^{\alpha_m} - x_1 = 0. \tag{3.0.3}$$

Let us write $f(\alpha) = \alpha_1 + r_2\alpha_2 + \cdots + r_m\alpha_m$ and suppose that the r_i are chosen so that the $f(\alpha)$ are distinct (it suffices for example to take $r_i = h^i$, where h is an integer strictly greater than all the α_i. Then there will be a unique system $\alpha = (\alpha_1, \dots, \alpha_m)$ such that $f(\alpha)$ is maximal and relation (3.0.3) may be written

$$a_\alpha Y_1^{f(\alpha)} + \sum_{j<f(\alpha)} Q_j(x_1, \dots, x_m) Y_1^j = 0. \tag{3.0.4}$$

where the Q_i are polynomials in $k[Y_1, \dots, Y_m]$. As $a_\alpha \neq 0$ is invertible in k, (3.0.4) is certainly an equation of integral dependence with coefficients in B, whence our assertion.

The field of fractions $k(Y_1, \dots, Y_m)$ of A is therefore algebraic over the field of fractions $k(x_1, \dots, x_m)$ of B, which proves that the x_i are algebraically independent. Moreover, every element $z \in \mathfrak{a}_1 \cap B$ may be written $z = x_1\tilde{z}$, where $\tilde{z} \in A \cap k(x_1, \dots, x_m)$. But $A \cap k(x_1, \dots, x_m) = k[x_1, \dots, x_m] = B$ since B is integrally closed by Corollary 13.1.33, whence $\mathfrak{a}_1 \cap B = Bx_1$.

We now do not assume that $\mathfrak{a}_1$ is principal and prove the theorem for $p = 1$ by induction on m. We may obviously suppose that $\mathfrak{a}_1 \neq 0$. Let x_1 be a non-zero element of $\mathfrak{a}_1$. By the argument above there exist $t_2, \dots, t_m$ such that $x_1, t_2 \dots, t_m$ are algebraically independent over k, A is integral over $C = k[x_1, t_2, \dots, t_m]$ and $x_1A \cap C = x_1C$. By the induction hypothesis there exist algebraically independent elements $x_2, \dots, x_m$ of $k[t_2, \dots, t_m]$ and an integer h such that

$k[t_2, \dots, t_m]$ is integral over $\tilde{B} = k[x_2, \dots, x_m]$, and the ideal $\mathfrak{a}_1 \cap \tilde{B}$ is generated by $x_2, \dots, x_h$. Then C is integral over $B = k[x_1, x_2, \dots, x_m]$ and hence so is A, therefore $x_1, \dots, x_m$ are algebraically independent over k. Finally, as $x_1 \in \mathfrak{a}_1$ and $B = \tilde{B}[x_1]$, $\mathfrak{a}_1 \cap B = Bx_1 + (\mathfrak{a}_1 \cap \tilde{B})$ and, as $\mathfrak{a}_1 \cap \tilde{B}$ is generated (in $\tilde{B}$) by $x_2, \dots, x_h$, we see $\mathfrak{a}_1 \cap B$ is generated (in B) by $x_1, x_2, \dots, x_h$.

Now assume the we have proved the theorem for $p-1$ idaels and let $t_1, \dots, t_m$ be elements of A satisfying the conditions of the theorem for the increasing sequence of ideals $\mathfrak{a}_1 \subset \cdots \subset \mathfrak{a}_{p-1}$ and let us write $r = h_{p-1}$. Apply the preceding proof for $\mathfrak{a}_p$, there exist algebraically independent elements $x_{r+1}, \dots, x_m$ of $C = k[t_{r+1}, \dots, t_m]$ and an integer s such that C is integral over $\tilde{B} = k[x_{r+1}, \dots, x_m]$ and the ideal $\mathfrak{a}_p \cap \tilde{B}$ is generated by $x_{r+1}, \dots, x_s$. Now write $x_i = t_i$ for $1 \le i \le r$ and $h_p = s$, then A is integral over $C[t_1, \dots, t_r]$ and hence also over $B = k[x_1, \dots, x_m] = \tilde{B}[t_1, \dots, t_r]$ since C is integral over $\tilde{B}$ (Corollary 13.1.14). In particular, we see the x_i are algebraically independent over k. On the other hand, for $j \le p-1$, the ideal

$$\mathfrak{a}_j \cap k[x_1, \dots, x_r, t_{r+1}, \dots, t_m]$$

is by hypothesis the set of polynomials in $x_1, \dots, x_r, t_{r+1}, \dots, t_m$ all of whose monomials contain one of the elements $x_1, \dots, x_{h_j}$. As $x_{r+1}, \dots, x_m$ are polynomials in $t_{r+1}, \dots, t_m$ with coeflficients in k, it is seen immediately that a polynomial in $x_1, \dots, x_m$ (with coefficients in k) can belong to $\mathfrak{a}_j$ only if all its monomials contain one of the elements $x_1, \dots, x_{h_j}$. Finally, as $x_1, \dots, x_r$ belong to $\mathfrak{a}_{p-1}$ and hence also to $\mathfrak{a}_p$, $\mathfrak{a}_p \cap \tilde{B}[x_1, \dots, x_r]$ consists of the polynomials in $x_1, \dots, x_r$ with coefficients in $\tilde{B}$ whose constant term belongs to $\mathfrak{a}_p \cap \tilde{B}$. This ideal is therefore generated by $x_1, \dots, x_r, x_{r+1}, \dots, x_s$. Therefore we see $(x_i)_{1 \le i \le m}$ satisfies the required conditions, which proves the theorem. □

Corollary 13.3.2. *Let A be an integral domain and B a finitely generated A-algebra containing A as a subring. Then there exist a nonzero element s of A and a subalgebra C of B isomorphic to a polynomial algebra $A[Y_1, \dots, Y_n]$ such that B_s is integral over C_s.*

Proof. Wewrite $S = A - \{0\}$ and let $k = S^{-1}A$ the field of fractions of A. Clearly $S^{-1}B$ is a finitely generated k-algebra and, as it contains k by hypothesis, it is not reduced to 0. By Theorem 13.3.1 applied to $\mathfrak{a}_1 = (0)$, there exists therefore a finite sequence $(x_i)_{1 \le i \le n}$ of elements of $S^{-1}B$ which are algebraically independent over k and such that $S^{-1}B$ is integral over $k[x_1, \dots, x_n]$. Let $(z_j)_{1 \le j \le m}$ be a system of generators of the A-algebra B. Then in $S^{-1}B$ each of the $z_j/1$ satisfies an equation of integral dependence

$$(z_j/1)^{q_j} + \sum_{k<q_j} P_{kj}(x_1, \dots, x_n)(z_j/1)^k = 0.$$

where the P_{kj} are polynomials in the x_i with coefficients in k. There exists an element $s \neq 0$ of A such that we may write $x_i = y_i/s$ where $y_i \in B$ and all the coefficients of the P_{kj} are of the form c/s where $c \in A$. Finally, replacing if need be, s by a product of elements of S, we may assume that in B,

$$s z_j^{q_j} + \sum_{k<q_j} Q_{kj} z_j^h = 0. \tag{3.0.5}$$

where the Q_{kj} are polynomials in $y_1, \dots, y_n$ with coeflicients in A. If we write $\tilde{z}_j = s z_j$, it is seen from (3.0.5) by multiplying $s^{q_j - 1}$ that $\tilde{z}_j$ is integral over $\tilde{B} = A[y_1, \dots, y_n]$. We show that the y_i are algebraically independent over A. If there is a relation of the form $\sum_\alpha a_\alpha y_1^{\alpha_1} \cdots y_n^{\alpha_n} = 0$

where $a_\alpha \in A$ for all α, we deduce that $\sum_\alpha b_\alpha x_1^{\alpha_1} \cdots x_n^{\alpha_n} = 0$ in $S^{-1}B$, where $b_\alpha = a_\alpha s^{|\alpha|}$. By hypothesis therefore $b_\alpha = 0$ for all α, whence $a_\alpha = 0$ for all α. Moreover, by Proposition 13.1.38 in the ring B_s each of the $\tilde{z}_j/1$ is integral over $\tilde{B}_s$ and, as $z_j/1 = (\tilde{z}_j/1)(1/s)$ in B_s, it is seen that the $z_j/1$ are integral over $\tilde{B}_s$, which completes the proof. □

Corollary 13.3.3. *Let L be a field, A a subring of L and K the field of fractions of A. If L is a finitely generated A-algebra, then $[L : K]$ is finite and there exists a nonzero element a in A such that $K = A_a$.*

Proof. It follows from Corollary 13.3.2 that there exist elements $x_1, \dots, x_n$ of L and an element $a \neq 0$ of A such that $x_1, \dots, x_n$ are algebraically independent over A (and therefore over K) and that L is integral over the subring $A[x_1, \dots, x_n]_a$. Then it follows from Proposition 13.1.62 that $A[x_1, \dots, x_n]_a$ is a field. But the only invertible elements of a polynomial ring $C[Y_1, \dots, Y_n]$ over an integral domain C are the invertible elements of C. Applying this remark to $C = A_a$, it is seen that necessarily $n = 0$ and that A_a is a field equal to K by definition of the latter. As L is integral over K and is a finitely generated K-algebra, the degree $[L : K]$ is finite. □

Corollary 13.3.4. *Let A be an integral domain, B a finitely generated A-algebra and b a nonzero element of B such that $z^n b \neq 0$ for all $z \neq 0$ in A and every integer $n > 0$. Let $\rho : A \to B$ be the canonical homomorphism. Then there exists a nonzero a in A such that, for every homomorphism ϕ from A to an algebraically closed field Ω such that $\phi(a) \neq 0$, there exists a homomorphism $\tilde{\phi}$ from B to Ω such that $\tilde{\phi}(b) \neq 0$ and $\phi = \tilde{\phi} \circ f$.*

Proof. The hypothesis on b implies that, if i is the canonical homomorphism $x \mapsto x/1$ of B to B_b, the homomorphism $i \circ f$ of A to B_b is injective. By Corollary 13.3.2 there therefore exist an element $a \neq 0$ of A and a subring $\tilde{B}$ of B_b such that $(B_b)_a$ is integral over $\tilde{B}_a$ and $\tilde{B}$ is isomorphic to a polynomial algebra $A[Y_1, \dots, Y_n]$. Let ϕ be a homomorphism from A to an algebraically closed field Ω such that $\phi(a) \neq 0$. There exists a homomorphism from $A[Y_1, \dots, Y_n]$ to Ω extending ϕ and hence there exists a homomorphism from $\tilde{B}$ to Ω extending ϕ, which we still denote by ϕ. As $\phi(a) \neq 0$ in Ω, there exists a homomorphism ψ from $\tilde{B}_a$ to Ω such that

$$\psi(x/a^n) = \phi(x)(\phi(a))^{-n}$$

for all $x \in \tilde{B}$ and all $n > 0$. Finally, as $(B_b)_a$ is integral over $\tilde{B}_a$, there exists a homomorphism $\tilde{\psi}$ from $(B_b)_a$ to Ω extending ψ (Corollary 13.1.73). If $j : x \mapsto x/1$ is the canonical homomorphism from B to $(B_b)_a$, then $\tilde{\phi} = \tilde{\psi} \circ j$ solves the problem for $j(b)$ is invertible in $(B_b)_a$ and hence $\tilde{\psi}(j(b)) \neq 0$ in Ω. □

Theorem 13.3.5. *Let A be a finitely generated integral k-algebra, K its field of fractions, L a finite algebraic extension of K, and $\bar{A}$ the integral closure of A in L. Then $\bar{A}$ is a finitely generated A-module and a finitely generated k-algebra.*

Proof. By Theorem 13.3.1 there exists a subalgebra C of A isomorphic to a polynomial algebra $k[X_1, \dots, X_n]$ and such that A is integral over C. Then $\bar{A}$ is obviously the integral closure of C in L (Proposition 13.1.16). We may therefore confine our attention to the case where $A = k[X_1, \dots, X_n]$.

Let N be the normal extension of L (in an algebraic closure of L) generated by L, which is a finite algebraic extension of K. It will suffice to prove that the integral closure of A in N is a finitely generated A-module, for $\bar{A}$ is a sub-A-module of that ring and A is a Noetherian ring.

We may therefore confine our attention to the case where L is a finite normal extension of K. Then we know that L is a (finite) Galois extension of a (finite) purely inseparable extension K' of K. If A' is the integral closure of A in K', $\overline{A}$ is the integral closure of A' in L and it will suffice to prove that A' is a finitely generated A-module and $\overline{A}$ is a finitely generated A'-module. Now, if it has been proved that A' is a finitely generated A-module, it is a Noetherian domain, integrally closed by definition. The fact that $\overline{A}$ is a finitely generated A'-module will follow from Corollary 13.1.50.

We see that we may confine our attention to the case where $A = k[X_1, \dots, X_n]$ and where L is a finite purely inseparable extension of $K = k(X_1, \dots, X_n)$. Then L is generated by a finite family of elements $(y_i)_{1 \le i \le m}$ and there exists a power q of the characteristic of k such that $y_i^q \in k(X_1, \dots, X_n)$ for all i. Let $(c_i)_{1 \le i \le r}$ be the coefficients of the numerators and denominators of the rational functions in $X_1, \dots, X_n$ that equal to y_i^q. Then L is contained in the extension $L' = k'(X_1^{1/q}, \dots, X_n^{1/q})$, where $k' = k(c_1^{1/q}, \dots, c_r^{1/q})$ (we are in an algebraic closure of L) and $\overline{A}$ is contained in the algebraic closure A' of A in L'. Now, k' is algebraic over k and hence $C' = k'[X_1, \dots, X_n]$ is integral over A. As $k'[X_1^{1/q}, \dots, X_n^{1/q}]$ is integrally closed by Corollary 13.1.34, it is seen that this ring is the integral closure of C' in L' and hence also that of A, in other words, $A' = k'[X_1^{1/q}, \dots, X_n^{1/q}]$. Now clearly A' is a finitely generated C'-module and, as k' is a finite extension of k, C' is a finitely generated A-module and hence A' is a finitely generated A-module. Since A is Noetherian and $\overline{A} \subseteq A'$, we see $\overline{A}$ is a finitely generated A-module. □

13.3.1 The Nullstellensatz

Proposition 13.3.6. *Let A be a finitely generated algebra over a field k and Ω the algebraic closure of k.*

(a) If $A \neq \{0\}$, there exists a nonzero k-homomorphism from A to Ω.

(b) Let ϕ_1, ϕ_2 be two k-homomorphisms from A to Ω. For ϕ_1 and ϕ_2 to have the same kernel, it is necessary and sufficient that there exist a k-automorphism σ of Ω such that $\phi_2 = \sigma \circ \phi_1$.

(c) Let $\mathfrak{a}$ be an ideal of A. For $\mathfrak{a}$ to be maximal, it is necessary and suffieient that it be the kernel of a k-homomorphism from A to Ω.

(d) For an element x of A to be such that $\phi(x) = 0$ for every k-homomorphism from A to L, it is necessary and sufficient that x be nilpotent.

Proof. Assertion (a) follows Corollary 13.3.4 applied replacing A by k, B by A, b by the unit element of B and ϕ by the canonical injection of k into Ω.

If ϕ is a k-homomorphism from A to Ω, $\phi(A)$ is a subring of Ω containing k. As Ω is an algebraic extension of k, $\phi(A)$ is a field and, if $\mathfrak{a}$ is the kernel of ϕ, $A/\mathfrak{a}$ is isomorphic to $\phi(A)$, therefore is a field, which proves that $\mathfrak{a}$ is maximal. Conversely, if $\mathfrak{a}$ is a maximal ideal of A it follows from (a) that there exists a k-homomorphism from $A/\mathfrak{a}$ to Ω and hence a k-homomorphism of A to Ω whose kernel $\mathfrak{b}$ contains $\mathfrak{a}$. But as $\mathfrak{a}$ is maximal, $\mathfrak{b} = \mathfrak{a}$, this proves (c).

We now prove (b). If σ is a k-automorphism of Ω such that $\phi_2 = \sigma \circ \phi_1$, clearly ϕ_1 and ϕ_2 have the same kernel. Conversely, suppose that ϕ_1 and ϕ_2 have the same kernel. Then there exists a k-isomorphism σ_0 of the field $\phi_1(A)$ onto the field $\phi_2(A)$ such that $\phi_2 = \sigma \circ \phi_1$. But by Theorem 9.1.32, σ_0 extends to a k-automorphism σ of Ω and hence $\phi_2 = \sigma \circ \phi_1$.

Finally, if $x \in A$ is such that $x^n = 0$, for every k-homomorphism ϕ from A to Ω, $(\phi(x))^n = \phi(x^n) = 0$ and hence $\phi(x) = 0$ since Ω is a field. Conversely, suppose that $x \in A$ is not nilpotent. Then A_x is a finitely generated A-algebra (and therefore a finitely generated k-algebra) not reduced to 0 and hence there exists a k-homomorphism ψ from A_x to Ω by (a). If $j : A \to A_x$ is the canonical homomorphism, $\phi = \psi \circ j$ a k-homomorphism from A to Ω and $\phi(x)\psi(1/x) = \psi(x/1)\psi(1/x) = \psi(1) = 1$, whence $\phi(x) \neq 0$. □

Lemma 13.3.7. *Let A be a finitely generated algebra over a field k, $(a_i)_{1\leq i\leq n}$ a system of generators of this algebra and $\mathfrak{r}$ the ideal of algebraic relations between the a_i with eoeflieients in k. For every extension field L of k, the mapping $\phi \mapsto (\phi(a_i))$ is a bijection of the set of k-homomorphisms from A to L onto the set of zeros of $\mathfrak{r}$ in L^n.*

Proof. There exists a unique k-algebra homomorphism η of $k[X_1, \dots, X_n]$ onto A such that $\eta(X_i) = a_i$ for $1 \leq i \leq n$ and by definition $\mathfrak{r}$ is the kernel of η. The map $\phi \mapsto \phi \circ \eta$ is a bijection of the set of k-homomorphisms from A to Ω onto the set of k-homomorphisms from $k[X_1, \dots, X_n]$ to Ω which are zero on $\mathfrak{r}$. For every polynomial $P \in k[X_1, \dots, X_n]$ and every element $\boldsymbol{x} = (x_1, \dots, x_n) \in L^n$ we write $\eta_{\boldsymbol{x}}(P) = P(\boldsymbol{x})$. Then the mapping $\boldsymbol{x} \mapsto \eta_{\boldsymbol{x}}$ is a bijection of L^n onto the set of k-homomorphisms from $k[X_1, \dots, X_n]$ to L (such a homomorphism being determined by its values at the X_i). To say that $\eta_{\boldsymbol{x}}$ is zero on $\mathfrak{r}$ means that $\boldsymbol{x}$ is a zero of $\mathfrak{r}$ in L^n, whence the lemma. □

Proposition 13.3.8 (Hilbert's Nullstellensatz). *Let k be a field and Ω an algebraic closure of k.*

(a) Every proper ideal $\mathfrak{r}$ of $k[X_1, \dots, X_n]$ admits at least one zero in Ω^n.

(b) Let $\boldsymbol{x}, \boldsymbol{y}$ be two elements of Ω^n. For the set of polynomials of $k[X_1, \dots, X_n]$ zero at $\boldsymbol{x}$ to be identical with the set of polynomials of $k[X_1, \dots, X_n]$ zero at $\boldsymbol{y}$, it is necessary and sufficient that there exists a k-automorphism σ such that $\boldsymbol{y} = \sigma(\boldsymbol{x})$.

(c) For an ideal $\mathfrak{a}$ of $k[X_1, \dots, X_n]$ to be maximal, it is necessary and sufficient that there exist an $\boldsymbol{x}$ in Ω^n such that $\mathfrak{a}$ is the set of polynomials of $k[X_1, \dots, X_n]$ zero at $\boldsymbol{x}$.

(d) For a polynomial P of $k[X_1, \dots, X_n]$ to be zero on the set of zeros in Ω^n of an ideal $\mathfrak{r}$ of $k[X_1, \dots, X_n]$, it is necessary and sufficient that there exist an integer $n > 0$ such that $P^n \in \mathfrak{r}$.

Proof. Apply Proposition 13.3.6 to the algebra $A = k[X_1, \dots, X_n]/\mathfrak{r}$ and use Lemma 13.3.7, we obtain part (a) and (d). Also, part (b) and (c) follows by the same argument applied to $A = k[X_1, \dots, X_n]$. □

13.3.2 Jacobson rings

Proposition 13.3.9. *Let A be a ring. Then the following conditions are equivalent.*

(i) Every prime ideal of A is the intersection of a family of maximal ideals.

(ii) For every ideal $\mathfrak{a}$ of A, the Jacobson radical of $A/\mathfrak{a}$ be equal to its nilradical.

(iii) For every ideal $\mathfrak{a}$ of A, the radical of $\mathfrak{a}$ is the intersection of the maximal ideals of A containing $\mathfrak{a}$.

(iv) Every prime ideal in A which is not maximal is equal to the intersection of the prime ideals which contain it strictly.

Proof. The Jacobson radical (resp. nilradical) of $A/\mathfrak{a}$ is the intersection of the maximal (resp. prime) ideals of $A/\mathfrak{a}$. Thus (ii) means for every ideal $\mathfrak{a}$ of A the intersection of the prime ideals containing $\mathfrak{a}$ is equal to the intersection of the maximal ideals containing $\mathfrak{a}$. This condition obviously holds for every ideal $\mathfrak{a}$ of A if (i) holds, and it implies (i) by taking $\mathfrak{a}$ to be prime ideals of A. This proves the equivalence of (i) and (ii). Also, it is clear that (iii) is equivalent to (ii)

Now assume (i) and let $\mathfrak{p}$ be a prime ideal of A that is not maximal. Then by (i), since $\mathfrak{p}$ is non maximal, we have

$$\mathfrak{p} = \bigcap_{\mathfrak{m}\supsetneq\mathfrak{p},\mathfrak{m}\in\mathrm{Max}(A)} \mathfrak{m} \supseteq \bigcap_{\mathfrak{q}\supsetneq\mathfrak{p},\mathfrak{q}\in\mathrm{Spec}(A)} \mathfrak{q} \supseteq \mathfrak{p}$$

whence (iv) holds. Conversely, suppose there is a prime ideal which is not an intersection of maximal ideals. Passing to the quotient ring, we may then assume that A is an integral domain whose Jacobson radical $\mathfrak{r}$ is not zero. Let a be a non-zero element of $\mathfrak{r}$. Then $A_a \neq 0$ since a is not nilpotent, hence has a maximal ideal, whose contraction in A is a prime ideal $\mathfrak{p}$ such that $a \notin \mathfrak{p}$. Since $a \in \mathfrak{r}$ we see $\mathfrak{p}$ is not maximal. Moreover, by our choice of $\mathfrak{p}$, every prime ideal of A that strictly contains $\mathfrak{p}$ has nonempty with the multiplicative subset $S = \{a^n : n > 0\}$ and therefore contains a. Hence a is contained in the intersection of prime ideals containing $\mathfrak{p}$ strictly, which therefore is not equal to $\mathfrak{p}$. This shows the equivalence of (i) and (iv) and completes the proof. □

A ring A is called a **Jacobson ring** if it satisfies the equivalent conditions of Proposition 13.3.9.

Example 13.3.10 (Examples of Jacobson rings).

(a) Every field is a Jacobson ring.

(b) The ring $\mathbb{Z}$ is a Jacobson ring, the unique prime ideal which is not maximal (0) being the intersection of the maximal ideals (p) of $\mathbb{Z}$, where p runs through the set of prime numbers.

(c) Let A be a Jacobson ring and let $\mathfrak{a}$ be an ideal of A. Then $A/\mathfrak{a}$ is a Jacobson ring, for the ideals of $A/\mathfrak{a}$ are of the form $\mathfrak{b}/\mathfrak{a}$, where $\mathfrak{b}$ is an ideal of A containing $\mathfrak{a}$ and $\mathfrak{b}/\mathfrak{a}$ is prime (resp. maximal) if and only if $\mathfrak{b}$ is.

Proposition 13.3.11. *Let A be a PID and $(p_i)_{i\in I}$ a representative system of irreducible elements of A. For A to be a Jacobson ring, it is necessary and sufficient that I be infinite.*

Proof. The maximal ideals of A are the (p_i). If I is finite, their intersection is the ideal (x) where $x = \prod_i p_i$ and hence different from (0). On the other hand, if I is infinite, the intersection of the (p_i) is (0), since every nonzero element of A can be divisible by only a finite number of irreducible elements. The proposition then follows from the fact that (0) is the only prime ideal which is not maximal in A. □

Proposition 13.3.12. *Let A be a ring and B an A-algebra integral over A. If A is a Jacobson ring, so is B.*

Proof. Replacing A by its canonical image in B, we may assume that $A \subseteq B$. Let $\mathfrak{P}$ be a prime ideal of B and let $\mathfrak{p} = A \cap \mathfrak{P}$. There exists by hypothesis a family $(\mathfrak{m}_i)_{i\in I}$ of maximal ideals of A whose intersection is equal to $\mathfrak{p}$. For all $i \in I$ there exists a maximal ideal $\mathfrak{M}_i$ of B lying over

$\mathfrak{m}_i$ and containing $\mathfrak{P}$ by the going up theorem. If we write $\mathfrak{Q} = \bigcap_i \mathfrak{M}_i$, then $\mathfrak{Q} \cap A = \bigcap_i \mathfrak{m}_i = \mathfrak{p}$ and $\mathfrak{Q} \supseteq \mathfrak{P}$, whence $\mathfrak{Q} = \mathfrak{P}$. □

Proposition 13.3.13. *Let A be a Jacobson ring, B a finitely generated A-algebra and $\rho : A \to B$ the canonical homomorphism. Then B is a Jacobson ring and for every maximal ideal $\mathfrak{M}$ of B, $\mathfrak{m} = \mathfrak{M}^c$ is a maximal ideal of A and $B/\mathfrak{M}$ is a finite algebraic extension of $A/\mathfrak{m}$.*

Proof. Let $\mathfrak{P}$ be a prime ideal of B and $\mathfrak{p} = \mathfrak{P}^c$. Let v be a nonzero element of $B/\mathfrak{P}$. As $B/\mathfrak{P}$ is a finitely generated integral $(A/\mathfrak{p})$-algebra and the canonical homomorphism $\eta : A/\mathfrak{p} \to B/\mathfrak{P}$ is injective, there exists a nonzero element u of $A/\mathfrak{p}$ such that, for every homomorphism ϕ from $A/\mathfrak{p}$ to an algebraically closed field Ω such that $\phi(u) \neq 0$, there exists a homomorphism ψ from $B/\mathfrak{P}$ to Ω such that $\psi(v) \neq 0$ and for which $\phi = \psi \circ \eta$ (Corollary 13.3.4). Since A is a Jacobson ring, there exists a maximal ideal $\mathfrak{m}$ of A containing $\mathfrak{p}$ and such that $u \notin \mathfrak{m}/\mathfrak{p}$. We take Ω to be an algebraic closure of $A/\mathfrak{m}$ and ϕ to be the canonical homomorphism $A/\mathfrak{p} \to \Omega$. Let $\psi : B/\mathfrak{P} \to \Omega$ be a homomorphism such that $\phi = \psi \circ \eta$ and $\psi(v) \neq 0$. Then

$$A/\mathfrak{m} \subseteq \phi(B/\mathfrak{P}) \subseteq \Omega$$

hence $\psi(B/\mathfrak{P})$ is a subfield of Ω and the kernel of ψ is therefore a maximal ideal of $B/\mathfrak{P}$ not containing v. Thus it is seen that the intersection of the maximal ideals of $B/\mathfrak{P}$ is reduced to 0, which proves that B is a Jacobson ring. Moreover, if $\mathfrak{P}$ is maximal, ψ is necessarily injective and hence $\mathfrak{p} = \mathfrak{m}$ is maximal. Finally $B/\mathfrak{P}$ is then a finitely generated algebra over the field $A/\mathfrak{m}$ and hence is a finite extension of $A/\mathfrak{m}$. □

Corollary 13.3.14. *Let A be a Jacobson ring. If there exists a finitely generated A-algebra B containing A and which is a field, then A is a field and B is an algebraic extension of A.*

Proof. It suffices to apply Proposition 13.3.13 with $\mathfrak{M} = (0)$. □

Corollary 13.3.15. *Every finitely generated algebra A over $\mathbb{Z}$ is a Jacobson ring. For a prime ideal $\mathfrak{p}$ of A to be maximal, it is necessary and sufficient that the ring $A/\mathfrak{p}$ be finite.*

Proof. If the integral domain $A/\mathfrak{p}$ is finite, it is a field, as, for every $u \neq 0$ in $A/\mathfrak{p}$, the mapping $v \mapsto uv$ of $A/\mathfrak{p}$ to itself is injective and hence bijective since $A/\mathfrak{p}$ is finite. Conversely, for every maximal ideal $\mathfrak{m}$ of A, the inverse image of $\mathfrak{m}$ in $\mathbb{Z}$ is a maximal ideal (p) and $A/\mathfrak{m}$ is finite over the prime field $\mathbb{Z}/(p) = \mathbb{F}_p$ by Proposition 13.3.13. □

Remark 13.3.1. Let A be a Jacobson ring. Then the ring $A[\![X]\!]$ is not Jacobson: in fact, let $\mathfrak{p}$ be a prime ideal of A, then $\mathfrak{p}A[\![X]\!]$ is not an intersection of maximal ideals of $A[\![X]\!]$ since any such ideal contains $X \cdot A[\![X]\!]$.

Theorem 13.3.16. *Let A be a ring. Then the following are equivalent.*

(i) A is a Jacobson ring.

(ii) Every finitely generated A-algebra B that is a field is finite over A.

Proof. First assume (ii). Let $\mathfrak{p}$ be a prime ideal of A which is not maximal, and let $B = A/\mathfrak{p}$. Let v be a non-zero element of B. Then $B_v = B[v^{-1}]$ is a finitely generated A-algebra. If it is a field then by condition (ii) it is finite over A, hence integral over B and therefore B is a field by

Proposition 13.1.62. Since $\mathfrak{p}$ is not maximal, we then see B_v is not a field and therefore has a non-zero maximal ideal, whose contraction in B is a non-zero prime ideal $\mathfrak{q}$ such that $v \notin \mathfrak{q}$. By Proposition 13.3.9(iv), this shows A is a Jacobson ring.

Conversely, let A be a Jacobson ring and B be a finitely generated A-algebra that is a field. Since a quotient ring of a Jacobson ring is Jacobson, we can assume B contains A as a subring. Let $s \in A$ be such that for every homomorphism ϕ from A to an algebraically closed field Ω such that $\phi(s) \neq 0$, there exists a homomorphism $\tilde{\phi}$ from B to Ω extending ϕ (Corollary 13.3.4). Since A is then a integral domain and Jacobson, there exists a maximal ideal $\mathfrak{m}$ of A not containing s. We take Ω to be the algebraic closure of $A/\mathfrak{m}$ and ϕ the canonical homomorphism $A \to A/\mathfrak{m} \to \Omega$. Then ϕ extends to a homomorphism ψ of B into Ω. Since B is a field, ψ is injective, and so B is algebraic (thus finite algebraic) over $A/\mathfrak{m}$, whence finite over A. □

Since a field is Jacobson, we get immediately the following statement.

Corollary 13.3.17 (Zariski's Lemma). *Let k ba a field and K a finitely generated k-algebra. If K is a field then it is a finite field extension of k.*

13.4 Exercise

Exercise 13.4.1. Let A be a Noetherian ring and $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ be all the minimal prime ideals of A. Suppose that $A_\mathfrak{p}$ is an integral domain for all $\mathfrak{p} \in \operatorname{Spec}(A)$. Then

(a) $\operatorname{Ass}(A) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$.

(b) $\mathfrak{n}(A) = \bigcap_{i=1}^n \mathfrak{p}_i = (0)$.

(c) $\mathfrak{p}_i + \bigcap_{j \neq i} \mathfrak{p}_j = A$ for all i.

Deduce that $A \cong A/\mathfrak{p}_1 \times \cdots \times A/\mathfrak{p}_n$.

Proof. Recall $\mathfrak{n}(A_\mathfrak{p}) = (\mathfrak{n}(A))_\mathfrak{p}$ from Corollary 10.2.38, but $(\mathfrak{n}(A))_\mathfrak{p} = (0)$ for all $\mathfrak{p} \in \operatorname{Spec}(A)$, so by Proposition 10.3.18 $\mathfrak{n}(A) = \bigcap_{i=1}^n \mathfrak{p}_i = (0)$. By Corollary 12.1.9,we then have

$$\operatorname{Ass}(A) \subseteq \bigcup_{i=1}^n \operatorname{Ass}(A/\mathfrak{p}_i) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}.$$

Since $\operatorname{supp}(A) = \operatorname{Spec}(A)$ and $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ are the minimal element of $\operatorname{Spec}(A)$, we then get $\operatorname{Ass}(A) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$.

We first prove that $\mathfrak{p}_i + \mathfrak{p}_j = A$ for any $i \neq j$: Assume the converse, then $\mathfrak{p}_i + \mathfrak{p}_j \subseteq \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. Then, in the localization $A_\mathfrak{m}$ there are two distinct minimal ideals $\mathfrak{p}_i A_\mathfrak{m}$ and $\mathfrak{p}_j A_\mathfrak{m}$. Thus

$$\mathfrak{n}(A_\mathfrak{m}) = \mathfrak{p}_i A_\mathfrak{m} \cap \mathfrak{p}_j A_\mathfrak{m}$$

Since $A_\mathfrak{m}$ is an integral domain, and $\mathfrak{p}_i \cap \mathfrak{p}_j \neq 0$, this is a contradiction.

Now since $\mathfrak{p}_i + \mathfrak{p}_j = A$, for $j \neq i$ we have

$$x_j + y_j = 1, \quad x_j \in \mathfrak{q}_i, y_j \in \mathfrak{q}_j$$

Now

$$\prod_{j\neq i}(1-x_i) = \prod_{j\neq i} y_j \in \bigcap_{j\neq i} \mathfrak{q}_j$$

and expand the term $\prod_{j\neq i}(1-x_i)$ we get $1+x$ for $x \in \mathfrak{q}_i$. Hence $\mathfrak{q}_i + \bigcap_{j\neq i} \mathfrak{p}_j = A$.

Finally, $\mathfrak{p}_i$ and $\mathfrak{p}_j$ are coprime, by the Chinese remainder theorem we have the claimed isomorphism. □

Chapter 14

Valuation rings

14.1 Valuation rings of fields

Let A be an integral domain, K its field of fractions. A is a **valuation ring** if, for each $x \in K$ and $x \neq 0$, either $x \in A$ or $x^{-1} \in A$ (or both). The case $A = K$ is the trivial valuation ring.

Proposition 14.1.1. *Let A be an integral domain, K its field of fractions. Then A is a valuation ring of K if and only if idels of A is totally ordered by inclusion.*

Proof. Assume that A is a valuation ring of K and let I, J be two ideals such that there is $b \in J$, $b \notin I$. Now for $a \in I$, either $a/b \in A$ or $b/a \in A$. If $b/a \in A$, then $b = (b/a) \cdot a \in I$, contradiction. So $a/b \in A$, and $a = b(a/b) \in J$. Hence $I \subseteq J$. Conversely, assume that ideals of A are totally ordered. Let $a, b \in A$. Then $(a) \subseteq (b)$ or $(b) \subseteq (a)$. Hence it is clear $a/b \in A$ or $b/a \in A$. This shows A is a valuation ring. □

Corollary 14.1.2. *If A is a valuation ring and $\mathfrak{p}$ is a prime ideal of A, then $A/\mathfrak{p}$ and $A_{\mathfrak{p}}$ are valuation rings of their fields of fractions.*

Proposition 14.1.3. *If A is a valuation ring of K, then*

(a) A is a local ring and if we write $\mathfrak{m}$ for the maximal ideal, then

$$K - A = \{x \in K^{\times} : x^{-1} \in \mathfrak{m}\}$$

Thus A is determined by K and $\mathfrak{m}$.

(b) A is integrally closed.

Proof. By Proposition 14.1.1, A has a unique maximal ideal, so is a local ring. Moreover, if $x \notin A$, then $x^{-1} \in A$ and x^{-1} is not a unit in A, so $x^{-1} \in \mathfrak{m}$. conversely, if $x^{-1} \in \mathfrak{m}$, then $x \notin A$ since x^{-1} is not a unit. Thus

$$K - A = \{x \in K^{\times} : x^{-1} \in \mathfrak{m}\}$$

Now given K and $\mathfrak{m}$, the set $K - A$ is then determined, so $A = K - (K - A)$ is uniquely determined.

Let $x \in K$ be integral over A. Then we have, say,

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

with the $b_i \in A$. If $x \in A$ there is nothing to prove. If not, then $x^{-1} \in A$, hence $x = -(a_{n-1} + a_{n-2}x^{-1} + \cdots + a_0 x^{-n}) \in A$. □

Proposition 14.1.4. *Let A be an integral domain, then the followings are equivalent:*

(i) A is a valuation ring.

(ii) A is a local domain and any finitely generated ideal is principal.

Proof. Let A be a valuation ring. By Proposition 14.1.3 A is a local ring. Let $I = (x_1, \ldots, x_n)$, since by Proposition 14.1.1 the set $\{(x_1), \ldots, (x_n)\}$ is totally ordered. Let's assume that (x_1) is the biggest element in it, then $(x_i) \subseteq (x_1)$ for all i, that is, $x_i = a_i x_1$. This implies I is generated by x_1.

Conversely, assume (b), and let $\mathfrak{m}$ be the unique maximal ideal of A. Write $\mathfrak{m}$ as the unqiue maximal ideal of A, so $J(A) = \mathfrak{m}$. Let $a, b \in A$, and write $(a, b) = (h)$. Then we have

$$a = uh, \ b = vh, \quad h = xa + yb, \quad u, v, x, y \in A.$$

Then $h = xuh + yvh$ are since A is a domain we get $1 = xu + yv$. If u is not a unit, then $u \in \mathfrak{m}$ and hence $1 - xu = yv$ is a unit. This implies v is a unit, and vice versa. Hence either $a/b \in A$ or $b/a \in A$, so A is a valuation ring. □

Proposition 14.1.5. *Let A be a valuation ring. Every finitely generated torsion-free A-madule is free. Every torsion-free A-module is flat.*

Proof. Let M be a finitely generated torsion-free A-module and let $x_1, \ldots, x_n$ be generators of E which are minimal in number; we show that they are linearly independent. If $\sum_{i=1}^n a_i x_i = 0$ is a non-trivial relation between the x_i, one of the a_i's, say a_1, divides all the others since the set of principal ideals of A is totally ordered by inclusion; then $a_1 \neq 0$ since the relation is non-trivial. As M is torsion-free, we can divide by a_1, which amounts to assuming that $a_1 = 1$. But then x_1 is a linear combination of $x_2, \ldots, x_n$, contrary to the minimal character of n. Hence M is free. The second claim follows since every finitely generated ideal is principal. □

Quite generally, we write $\mathfrak{m}_A$ for the maximal ideal of a local ring A. If A and B are local rings with $B \subseteq A$ and $\mathfrak{m}_B \cap A = \mathfrak{m}_A$, we say that B **dominates** A and write $B \geq A$. If $B \geq A$ and $B \neq A$, we write $B > A$.

Proposition 14.1.6. *Let A and B be local rings such that $A \subseteq B$. Then the following conditions are equivalent:*

(i) $\mathfrak{m}_A \subseteq \mathfrak{m}_B$;

(ii) B dominates A;

(iii) the ideal generated by $\mathfrak{m}_A$ in B is proper.

Proof. If $\mathfrak{m}_A \subseteq \mathfrak{m}_B$, then $\mathfrak{m}_B \cap A$ is a proper prime ideal containing the maximal ideal of A, so $\mathfrak{m}_A = \mathfrak{m}_B \cap A$ and B dominates A. If B dominates A, then the ideal $\mathfrak{m}_A B$ is contained in $\mathfrak{m}_B$ and so is proper, this shows (ii)⇒(iii). Finally, if (iii) holds, $\mathfrak{m}_A B$ is contained in the unique maximal ideal of $\mathfrak{m}_B$ of B, hence (i). □

Theorem 14.1.7. *Let K be a field, $A \subseteq K$ a subring, and $\mathfrak{p}$ a prime ideal of A. Then there exists a valuation ring B of K satisfying*

$$A \subseteq B, \quad \mathfrak{m}_B \cap A = \mathfrak{p}.$$

Moreover, valuation rings are maximal with respect to the domination relation.

Proof. Replacing A by $A_{\mathfrak{p}}$ we can assume that A is a local ring with $\mathfrak{p} = \mathfrak{m}_A$. Now write $\mathscr{F}$ for the set of all subrings of K containing A and to which $\mathfrak{p}$ extended to a nontrivial ideal. Now $A \in \mathscr{F}$, and if $\mathscr{L} \subseteq \mathscr{F}$ is a subset totally ordered by inclusion then the union of all the elements of $\mathscr{L}$ is again an element of $\mathscr{F}$, so that, by Zorn's lemma $\mathscr{F}$ has a maximal element B. Since $\mathfrak{p}^e \neq B$, there is a maximal ideal $\mathfrak{m}$ of B containing $\mathfrak{p}^e$. Then $B \subseteq B_{\mathfrak{m}} \in \mathscr{F}$, so that $B = B_{\mathfrak{m}}$, and B is local. Also $\mathfrak{p} \subseteq \mathfrak{m} \cap A$ and $\mathfrak{p}$ is a maximal ideal of A, so that $\mathfrak{m} \cap A = \mathfrak{p}$. Thus it only remains to prove that B is a valuation ring of K.

Let $x \in K$. If $x \notin B$ then since $B[x] \notin \mathscr{F}$ and $B[x] \supseteq A$, we must have $1 \in \mathfrak{p}B[x]$, and there exists a relation of the form

$$1 = a_0 + a_1 x + \cdots + a_n x^n, \quad a_i \in \mathfrak{p}B$$

Since $a_0 \in \mathfrak{p}B \subseteq \mathfrak{m} = J(B)$, $1 - a_0$ is unit of B and we can modify this to get a relation

$$1 = b_1 x + \cdots + b_n x^n, \quad b_i \in \mathfrak{m} \tag{1.0.1}$$

Among all such relations, choose one for which n is as small as possible. If we also have $x^{-1} \notin B$, then by the same argument, there is a relation

$$1 = c_1 x^{-1} + \cdots + c_m x^{-m}, \quad c_i \in \mathfrak{m} \tag{1.0.2}$$

for which m is as small as possible. If $n \geq m$ we can multiply (1.0.2) by $b_n x^n$ and substract from (1.0.1) to obtain a relation of the form (1.0.1) but with a strictly smaller degree n, which is a contradiction; if $n < m$ then we get the same contradiction on interchanging the roles of x and x^{-1}. Thus if $x \notin B$ we must have $x^{-1} \in B$.

Finally, if $A \subseteq B$ are valuation rings of K, then by Proposition 14.3.2 we have $\mathfrak{m}_B \subseteq \mathfrak{m}_A$, and $\mathfrak{m}_A = \mathfrak{m}_B$ iff $A = B$. It follows that B dominates A iff $A = B$. □

Theorem 14.1.8. *Let K be a field, $A \subseteq K$ a subring, and let $\overline{A}$ be the integral closure of A in K. Then $\overline{A}$ is the intersection of all the valuation rings of K containing A. If A is local, $\overline{A}$ is the intersection of the valuation rings of K which dominate A.*

Proof. Every element $x \in \overline{A}$ is integral over A, so over any valuation ring $B \supseteq A$. But since B is integer closed, we must have $x \in B$, thus $\overline{A} \subseteq B$ for every valuation ring containing A. Conversely, let $x \notin \overline{A}$. Then $x \notin A[x^{-1}]$, so x^{-1} is not a unit of $A[x^{-1}]$. It follows that x^{-1} is contained in a maximal ideal $\mathfrak{M}$ of $A[x^{-1}]$, and by Theorem 14.1.7 there exists a valuation ring B of K such that $B \supseteq A[x^{-1}]$ and $\mathfrak{m}_B \cap A[x^{-1}] = \mathfrak{M}$. Now since $x^{-1} \in \mathfrak{M} \subseteq \mathfrak{m}_B$, we have $x \notin B$. Further $\mathfrak{M} \cap A$ is a maximal ideal of A, hence, if A is local, $\mathfrak{M} \cap A = \mathfrak{m}_A$ and B dominates A. □

Corollary 14.1.9. *For an integral domain to be integrally closed, it is necessary and sufficient that it be the intersection of a family of valuation rings of its field of fractions.*

Corollary 14.1.10. *Let K be a field, L an extension of K and A a valuation ring of K. The integral closure of A in L is the intersection of the valuation rings B of L such that $B \cap K = A$.*

Proof. If B is a valuation ring of L, then $B \cap K$ is a valuation ring of K and B dominates $B \cap K$. For B to dominate A, it is necessary and sufficient that $B \cap K$ dominate A and therefore be equal to it. □

14.2 Ordered groups and valuations

Let Γ be a commutative group. A order $\leq$ on Γ is said to be compatible with the group structure of Γ if for $\alpha, \beta, \gamma, \delta \in \Gamma$,

$$\alpha \geq \beta, \gamma \geq \delta \Rightarrow \alpha + \gamma \geq \beta + \delta.$$

In this case, the group Γ is called an **ordered group**, and a **totally ordered group** if its order is a total order. In this section we only consider totally ordered groups and if Γ is an ordered group, we usually make an ordered set $\Gamma \cup \{\infty\}$ by adding to Γ an element ∞ bigger than all the elements of Γ, and fix the conventions $\infty + \alpha = \infty$ for $\alpha \in \Gamma$ and $\infty + \alpha = \infty$.

Example 14.2.1 (Examples of totally ordered groups).

(a) The additive group of real numbers $\mathbb{R}$, or any subgroup of this.

(b) The direct product $\mathbb{Z}^n$ of n copies of $\mathbb{Z}$, with lexicographical order.

(c) The group $\mathbb{Q}$ of rational integers.

Theorem 14.2.2. *For a commutative group Γ to be such that there exists on Γ a total ordering compatible with the group struclure of Γ, it is necessary aad sufficient that Γ be torsion free.*

Proof. If there exists such an order structure on Γ and if $\alpha > 0$, then $\alpha + \mu > 0$ for all $\mu > 0$ and in particular, by induction we see $n\alpha \geq 0$ which proves that Γ is torsion free. Conversely, if Γ is torsion-free, it is a sub-$\mathbb{Z}$-module of a vector $\mathbb{Q}$-space, which may be assumed of the form $\mathbb{Q}^{\oplus I}$. If I is given a well ordering and $\mathbb{Q}^{\oplus I}$ its usual ordering, the set $\mathbb{Q}^{\oplus I}$ with the lexicographical ordering is totally ordered. It is immediate that this ordering is compatible with the additive group structure of $\mathbb{Q}^{\oplus I}$. □

Let K be a field and Γ a totally ordered group. A map $v : K \to \Gamma \cup \{\infty\}$ is called an **additive valuation** or just a **valuation** of K if it satisfies the conditions

(a) $v(xy) = v(x) + v(y)$.

(b) $v(x + y) \geq \min\{v(x), v(y)\}$.

(c) $v(x) = \infty$ if and only if $x = 0$.

If we write $K^\times$ for the multiplicative group of K then v defines a homomorphism $K^\times \to \Gamma$ whose image is a subgroup of Γ, called the **value group** of v. The valuation v defined by $(x) = 0$ for any $x \in K^\times$ is called the **trivial valuation**.

Proposition 14.2.3. *Let v be a valuation on a field K. For any elements $x_1, \dots, x_n \in K$, we have*

$$v(\sum_{i=1}^{n} x_i) \geq \min\{v(x_1), \dots, v(x_n)\}.$$

Moreover, if there exists a single index k such that $v(x_k) = \min_i v(x_i)$, then the equality holds. In particular, if $v(x) \neq v(y)$, then $v(x+y) = \min\{v(x), v(y)\}$.

Proof. The first inequality follows by induction. Now if there exists a single index k such that $v(x_k) = \min_i v(x_i)$, then, writing $y = \sum_{i \neq k} x_i$ and $z = \sum_{i=1}^{n} x_i$, we have $v(y) > v(x_k)$ and $v(z) \geq v(x_k)$. If $v(z) > v(x_k)$, then the relation $x_k = z - y$ implies $v(x_k) \geq \min\{v(y), v(z)\} > v(x_k)$, which is absurd. Thus $v(z) = v(x_k)$ and the claim is proved. □

Valuations are connected to valuation rings in the following way. If v is a valuation on K, we set

$$A_v = \{x \in K \mid v(x) \geq 0\}, \quad \mathfrak{m}_v = \{x \in K \mid v(x) > 0\}, \quad \kappa_v = A_v/\mathfrak{m}_v.$$

Then by the properties of v we see that A_v is a valuation ring and $\mathfrak{m}_v$ is a maximal ideal. We call A_v the **valuation ring** of v, $\mathfrak{m}_v$ the **valuation ideal** of v, and κ_v the **residue field** of v. Conversely, if A is a valuation ring of K, then the set $\Gamma = \{xA : x \in K^\times\}$ is a group with operation defined by $xA \cdot yA = xyA$. Moreover, if we define an order $\leq$ on Γ by

$$xA \leq yA \iff yA \subseteq xA \iff y/x \in A$$

then Γ becomes a totally ordered group with $\leq$ (since A is a valuation ring), and we obtain an additive valuation of K with value group Γ by setting $v(x) = xA$ and $v(0) = \infty$. It is easy to see the valuation ring of v is A.

The additive valuation corresponding to a valuation ring A is not quite unique, so we introduce the following notation. Two valuations v and w on a field K with value groups Γ_v and Γ_w are called equivalent if and only if there exists an order-isomorphism $\varphi : \Gamma_v \to \Gamma_w$ such that $w = \varphi \circ v$.

Theorem 14.2.4. *Let K be a field. Then valuation rings of K are in one-to-one correspondence to equivalent class of valuations on K.*

Proof. One direction is clear: If two valuations are equivalent, then they determine the same valuation ring. For the converse, assume that v and w are valuations on K with value groups Γ_v and Γ_w such that $A_v = A_w$. We define the homomorphism $\varphi : \Gamma_v \to \Gamma_w$ by

$$\varphi(v(x)) = w(x) \quad \text{for} \quad x \in K^\times.$$

Since $U(A_v) = U(A_w)$, it is easy to see φ is well defined and injective. Clearly φ satisfies the condition $w = \varphi \circ v$ and is surjective. Now, for $x, y \in K^\times$ we have

$$\varphi(v(x) + v(y)) = \varphi(v(xy)) = w(xy) = w(x) + w(y),$$

and

$$v(x) > 0 \iff x \in A_v = A_w \iff w(x) = \varphi(v(x)) > 0.$$

Thus φ is an order-isomorphism from Γ_v to Γ_w and v and w are equivalent. □

In view of this proposition, we think of valuation rings and additive valuations as being two aspects of the same thing, and we may assume that all valuations are *surjective*. In this part, we use this point of view to establish some results for valuation rings.

The first non-trivial examples of valuations are the ***p*-adic valuation** v_p on $\mathbb{Q}$ where p is a prime number, and similarly the p-adic valuation v_p on the rational function field $k(X)$ where p is any irreducible polynomial from $k[X]$, k being an arbitrary field. In the second case, v_p restricted to k is trivial.

There is one more interesting valuation on $k[X]$, trivial on k. This is the degree valuation v_∞ defined for non-zero polynomials $f, g \in k[X]$ by

$$v_\infty(f/g) = \deg g - \deg f.$$

One easily checks the axioms of a valuation. Moreover, f/g is a unit in the valuation ring A_{v_∞} if and only if $\deg f = \deg g$. Thus if

$$f = \sum_{i=0}^{n} a_i X^i$$

with $a_i \in k$ and $a_n \neq 0$, then we see that $f(X)/X^n$ is a unit that maps to a_n in the residue class field. Hence it follows that the residue class field is exactly k.

Proposition 14.2.5. *Every non-trivial valuation on $\mathbb{Q}$ is a p-adic valuation for some rational prime p. Every non-trivial valuation on $k(X)$, trivial on k, is either the degree valuation v_∞ or a p-adic valuation for some irreducible polynomial $p \in k[X]$.*

Proof. Let K be either $\mathbb{Q}$ or $k(X)$ and v some non-trivial valuation on K. Then the valuation ring A is different from K. In the second case v is assumed to be trivial on k. This means that $k \subseteq A$.

First consider the case $K = \mathbb{Q}$. Since $1 \in A$, we have $\mathbb{Z} \subseteq A$. As $A \neq \mathbb{Q}$, at least one prime p must lie in $\mathfrak{m}_A$. If q is a prime different from p, we have $ap + bq = 1$ for some $a, b \in \mathbb{Z}$, whence $q \notin \mathfrak{m}_A$. Hence all primes $q \neq p$ are units in A. Using the factorization of integers we therefore see that for $a, b \in \mathbb{Z}$, relatively prime, we have $a/b \in A$ iff $p \nmid b$, whence $A = \mathbb{Z}_{(p)}$, i.e., v is equivalent to the p-adic valuation v_p.

Let $K = k(X)$ and $\mathbb{Z} \subseteq A \neq K$. If $X \in A$, then $k[X] \subseteq O$ and we can argue as in the case of $\mathbb{Q}$ replacing $\mathbb{Z}$ by $k[X]$. If $X \notin A$, then $X^{-1} \in \mathfrak{m}_A$. In this case $v(X) < 0$ and $v(X^m) < v(X^n)$ whenever $0 < n < m$. Since $v(a) = 0$ for every $a \in k^\times$, we get

$$v(a_n X^n + \cdots + a_1 X + a_0) = v(a_n X^n) = nv(X)$$

in the case $a_n \neq 0$. Hence the value group of v is $v(X)\mathbb{Z}$. By sending $v(X)$ to -1, we therefore get an order-preserving isomorphism with $\mathbb{Z}$, showing that v is equivalent to the degree valuation. □

Definition 14.2.6. *A subset Δ of a totally ordered group Γ is called a **segment** if Δ is non-empty and if for any element α of Γ which belongs to Δ, all the elements β of Γ which lie between α and $-\alpha$ also belong to Δ. A subgroup of Γ is called an **isolated subgroup** if it is a segment of Γ.*

Isolated subgroups occurs naturally in the theory of totally ordered groups due to the following proposition.

Proposition 14.2.7. *A subgroup Δ of Γ is isolated if and only if it is the kernel of an order homomorphism from Γ to a totally ordered group.*

Proof. Let $\phi : \Gamma \to \Gamma'$ be an order-homomorphism between to tally ordered groups and $\Delta = \ker \phi$. we show that Δ is isolated. In fact, if $\alpha \in \Delta$ and β lie between α and $-\alpha$, then since $\phi(\alpha) = \varphi(-\alpha)$, we must have $0 \leq \phi(\beta) \leq 0$, whence $\beta \in \Delta$.

Conversely, let Δ be a isolated subgroup of Γ and Γ/Δ be the quotient group. We define an order on Γ/Δ by

$$\alpha + \Delta \leq \beta + \Delta \iff \alpha \leq \beta.$$

This definition makes sense since for $\alpha > 0$ and $\alpha \notin \Delta$ we have $\alpha > \beta$ for all $y \in \Delta$. It is easy to see Γ/Δ becoms a tally ordered group and the quotient map $\pi : \Gamma \to \Gamma/\Delta$ is an order homomorphism with kernel Δ. □

Note that the set of segements of a tally ordered group Γ is totally ordered by inclusion. Therefore, we defined the **rank** of Γ, denoted by rank(Γ), to be the maximal length of ascending chains in this set (just like the definition of the Krull dimension of a ring). The **rank of a valuation** is defined to be the rank of the corresponding value group.

Using the valuation map, there is a connection between idelas of a valuation ring and isolated subgroups of its value group, which we now explain.

Theorem 14.2.8. *Let $v : K^\times \to \Gamma$ be a valuation and A be its valuation ring. For any subset $S \subseteq A$, we define*

$$\Delta_S = \{\alpha \in \Gamma : \alpha \notin v(S) \text{ and } \alpha \notin -v(S)\}.$$

(a) If I is an ideal of A then Δ_I is a segement in Γ, and is an isolated subgroup if and only if I is prime.

(b) The map $I \mapsto \Delta_I$ is an order-reversing bijection from the set of all ideals of A onto the set of all segments of Γ.

Proof. Let I be an ideal of A. To show Δ_I is a segement, we only need to verify that, if $\alpha \notin \Delta_I$ and $\beta > \alpha > 0$, then $\beta \notin \Delta_I$. Now by definition, if $\alpha \notin \Delta_I$ and $\alpha > 0$, then $\alpha \in v(I)$. Since $\beta > \alpha$, we have $\beta - \alpha \in v(A)$, and hence $\beta = \alpha + \beta - \alpha \in v(A)v(I) \subseteq v(I)$. Furthermore, from the definition of Δ_I, it is easy to see Δ_I is a subgroup if and only if I is prime. For (b), we construct an inverse of the map $I \mapsto \Delta_I$. Let Δ be a segment in Γ, and define

$$I_\Delta = \{a \in A : v(a) > \alpha \text{ for all } \alpha \in \Delta\}.$$

It is easy to see I_Δ is an ideal of A, and we have $\Delta_{I_\Delta} = \Delta$, $I_{\Delta_I} = I$, so the claim is proved. □

Corollary 14.2.9. *The rank of a valuation equals the Krull dimension of its valuation ring.*

14.2.1 Valuations of rank one

As an important example, we consider the condition under which a valuation has rank 1. By Corollary 14.2.9, we know this happens if and only if $\dim A_v = 1$. Here we provides another characterization.

Proposition 14.2.10. *Let v be a nontrivial valuation, Γ be the value group of v, and A the valuation ring. Then the following are equivalent.*

(i) $\operatorname{rank}(v) = 1$, *or equivalently* $\dim A = 1$.

(ii) Γ *is order isomorphic to a subgroup of* $\mathbb{R}$.

(iii) Γ *is* ***Archimedean****, that is, for any* $\alpha, \beta \in \Gamma$ *with* $\alpha > 0$*, there exist* $n \in \mathbb{N}$ *such that* $nx > y$.

Proof. We will show that (iii)⇒(ii)⇒(i)⇒(iii). First, assume that Γ is Archimedean, and we may suppose that $\Gamma \neq \{0\}$. Fix some $0 < \alpha \in \Gamma$. For any $\beta \in \Gamma$, there is a well-defined largest integer n such that $n\alpha \leq \beta$ (if $\beta \geq 0$ this is clear by assumption; if $\beta < 0$, let m be the smallest integer such that $-\beta \leq m\alpha$, and set $n = -m$), which we will denote by n_0. Now set $\beta_1 = \beta - n_0\alpha$ and let n_1 be the largest integer n such that $n\alpha < 10\beta_1$; we have $0 \leq n_1 < 10$. Set $\beta_2 = 10\beta_1 - n_1\alpha$ and let n_2 be the largest integer n such that $n\alpha < 10\beta_2$. Continuing in the same way, we find a sequence of integers $\{n_i\}$ and set $\phi(\beta)$ to be the real number given by the decimal expression $n_0.n_1n_2\ldots$. Then it can easily be checked that $\phi : \Gamma \to \mathbb{R}$ is order-preserving and injective. Now let $\beta, \beta' \in \Gamma$. For $r \in \mathbb{N}$ arbitrary, let n and n' be the interger determined by the inequalities

$$n\alpha \leq 10^r\beta < (n+1)\alpha, \quad n'\alpha \leq 10^r\beta' \leq (n'+1)\alpha.$$

Then we see $(n+n')\alpha \leq 10^r(\beta+\beta') < (n+n'+2)\alpha$. If we use $\phi_r(\beta)$ to denote the number obtained by taking the first r decimal places of $\phi(\beta)$, then $n = \phi_r(\beta)$, $n' = \phi_r(\beta')$, and hence

$$\begin{aligned}|\phi(\beta+\beta') - \phi(\beta) - \phi(\beta')| &= |\phi(\beta+\beta') - \phi_r(\beta+\beta')| + |\phi_r(\beta+\beta') - \phi_r(\beta) - \phi_r(\beta')| \\ &\quad + |\phi_r(\beta) - \phi(\beta)| + |\phi(\beta') - \phi_r(\beta')| \leq 4 \cdot 10^{-r}.\end{aligned}$$

Since r is arbitrary, we see ϕ is a homomorphism, hence Γ is order isomorphic to a subgroup of $\mathbb{R}$.

Now let Γ be a nonzero subgroup of $\mathbb{R}$. Since $\Gamma \neq 0$, A is not a field. Suppose that $\mathfrak{p}$ is a prime ideal of A distinct from $\mathfrak{m}_A$. Let $a \in \mathfrak{m}_A - \mathfrak{p}$ and set $v(a) = \alpha$. Suppose that $0 \neq b \in \mathfrak{p}$, and set $\beta = v(b)$; then $\beta \in \Gamma$ and $\alpha > 0$, so that $n\alpha > y$ for some sufficiently large natural number n. This means $a^n/b \in A$, so that $a^n \in bA \subseteq \mathfrak{p}$; then since $\mathfrak{p}$ is prime we have $a \in \mathfrak{p}$, which is a contradiction. Thus $\mathfrak{p} = (0)$ and the only prime ideals in A are (0) and $\mathfrak{m}_A$. That is, $\dim A = 1$.

Finally, assume that $\dim A = 1$. If $0 \neq b \in \mathfrak{m}_A$ then $\mathfrak{m}_A$ is the unique prime ideal containing b, and hence $\sqrt{bA} = \mathfrak{m}_A$. Thus for any $a \in \mathfrak{m}_R$ there exists a natural number n such that $a^n \in bA$. From this one sees easily that Γ satisfies the Archimedean axiom. □

Proposition 14.2.11. *Let* K *be a field,* v *a nontrivial valuation on* K *and* A *the ring of* v*. For* A *to be completely integrally closed, it is necessary and sufficient that* v *be of rank* 1.

Proof. Suppose v is of rank 1. Let $x \in K$ be such that the $A[x]$ are all contained in a finitely generated sub-A-module of K. There exists $d \in A - \{0\}$ such that $dx^n \in A$ for all $n \geq 0$. Then $v(d) + nv(x) \geq 0$, that is $n(-v(x)) \leq v(d)$ for all $n \geq 0$, whence $-v(x) \leq 0$ (since Γ_v is Archimedean) and $x \in A$. Thus A is completely integrally closed.

Suppose now that v is not of rank 1. Then there exist $y \in \mathfrak{m}_v$ and $t \in A$ such that $nv(y) < v(t)$ for all $n \geq 0$. Then $ty^{-n} \in A$ for all $n \geq 0$, but $y^{-1} \notin A$. Hence A is not completely integrally closed. □

Corollary 14.2.12. *Let* K *be a field,* $(v_i)_{i\in I}$ *a family of valuations of rank* 1 *on* K *and* A *the intersection of the rings of the* v_i*. Then* A *is a completely integrally closed domain.*

Proof. An intersection of completely integrally closed rings is completely integrally closed, hence the claim. □

14.2.2 Discrete valuation rings

A valuation ring whose value group is isomorphic to $\mathbb{Z}$ is called a **discrete valuation ring** (DVR). Discrete refers to the fact that the value group is a discrete subgroup of $\mathbb{R}$.

Example 14.2.13. The two standard examples are:

(a) $K = \mathbb{Q}$. Take a fixed prime p, then any non zero $x \in \mathbb{Q}$ can be written uniquely in the form $p^a y$, where $a \in \mathbb{Z}$ and both numerator and denominator of y are prime to p. Define $v_p(x)$ to be a. The valuation ring of v_p is the local ring $\mathbb{Z}_{(p)}$.

(b) $K = k(X)$, where k is a field and X an indeterminate. Take a fixed irreducible polynomial $f \in k[X]$ and define v_f just as in (a). The valuation ring of v_f is then the local ring $k[X]_{(f)}$.

(c) Let k be a field, and let $k((X))$ be the field of formal Laurent series in one variable over k. For every non-zero series

$$f(X) = \sum_{n \geq n_0} a_n X^n, \quad a_{n_0} \neq 0$$

one defines the order $v(f)$ of f to be the integer n_0. One obtains thereby a discrete valuation of $k((X))$, whose valuation ring is $k[\![X]\!]$, the set of formal series; its residue field is k.

Proposition 14.2.14. *Let A be a valuation ring. Then the following conditions are equivalent.*

(a) A is a DVR.

(b) A is a PID.

(c) A is Noetherian.

(d) The value group Γ of A is discrete under order topology and has rank 1.

Proof. Let K be the field of fractions of A and $\mathfrak{m}$ its maximal ideal. Since A is a valuation ring, we know finitely generated idels of A are principal, so A is a PID if and only if it is Noetherian. Now, we first show that if A_v is Noetherian then v must has rank 1. For suppose that $\operatorname{rank}(v) > 1$, there must exists a nontrivial isolated subgroup Δ. Fix a positive element $x \in \Delta$, then we get a chain of elements

$$x < 2x < \cdots < nx < \cdots .$$

Since Δ is proper, we can find $y \in G$ which does not belong to Δ. Then since Δ is isolated, y is bigger than any elements in Δ, and in particular bigger than any nx, $n \in \mathbb{N}$. Equivalently, we get a decreasing sequence of positive elements in G:

$$y - x > y - 2x > \cdots > y - nx > \cdots > 0$$

which gives an infinite strictly descending segements in G, hence an infinite ascending sequence of ideals in A_v (by Theorem 14.2.8). Hence R_v is not Noetherian.

Now since v has rank 1, G can be identified as a subgroup of $\mathbb{R}$. Moreover, the maximal ideal $\mathfrak{m}$ is principal, which means G has a smallest positive element. Then we see G is discrete and hence isomorphic to $\mathbb{Z}$. The converse is obvious, since the group $\mathbb{Z}$ has no infinite descending sequence of positive elements.

Finally, it is clear that $\mathbb{Z}$ is discrete and has rank 1. Conversely, if the value group G of A has rank 1 then it can be embedded into $\mathbb{R}$, and is isomorphic to $\mathbb{Z}$ if it is discrete. This completes the proof. □

If A is a DVR with maximal ideal $\mathfrak{m}$ then an element $t \in R$ such that $\mathfrak{m} = (t)$ is called a **uniformising element** (or **prime element**) of A.

Example 14.2.15. A valuation ring B whose maximal ideal $\mathfrak{m}_B$ is principal does not have to be a DVR. In fact, the maximal ideal of a valuation ring is principal if and only if its value group G has a smallest positive element, if and only if G is discrete under order topology.

To obtain a counter-example, let K be a field, and A a DVR of K. If $\bar{B}$ is a DVR for the residue field $k = A/\mathfrak{m}_A$, then their composite B will be a valuation ring of K with rank bigger than 2, hence not a DVR. However, let $s \in B$ be a preimage of a uniformising element $\bar{s}$ of $\bar{B}$. Then $s \notin \mathfrak{m}_A$ and we have

$$\mathfrak{m}_A \subseteq \mathfrak{m}_B \subseteq B \subseteq A, \quad \mathfrak{m}_B/\mathfrak{m}_A = \bar{s}\bar{B},$$

so $\mathfrak{m}_B = \mathfrak{m}_A + sB$. On the other hand, since $s \in A - \mathfrak{m}_A$, we have $s^{-1} \in A$ and thus $s^{-1}\mathfrak{m}_A \subseteq A \subseteq B$. This implies $\mathfrak{m}_A \subseteq sB$, so $\mathfrak{m}_B = sB$.

The previous theorem gives a characterisation of DVRs among valuation rings; now we consider characterisations among all rings.

Proposition 14.2.16. *Let A be a ring with fraction field K. Then the following conditions are equivalent:*

(a) A is a DVR.

(b) A is a local PID, and not a field.

(c) A is a Noetherian local ring with positive dimension and the maximal ideal $\mathfrak{m}_A$ is principal.

(d) A is a one-dimensional normal Noetherian local ring.

Proof. If A is a DVR, conditions (b), (c), (d) hold by Proposition 14.2.14, Proposition 14.1.3 and Proposition 13.1.38. Conversely, we now show that either one of these three conditions implies A is a DVR.

If A is a local PID and not a field, then A is Noetherian and the maximal ideal $\mathfrak{m}$ is nonzero and principal, so (b) implies (c). Now assume (c), and let $\mathfrak{m} = (t)$ be the maximal ideal of A. Then t can not by nilpotent since otherwise $\mathfrak{m}$ is the unique prime ideal of A, whence $\dim A = 0$. By the Krull intersection theorem we have $\bigcap_{n=1}^{\infty}(t^n) = (0)$, so that for $0 \neq x \in A$ there is a well-determined n such that $x \in (t^n)$ but $x \notin (t^{n+1})$. If $x = t^n u$, then since $u \notin (t)$ it must be a unit. Similarly, for $0 \neq y \in A$ we have $y = t^m v$, with v a unit. Therefore $yz = t^{m+n}uv \neq 0$, and so A is an integral domain. Finally, any element α of K can be written $\alpha = x^v u$, with u a unit of A and $v \in \mathbb{Z}$, and it is easy to see that setting $v(t) = v$ defines an additive valuation of K whose valuation ring is A.

Finally, assume that A is a one-dimensional noraml Noetherian local ring. Let x be a nonzero element of $\mathfrak{m}$. By hypothesis, $\mathfrak{m}$ is the only nonzero prime ideal, so $\sqrt{(x)} = \mathfrak{m}$. Then by Proposition 6.2.3 (x) contains a power of $\mathfrak{m}$, and we may assume that $(x) \neq \mathfrak{m}$. Then there exists $n > 1$ such that $\mathfrak{m}^n \subseteq (x)$ but $\mathfrak{m}^{n-1} \nsubseteq (x)$. If $y \in \mathfrak{m}^{n-1} - (x)$ and $\beta = x/y \in K$, then we have $\beta^{-1} = y/x \notin A$ since $y \notin (x)$. Since A is integrally closed, β^{-1} is not integral over A. But then $\beta^{-1}\mathfrak{m} \nsubseteq \mathfrak{m}$, in view of Proposition 7.1.1. Now use $y \in \mathfrak{m}^{n-1}$ we have

$$\beta^{-1}\mathfrak{m} = (y/x)\mathfrak{m} \subseteq (1/x)\mathfrak{m}^n \subseteq (1/x)(x) = A.$$

Thus $\beta^{-1}\mathfrak{m}$ is an ideal of A, and it must be A since $\beta^{-1}\mathfrak{m} \nsubseteq \mathfrak{m}$. Hence $\mathfrak{m}$ is the principal ideal (β), and by the preceeding argument we can show that A is a DVR. □

To conclude this part, we introduce the concept of rational rank of a totally ordered group Γ, denoted by $\mathrm{rank}_{\mathbb{Q}}(\Gamma)$, which is defined to be the maximal number of rationally independent elements of Γ. In other words,

$$\mathrm{rank}_{\mathbb{Q}}(\Gamma) := \dim_{\mathbb{Q}}(\mathbb{Q} \otimes_{\mathbb{Z}} \Gamma).$$

Note that the rational rank of a group Γ is zero if and only if Γ is a torsion group. If Γ is a value group of a valuation, Γ is totally ordered, then its rational rank is zero if and only if $\Gamma = \{0\}$, i.e. if and only if the valuation is the trivial valuation.

Proposition 14.2.17. *Let Γ be an abelian group and Δ a subgroup of Γ. Then*

(a) $\mathrm{rank}_{\mathbb{Q}}(\Gamma) = \mathrm{rank}_{\mathbb{Q}}(\Gamma/\Delta) + \mathrm{rank}_{\mathbb{Q}}(\Delta)$.

(b) If Γ is ordered then $\mathrm{rank}(\Gamma) = \mathrm{rank}(\Gamma/\Delta) + \mathrm{rank}(\Delta)$.

(c) If Γ is ordered then $\mathrm{rank}(\Gamma) \leq \mathrm{rank}_{\mathbb{Q}}(\Gamma)$.

Proof. Since $\mathbb{Q}$ is $\mathbb{Z}$-flat (it is torsion free), we see that

$$(\mathbb{Q} \otimes_{\mathbb{Z}} \Gamma)/(Q \otimes_{\mathbb{Z}} \Delta) = \mathbb{Q} \otimes_{\mathbb{Z}} (\Gamma/\Delta)$$

whence the first equality follows. Now it is easy to see the isolated groups in Γ/Δ are in one-to-one correspondence to isolated subgroups in Γ containing Δ, so the second equality follows. Finally, assume that Γ is ordered and let $\Delta_0 \leq \Delta_1 \leq \cdots \leq \Delta_{s-1}$ be a stirct chain of isolated subgroups of Γ. For each i, choose an element $\alpha_i \in \Delta_i \setminus \Delta_{i-1}$ (with $\Delta_s = \Gamma$), then we see $\alpha_1, \ldots, \alpha_r$ are rationally independent: let $\sum_{i=1}^t r_i\alpha_i = 0$ with $r_t \neq 0$ and $t \leq s$, then $r_t\alpha_t \in \Delta_{t-1}$, and since Δ_{r-1} is a segment and $r_t \neq 0$, we find $\alpha_t \in \Gamma_{t-1}$, contradiction. Thus $\mathrm{rank}(\Gamma) \leq \mathrm{rank}_{\mathbb{Q}}(\Gamma)$. □

14.3 Compare valuation rings of a field

As an immediate observation, if $\mathfrak{p}$ is a prime ideal of A, then the localized ring $A_{\mathfrak{p}}$ is a local ring containing A. Therefore, $A_{\mathfrak{p}}$ is also a valuation of K. We have seen in Theorem 14.2.8 that such a prime ideal $\mathfrak{p}$ corresponds to a proper isolated subgroup Δ of G. Now we determine the value group of $A_{\mathfrak{p}}$.

Proposition 14.3.1. *The value group of $A_\mathfrak{p}$ is isomorphic to the quotient group Γ/Δ, where Δ is the isolated subgroup of Γ corresponds to $\mathfrak{p}$. In this way the valuation $v_\mathfrak{p}$ associated to $A_\mathfrak{p}$ is given by the composition of $v : K^\times \to \Gamma$ and $\pi : \Gamma \to \Gamma/\Delta$.*

Proof. We define $\tilde{v} = \pi \circ v : K^\times \to \Gamma/\Delta$, which is easily seen to be a valuation of K. If we embedd $A_\mathfrak{p}$ in K, then we have $v(A_\mathfrak{p}) = \Delta \cup \Gamma_+$. On the other hand, we observe that

$$A_{\tilde{v}} = \{x \in K : \pi(v(x)) \geq 0\} = \{x \in K : v(x) > \Delta \text{ or } v(x) \in \Delta\} = A_\mathfrak{p},$$

so the claim follows from Theorem 14.2.4. □

With Proposition 14.3.1, we can now classifies all valuation rings of K containing A: they are in one-to-one correspondence to prime ideals of A.

Proposition 14.3.2. *Let A be a valuation ring and $\mathfrak{m}_A$ be the maximal ideal of A.*

(a) Any localization $A_\mathfrak{p}$ of A at a prime ideal $\mathfrak{p}$ of A is a valuation ring of K containing A, and $\mathfrak{p}$ is the maximal ideal of $A_\mathfrak{p}$.

(b) The mapping $\mathfrak{p} \mapsto A_\mathfrak{p}$ is a bijection from the set of prime ideals of A onto the set of rings B with $A \subseteq B \subseteq K$, which is orderreversing for the relation of inclusion. The inverse map is defined by $B \mapsto \mathfrak{m}_B$.

Proof. We have already seen that $A_\mathfrak{p}$ is a valuation ring containing A. Now, from the definition of the valuation ideal and Proposition 14.3.1, we have

$$\mathfrak{m}_{A_\mathfrak{p}} = \{x \in K : v_\mathfrak{p}(x) > 0\} = \{x \in K : \pi(v(x)) > 0\} = \{x \in K : v(x) > \Delta\} = \mathfrak{p}.$$

Therefore $\mathfrak{p}$ is the maximal ideal of $A_\mathfrak{p}$.

Now let B be a ring such that $A \subseteq B \subseteq K$. Note that if $x \in \mathfrak{m}_B$ then $x^{-1} \notin B \supseteq A$, and hence $x \in \mathfrak{m}_A$. This implies $\mathfrak{m}_B \subseteq \mathfrak{m}_A \subseteq A \subseteq B$. Also, note that by (a), $\mathfrak{m}_B$ is the maximal ideal of both $A_{\mathfrak{m}_B}$ and B. Since a valuation ring is uniquely determined by its maximal ideal, we get $B = A_{\mathfrak{m}_B}$, hence the claim. □

Since $A_\mathfrak{p}$ is a valuation ring and $\mathfrak{p}$ is its maximal ideal, we can consider its residue field $\kappa_\mathfrak{p} = A_\mathfrak{p}/\mathfrak{p}$. Then since A is a valuation ring, it is easy to see $\bar{A} = A/\mathfrak{p}$ is a valuation ring of $\kappa_\mathfrak{p}$. Moreover, we can determine the value group of $\bar{A}$.

Proposition 14.3.3. *Let $\mathfrak{p}$ be a prime ideal of A with corresponding isolated subgroup Δ. Then $\bar{A}$ is a valuation ring of κ_v with value group Δ.*

Proof. Let $\pi : A_\mathfrak{p} \to A_\mathfrak{p}/\mathfrak{p}$ be the quotient map. Then since $A/\mathfrak{p}$ is local with maximal ideal $\mathfrak{m}_A/\mathfrak{p}$, we see $U(A/\mathfrak{p}) = \pi(U(A))$, hence there is an isomorphism ψ given by

$$\psi : U(A_\mathfrak{p})/U(A) \to U(A_\mathfrak{p}/\mathfrak{p})/U(A/\mathfrak{p}), \quad x + U(A) \mapsto \pi(x) + U(A/\mathfrak{p}).$$

Also, we note that $U(A_\mathfrak{p})/U(A) \cong \Delta$, with the isomorphism given by

$$\psi : U(A_\mathfrak{p})/U(A) \to \Delta, \quad x + U(A) \mapsto v(x).$$

With these observations, we now define a valuation on $\kappa_v^\times = U(A_\mathfrak{p}/\mathfrak{p})$ by

$$\bar{v} : U(A_\mathfrak{p}/\mathfrak{p}) \to \Delta, \quad \bar{v}(\pi(x)) = \psi(\phi^{-1}(\pi(x) + U(A/\mathfrak{p}))) = v(x).$$

With this, it is easy to check that

$$A_{\bar{v}} = \{\pi(x) : \bar{v}(\pi(x)) \geq 0\} = \{\pi(x) : v(x) \geq 0\} = A/\mathfrak{p}.$$

Thus the claim follows. □

It turns out that all valuation rings contained in a given valuation ring arise in this way: we have the following proposition.

Proposition 14.3.4. *Let A be a valuation ring of K and $\pi : A \to A/\mathfrak{m}_A$ be the canonical map.*

(a) Let $B \subseteq A$ be a valuation ring of K, then the image $\bar{B}$ under π_A is a valuation ring of κ_v.

(b) Let $\bar{B}$ be a valuation ring of κ_v, then its preimage $B \subseteq A$ under π_A is a valuation ring of K.

Proof. Let $B \subseteq A$ be a valuation ring of K and $\pi(x) \in \kappa_v - \bar{B}$. Then $x \notin B$, and hence $x^{-1} \in B$. Since $\pi(x^{-1}) = \pi(x)^{-1}$, we see $\pi(x)^{-1} \in \bar{B}$, hence $\bar{B}$ is a valuation ring of κ_v.

Conversely, let $\bar{B}$ be a valuation ring of K and B be its preimage under π. Let $x \in K - B$, then $\pi(x) \in \kappa_v - \bar{B}$ and hence $\pi(x^{-1}) \in \bar{B}$. Then it follows that $x^{-1} \in B$ so B is a valuation of K. □

The formulation of Proposition 14.3.4 can be defined on valuations as follows. Let $v : K^\times \to \Gamma$ be a valuation of K with residue field κ_v, and let $\bar{v} : \kappa_v \to \bar{\Gamma}$ be a valuation of κ_v. Then we can define a new valuation w of K by letting its valuation ring to be

$$A_w = \{a \in A : \bar{v}(\bar{a}) \geq 0\}.$$

The valuation w is called the composite of v and $\bar{v}$, and denoted by $w = v \circ \bar{v}$.

Let v and w be two valuations of K. We say w dominates v, or $w \geq v$, if $A_w \subseteq A_v$ or equivalently $\mathfrak{m}_w \supseteq \mathfrak{m}_v$. Then Proposition 14.3.4 just says all valuations $w \geq v$ are composite of v. By Proposition 14.3.1 and Proposition 14.3.3, the following result is immediate.

Proposition 14.3.5. *If w is the composite valuation $v \circ \bar{v}$ we have the equalities*

$$\operatorname{rank}(w) = \operatorname{rank}(v) + \operatorname{rank}(\bar{v}), \quad \operatorname{rank}_\mathbb{Q}(w) = \operatorname{rank}_\mathbb{Q}(v) + \operatorname{rank}_\mathbb{Q}(\bar{v}).$$

In fact, by Proposition 14.3.1 and Proposition 14.3.3, if we have the valuations v of K and $\bar{v}$ of κ_v, then the composite valuation $w = v \circ \bar{v}$ defines an extension of the value group Γ of v by the value group $\bar{\Gamma}$ of $\bar{v}$, i.e. an exact sequence of totally ordered groups:

$$0 \longrightarrow \bar{\Gamma} \longrightarrow \widetilde{\Gamma} \longrightarrow \Gamma \longrightarrow 0$$

If this exact sequence splits, the value group $\widetilde{\Gamma}$ is isomorphic to the group $\Gamma \times \bar{\Gamma}$ with the lexicographic order. If the valuation v is a discrete valuation of rank one, i.e. for $\Gamma = \mathbb{Z}$, the exact sequence always splits (this follows from the observation that $\mathbb{Z}$ can be embedded into any nonzero totally ordered group) and we can describe the composite valuation $w = v \circ \bar{v}$ in the

following way. The maximal ideal of the valuation ring A_v associated to v is generated by an element t and we can associate to any non zero element x in K the nonzero element $\pi(xt^{-v(x)})$ in the residue field, where $\pi : A_v \to \kappa_v$ is the canonical map. The composite valuation w is then defined by $w(x) = (v(x), \bar{v}(\pi(xt^{-v(x)}))$.

14.4 Dependent valuations and induced topology

With the notation of composite, we say two valuations v, w of K are **dependent** if they are the composite of a common nontrivial valuation. If these do not hold, we say v and w are **independent**. Equivalently, by Proposition 14.3.4 v and w are independent if and only if the valuation rings A_v and A_w are not contained in a proper valuation ring of K, if and only if AB, the smallest ring containing A and B, is a proper subring of K.

we see from Proposition 14.3.2 that the dependence relation is an equivalence relation. Indeed, if A and B are dependent and also B and C are dependent, then AB and BC are both overrings of B. Thus there is some inclusion, say $AB \subseteq BC$. But then A and B are both contained in BC. Hence they are dependent. We shall now study the topology induced by a valuation on a field K. Let $v : K^\times \to \Gamma$ be a valuation of K. For each $\gamma \in \Gamma$ and each $x \in K$ we define the set

$$U_\gamma(x) = \{y \in K : v(y - x) > \gamma\}.$$

These sets form a basis of open neighborhoods of x, due to the following observations:

- $x \in U_\gamma(x)$,
- If $y \in U_\gamma(x) \cap U_{\gamma'}(x')$ and $\delta > \max\{\gamma, \gamma'\}$, then for $z \in U_\delta(y)$, we have

$$v(z - x) = v(z - y + y - x) > \gamma, \quad v(z - x') = v(z - y + y - x') > \gamma'$$

  whence $U_\delta(y) \subseteq U_\gamma(x) \cap U_{\gamma'}(x')$.

Therefore, the sets $\{U_\gamma(x) : x \in K, \gamma \in \Gamma\}$ is a basis for a topology $\mathcal{T}_v$ on K, called the **topology induced by the valuation** v. Some properties of the topology $\mathcal{T}_v$ are gathered below.

Proposition 14.4.1. *Let v be a valuation on K and $\mathcal{T}_v$ the topology induced by v.*

(a) The topology $\mathcal{T}_v$ is Hausdorff and totally disconnected, and it is discrete if and only if v is trivial.

(b) The field operations are continuous with respect to $\mathcal{T}_v$.

(c) The valuation $v : K^\times \to \Gamma$ is continuous if Γ is given the discrete topology.

(d) The quotient topology induced on the residue field κ_v is discrete.

Proof. Let A be the valuation ring of v. Let $x, y \in K$ and $x \neq y$. If $\gamma = v(x - y)$, then $\gamma \neq \infty$ and we see $U_\gamma(x) \cap U_\delta(y) = \varnothing$ if $\gamma, \delta > v(x - y)$. Therefore $\mathcal{T}_v$ is Hausdorff. Also, it is easy to see $\mathcal{T}_v$ is discrete if and only if v is trivial. We next claim that the set $U_\gamma^c(x) = \{y \in K : v(y - x) \leq \gamma\}$ is also open in K. To prove this, we first observe that, if $v(z - y) > v(y - x)$ then we have $(z - y)/(y - x) \in \mathfrak{m}_A$, whence $1 + (z - y)/(y - x) = (z - x)/(y - x)$ is a unit in A. That is, we have

$$v(z - y) > v(y - x) \Rightarrow v(z - x) = v(y - x).$$

From this, it follows that $U_{v(y-x)} \subseteq U_\gamma(x)^c$ if $y \in U_\gamma(x)^c$, so $U_\gamma(x)^c$ is open. Since $U_\gamma(x)$ is a basis for $\mathcal{T}_v$, it follows that $\mathcal{T}_v$ is totally disconnected.

Since $v(x+y) \geq \min\{v(x), v(y)\}$, we have $U_\gamma(x) + U_\gamma(y) \subseteq U_\gamma(x+y)$. Moreover, from

$$ab - xy = (a-x)(b-y) + (a-x)y + (b-y)x$$

it follows that $U_\gamma(x)U_\gamma(y) \subseteq U_\delta(xy)$, where $\delta = \min\{2\gamma, \gamma + v(x), \gamma + v(y)\}$. These shows addition and multiplication are continuous under $\mathcal{T}_v$.

Let $x_0 \in K^\times$, if $x \in K^\times$ satisfies $v(x - x_0) > \max\{\gamma + 2v(x_0), v(x_0)\}$, then we have $v(x) = v(x_0)$ and

$$\begin{aligned} v(x^{-1} - x_0^{-1}) &= v(x^{-1}(x_0 - x)x_0^{-1}) = v(x_0 - x) - v(x) - v(x_0) \\ &> \gamma + 2v(x_0) - 2v(x_0) = \gamma \end{aligned} \tag{4.0.1}$$

hence the inverse map is also continuous. These proves (b). Also, the single condition $v(x - x_0) > v(x_0)$ implies $v(x) = v(x_0)$, hence the map $v : K^\times \to G$ is continuous if G is given the discrete topology. Finally, note that $\mathfrak{m}_v = U_0(0)$ is clopen in A and so the quotient topology is discrete. □

Theorem 14.4.2. *Two nontrivial valuations v and w of K are dependent if and only if they induce the same topology on K.*

Proof. Since two dependent valuation rings have a common non-trivial coarsening, to show that they induce the same topology it is enough to consider the particular case $A_v \subseteq A_w$.

Let $v : K^\times \to \Gamma$ be the valuation. Since $A_v \subseteq A_w$, by Proposition 14.3.2 there exists a isolated subgroup Δ of Γ such that w is given by $K^\times \to \Gamma \to \Gamma/\Delta$. Since w is nontrivial, $A_w \neq K$ and $\Delta \neq \Gamma$. Write

$$U_\gamma(0) = \{x \in K : v(x) > \gamma\}, \quad U_{\gamma+\Delta}(0) = \{x \in K : w(x) > \gamma + \Delta\},$$

then we see $U_{\gamma+\Delta}(0) \subseteq U_\gamma(0)$. On the other hand, if $v(x) > 2\gamma$ with $0 < \gamma \notin \Delta$ then $2\gamma > \gamma + \Delta$, hence $U_{2\gamma}(0) \subseteq U_{\gamma+\Delta}(0)$, whence v and w induces the same topology on K.

Conversely, let $\mathfrak{m}_v$ and $\mathfrak{m}_w$ be the valuation ideals of v and w. If v and w induce the same topology on K, then w is an open neighbourhood of 0 in $\mathcal{T}_v$, so there exists $a \in K^\times$ such that $a\mathfrak{m}_v \subseteq \mathfrak{m}_w$. As $\mathfrak{m}_w$ is the maximal ideal of the valuation ring A_w, the set $K - \mathfrak{m}_w$ is multiplicatively closed. Thus we can form the ring

$$A = \{x/y \in K : x \in A_v, y \in A_v - \mathfrak{m}_w\} = \{x/y \in K : v(x) \geq 0, v(y) \geq 0, w(y) \leq 0\}.$$

Since $A_v \subseteq A$, A is also a valuation ring. Moreover, A contins A_w since if $x \in A_w - A_v$ then $w(x) \geq 0$ and we have $x = 1/x^{-1} \in A$. Finally, $A \neq K$: let $z \in A_v \setminus \{0\}$, then $\frac{1}{az} \notin A$ since otherwise $1/(az) = x/y$ with $x \in A_v$ and $y \in A_v - \mathfrak{m}_w$, and we have $y = azx \in a\mathfrak{m}_v \subseteq \mathfrak{m}_w$, a contradiction. Hence v and w are dependent. □

Theorem 14.4.2 is another way to see that the dependence relation among the valuation rings of a field K is an equivalence relation, as we already saw above. Let A be a non-trivial valuation ring of K and take the dependence class $[A]$ of all non-trivial valuation rings of K dependent on A. Clearly $[A]$ is an upwardly directed set with respect to the partial order of inclusion.

Proposition 14.4.3. *Let A be any non-trivial valuation ring of K. Then we have the following case distinction:*

(a) $[A]$ *has a maximal valuation ring B_0 which is a maximal non-trivial overring of A; moreover B_0 has dimension* 1 *and its maximal ideal is the intersection of all non-zero prime ideals of A, or*

(b) there is no maximal non-trivial overring of A. Then the maximal ideals $\mathfrak{m}_B$ of valuation rings $B \in [A]$ form a neighborhood system of 0 *for the topology induced by A. In this case the set of all non-zero prime ideals of A is also a neighborhood system of* 0.

Proof. If $[A]$ has a maximal element B_0, then it is clear that B_0 contains A and is the maximal overring of A. Thus the first part follows from Proposition 14.3.2. Now assume that $[A]$ has no maximal element. Suppose we are given a positive $\delta \in \Gamma$. We seek a valuation ring $B \supseteq A$ such that $B \neq K$ and whose maximal ideal $\mathfrak{m}_B$ satisfies $\mathfrak{m}_B \subseteq U_\delta(0)$. Let Δ be the convex hull of the subgroup generated by δ in Γ, i.e.,

$$\Delta = \{\gamma \in \Gamma : \gamma, -\gamma < n\delta \text{ for some } n \in \mathbb{N}\}.$$

Then Δ defines a valuation ring $B \supseteq A$ with $\mathfrak{m}_B \subseteq U_\delta(0)$. It remains to show that $B \neq K$.

If $B = K$, then $\Delta = \Gamma$ and thus δ is an element of Γ such that Γ is the convex hull of $\delta\mathbb{Z}$. Let Δ^* be the largest isolated subgroup of Γ not containing δ. Then $\Gamma^* = \Gamma/\Delta^*$ is archimedean ordered and thus the overring A^* of A corresponding to Δ^* is maximal according to Proposition 14.3.2. This contradicts our assumption. □

We are now in a position to prove an approximation theorem for independent valuations. For this we need some preparations.

Lemma 14.4.4. *Let $v_1, \dots, v_n$ be valuations on the field K and $x \in K^\times$. Then there exists a polynomial $f(X)$ of the form*

$$f(X) = 1 + n_1 X + \cdots + n_{k-1} X^{k-1} + X^k, \quad n_i \in \mathbb{Z}, k \geq 2 \tag{4.0.2}$$

such that $f(x) \neq 0$ and $z = f(x)^{-1}$ satisfies

$$\begin{aligned} v_i(z) &= 0 && \text{if } v_i(x) \geq 0, \\ v_i(z) + v_i(x) &> 0 && \text{if } v_i(x) < 0. \end{aligned}$$

Proof. Let I be the set of indices i such that $v_i(x) \geq 0$. For all $i \in I$, let x_i denote the canonical image of x in κ_{A_i}. For all $i \in I$ we construct a polynomial f_i as follows: if there exists a polynomial $g(X)$ of the form (4.0.2) such that $g(\bar{x}_i) = 0$ in κ_{A_i}, we take f_i to be such a polynomial; otherwise we take $f_i = 1$. Then we write $f(X) = 1 + X^2 \prod_{i \in I} f_i(X)$. It is obviously a polynomial of the form (4.0.2). If $i \in I$, then $f(x) \in A_i$ and also $f(\bar{x}_i) \neq 0$ by construction; hence $f(x) \notin \mathfrak{m}_i$, $v_i(f(x)) = 0$ and $v_i(z) = 0$. If $i \notin I$, then $v_i(x) < 0$, whence $v_i(f(x)) = kv_i(x)$ (by Proposition 14.2.3) and

$$v_i(x) + v(z) = (1-k)v_i(x) > 0,$$

so the lemma is proved. □

Proposition 14.4.5. *Let $A_1, \dots, A_n$ be valuation rings of a field K, $B = \bigcap_{i=1}^n A_i$ and $\mathfrak{p}_i = \mathfrak{m}_{A_i} \cap B$. Then $A_i = B_{\mathfrak{p}_i}$ and the fraction field of B is K.*

Proof. Clearly $B_{\mathfrak{p}_i} \subseteq A_i$ since $B \subseteq A_i$ and $B - \mathfrak{p}_i \subseteq A - \mathfrak{m}_i$ is a unit in A_i. Now let x be a nonzero element in A_i. We apply the lemma to x and valuations v_i associated with the A_i. Then $v_i(z) \geq 0$ and $v_i(zx) \geq 0$ for all i, hence $z, zx \in B$. As $v_i(x) \geq 0$ and $v_i(z) = 0$, we see $z \notin \mathfrak{p}_i$. Hence $x = xz/z \in B_{\mathfrak{p}_i}$. The field of fractions of B then contains A_i and hence is K. □

Proposition 14.4.6. *With the hypotheses of Proposition 14.4.5, suppose further that $A_i \not\subseteq A_j$ for $i \neq j$. Then the $\mathfrak{p}_i$'s are distinct maximal ideals of B and every maximal ideal of B is equal to one of the $\mathfrak{p}_i$.*

Proof. If $\mathfrak{p}_i \subseteq \mathfrak{p}_j$ for $i \neq j$ then $A_i = B_{\mathfrak{p}_i} \sup B_{\mathfrak{p}_j} = A_j$, which is a contradiction. Then the claim follows from Corollary 10.1.19. □

Corollary 14.4.7. *Suppose that $A_1, \ldots, A_n$ are incomparable valuation rings. For every family of element $a_1 \in A_1, \ldots, a_n \in A_n$, there exists $x \in B$ such that $x \equiv a_i$ mod $\mathfrak{m}_i$ for each i.*

Proof. Since the $\mathfrak{p}_i$ are maximal ideals of B, $A/\mathfrak{m}_A = B_{\mathfrak{p}_i}/\mathfrak{p}_i B_{\mathfrak{p}_i} = B/\mathfrak{p}_i$ and it may therefore be assumed that $a_i \in B$ for all i. The corollary then follows from the fact that the canonical mapping from B to $\prod_{i=1}^n (B/\mathfrak{p}_i)$ is surjective. □

Corollary 14.4.8. *Suppose that $A_1, \ldots, A_n$ are incomparable valuation rings. There exist element $x_1, \ldots, x_n$ of K such that $v_i(x_i) = 0$ and $v_j(x_i) > 0$ for $j \neq i$.*

Proof. For each index i apply Corollary 14.4.7 to the family (a_i) such that $a_i = 1$ and $a_j = 0$ for $j \neq i$. □

Corollary 14.4.9. *Every valuation ring of K containing B contains one of the A_i.*

Proof. We may confine our attention to the case where A_i's are incomparable. Let A be a valuation ring of K containing B. We write $\mathfrak{p} = \mathfrak{m}_A \cap B$. There exists a maximal ideal $\mathfrak{p}_i$ of B containing $\mathfrak{p}$, whence $A_i = B_{\mathfrak{p}_i} \subseteq B_{\mathfrak{p}} \subseteq A$. □

Now for independent valuations, we have the following approximation theorem.

Theorem 14.4.10 (Approximation Theorem). *Suppose $A_1, \ldots, A_n$ are pairwise independent valuation rings of K. For every i, let $v_i : K^\times \to \Gamma_i$ be the valuation corresponding to A_i. Then for any $a_1, \ldots, a_n \in K$ and $\gamma_1 \in \Gamma_1, \ldots, \gamma_n \in \Gamma_n$, there exists an $x \in K$ with*

$$v_i(x - a_i) > \gamma_i \quad \text{for all } i \in \{1, \ldots, n\}.$$

Proof. Let A_i be the valuation ring of v_i and set $B = \bigcap_{i=1}^n A_i$, $\mathfrak{p}_i = \mathfrak{m}_{A_i} \cap B$. By Proposition 14.4.5 we have $A_i = B_{\mathfrak{p}_i}$ and K is the fraction field of B, so the a_i may be written as $a_i = b_i/s$ with $b_i \in B$ and $s \in B \setminus \{0\}$. If we write $x = y/s$ and $\gamma_i' = \gamma_i + v(s)$, then

$$v_i(x - a_i) = v_i(y - b_i) - v(s) > \gamma_i \iff v_i(y - b_i) > \gamma_i'.$$

This shows that we may assume that $a_i \in B$ for all i; we may also assume that $\gamma_i > 0$ for all i. Define ideals of A_i and B by

$$I_i = \{z \in K : v_i(z) \geq \gamma_i\} \subseteq \mathfrak{m}_i, \quad J_i = I_i \cap B \subseteq \mathfrak{p}_i.$$

For $x \in B$, $v_i(x - a_i) \geq \gamma_i$ is equivalent to $x \equiv a_i \bmod I_i$. We therefore need to show that the canonical homomorphism $B \to \prod_{i=1}^n (B/J_i)$ is surjective, that is, J_i's are pairwise coprime. As the maximal ideals of B are the $\mathfrak{p}_i$, it will suffice for this to show that $J_i \not\subseteq \mathfrak{p}_j$ for $i \neq j$.

Suppose that there exists i, j such that $J_i \subseteq \mathfrak{p}_j$ and $i \neq j$. We shall see shortly that the radical of J_i is a prime ideal $\mathfrak{p}$ of B, so that $\mathfrak{p} \subseteq \mathfrak{p}_j$. Since $\gamma_i > 0$ we also have $J_i \subseteq \mathfrak{p}_i$, so $A_j = B_{\mathfrak{p}_j} \subseteq B_{\mathfrak{p}}$ and similarly $A_i \subseteq B_{\mathfrak{p}}$. Now, as $I_i \neq (0)$ and $I_i = B_{\mathfrak{p}_i} J_i$ (Proposition 10.2.36), $J_i \neq (0)$ whence $\mathfrak{p} \neq (0)$ and $B_{\mathfrak{p}} \neq K$. This contradicts the hypothesis that A_i and A_j are independent.

It remains to show that $\mathfrak{p} = \sqrt{J_i}$ is prime for each i. Suppose that $xy \in \mathfrak{p}$, so that $x^n y^n \in J_i$ for some i. Then, if for example $v(x) \geq v(y)$, we have

$$v(x^{2n}) = 2nv(x) \geq nv(x) + nv(y) = v(x^n y^n) \geq \gamma_i$$

whence $x^{2n} \in J_i$ and $x \in \mathfrak{p}$. This finishes the proof. □

Corollary 14.4.11. *For every family of elements $\gamma_1 \in \Gamma_1, \ldots, \gamma_n \in \Gamma_n$, there exists $x \in K$ such that $v_i(x) = \gamma_i$.*

Proof. We may assume that $A_i \neq K$ for all i. Then, there exists for all i an $a_i \in K$ such that $v_i(a_i) = \gamma_i$, and an $\alpha_i \in \Gamma_i$ such that $\gamma_i < \alpha_i$. We apply Theorem 14.4.10 to these elements a_i there exists a $x \in K$ such that $v_i(x - a_i) > \gamma_i = v_i(a_i)$, whence $v_i(x) = v_i(a_i) = \gamma_i$. □

Here we introduce the concept of absolute values over a field, which has a deep connection with valuations of rank 1. Let K be a field. An **absolute value** on K is a map $|\cdot| : K \to \mathbb{R}$ satisfying the following axioms for all $x, y \in K$,

(a) $|x| > 0$ for all $x \neq 0$ and $|0| = 0$.

(b) $|xy| = |x||y|$.

(c) $|x + y| \leq |x| + |y|$.

The absolute value sending all $x \neq 0$ to 1 is called the **trivial absolute value** on K. Note that by (b) we have $|1| = 1$, $|-x| = |x|$, and $|x^{-1}| = |x|^{-1}$, thus $|\cdot|$ is a group homomorphism from $K^\times$ to $\mathbb{R}^\times$.

Proposition 14.4.12. *The set $\{|n \cdot 1| : n \in \mathbb{Z}\}$ is bounded if and only if $|\cdot|$ satisfies the **ultrametric inequality***

$$|x + y| \leq \max\{|x|, |y|\}$$

for all $x, y \in K$.

Proof. If $|\cdot|$ satisfies the inequality, then by induction, the set $\{|n \cdot 1| : n \in \mathbb{Z}\}$ is bounded by 1. Conversely, let $|n \cdot 1| \leq C$. Then

$$|x + y|^n = |(x + y)^n| \leq \sum_\nu \left| \binom{n}{\nu} x^\nu y^{n-\nu} \right| \leq (n + 1)C \max\{|x|, |y|\}^n.$$

Taking n-th roots and letting n go to infinity proves the assertion of the proposition. □

If an absolute value satisfies the ultrametric inequality, it is called **non-archimedean**; otherwise it is called **archimedean**. Clearly, if $\mathrm{char} K \neq 0$, K cannot carry any archimedean absolute

value. A typical example of an archimedean absolute value is the ordinary absolute value on $\mathbb{R}$, which is given by $|x|_0 = x$ if $x \geq 0$ and $-x$ if $x < 0$. Note that if $v : K^\times \to \mathbb{R}$ is a rank 1 valuation on K then the absolute value defined by

$$|x| = e^{-v(x)}, \quad x \in K$$

is non-archimedean. Conversely, if $|\cdot|$ is a non-archimedean absolute value then $v(x) := -\ln|x|$ is a valuation on K. Thus we see non-archimedean absolute values corresponds to rank 1 valuations.

An absolute value $|\cdot|$ on K defines a metric by taking $|x-y|$ as distance, for $x, y \in K$. In particular, $|\cdot|$ induces a topology on K. If two absolute values induce the same topology on K, they are called dependent (otherwise independent).

Proposition 14.4.13. *Let $|\cdot|_1$ and $|\cdot|_2$ be two non-trivial absolute values on K. They are dependent if and only if for all $x \in K$,*

$$|x|_1 < 1 \Rightarrow |x|_2 < 1.$$

If they are dependent, then there exists a real number $\lambda > 0$ such that $|x|_1 = |x|_2^\lambda$ for all $x \in K$.

Proof. For $|\cdot|_1$ and $|\cdot|_2$ non-trivial and dependent absolute values on K there exists $\varepsilon > 0$ such that $\{x \in K : |x|_1 < \varepsilon\} \subseteq \{x \in K : |x|_2 < 1\}$. If $|x|_1 < 1$, there is $m \geq 1$ such that $(|x|_1)^m = |x^m| < \varepsilon$. Hence $(|x|_2)^m = |x^m|_2 < 1$ and consequently $|x|_2 < 1$, as required.

Conversely, by the non-triviality of $|\cdot|_1$, there exists $z \in K$ with $|z|_2 > 1$. Thus $|z^{-1}|_1 < 1$ and so $|z^{-1}|_1 < 1$, by assumption. Hence $|z|_2 > 1$, too. Now we claim that, for every $x \in K$, $x \neq 0$, we have

$$\frac{\log|x|_1}{\log|x|_2} = \frac{\log|z|_1}{\log|z|_2}.$$

In fact, for $m, n \in \mathbb{Z}$, $n > 0$, such that

$$\frac{m}{n} > \frac{\log|x|_1}{\log|z|_1},$$

it follows that $(|z|_1)^m > (|x|_1)^n$. Consequently, $|x^n z^{-m}|_1 < 1$ and then, by assumption, $|x^n z^{-m}|_2 < 1$. Walking back the steps of the last argument one gets

$$\frac{m}{n} > \frac{\log|x|_2}{\log|z|_2}.$$

It then follows that

$$\frac{\log|x|_1}{\log|z|_1} \geq \frac{\log|x|_2}{\log|z|_2}.$$

Similarly one proves the reverse inequality. So the claim follows.

Now set $\lambda = \log|z|_1/\log|z|_2$, it follows that $|x|_1 = |x|_2^\lambda$, for every $x \in K$, as required. Finally, the last equation implies that $|\cdot|_1$ and $|\cdot|_2$ are dependent. □

Now we prove an approximation theorem for absolute values.

Theorem 14.4.14. *Let K be a field and $|\cdot|_1, \ldots, |\cdot|_n$ be non-trivial pairwise-independent absolute values on K. Moreover let $x_1, \ldots, x_n \in K$, and $0 < \varepsilon \in \mathbb{R}$. Then there exists $x \in K$ such that $|x - x_i| < \varepsilon$ for all i.*

Proof. We shall first prove that for every $1 \leq i \leq n$ there exists $a_i \in K$ such that $|a_i|_i > 1$ and $|a_i|_j < 1$, for all $j \neq i$. We may fix $i = 1$ without loss of generality, and write $a = a_1$. We proceed by induction on n. For $n = 2$, Proposition 14.4.13 implies the existence of $b, c \in K$ such that

$$|b|_1 < 1, |b|_2 \geq 1, \quad |c|_1 \geq 1, |c|_2 < 1.$$

Thus $a = b^{-1}c$ has the desired properties.

Assume next that there is $y \in K$ such that $|y|_1 > 1$ and $|y|_j < 1$ for all $j = 2, \ldots, n-1$. Applying the first case to $|\cdot|_1$ and $|\cdot|_n$, one has $|z|_1 > 1$ and $|z|_n < 1$, for some $z \in K$. Therefore, if $|y|_n \leq 1$, then $|zy^\nu|_1 > 1$ and $|zy^\nu|_n < 1$ for every integer $\nu \geq 1$. On the other hand, for a sufficiently large integer $\nu \geq 1$, $|zy^\nu|_j < 1$ for every $j = 2, \ldots, n-1$. For such a ν, $a = zy^\nu$ satisfies the requirements.

Consider now the case $|y|_n > 1$, and form the sequence

$$w_\nu = \frac{y^\nu}{1 + y^\nu}$$

The usual properties of sequences of ordinary real numbers imply that $\lim_\nu |w_\nu|_j = 0$ for $j = 2, \ldots, n-1$ and $\lim_\nu |w_\nu - 1|_j = 0$ for $j = 1$ and n. Consequently, $\lim_\nu |zw_\nu|_j = 0$ for $j = 2, \ldots, n-1$ and $\lim_\nu |zw_\nu|_j = |z|_j$ for $j = 1$ and n. Hence, for sufficiently large ν, $a = zw_\nu$ has the required properties.

Now we prove that for any real number $\varepsilon > 0$ and every i such that $1 \leq i \leq n$, there exists $c_i \in K$ such that $|c_i - 1|_i < \varepsilon$ and $|c_i|_j < \varepsilon$, for all $j \neq 1$. As before, it is enough to consider the case $i = 1$. Let $a \in K$ satisfy $|a|_1 > 1$ and $|a|_j < 1$ for $j > 1$. Then the sequence $|a^\nu/(1 + a^\nu)|_j$ converges to 1 for $j = 1$, and converges to 0 if $j > 1$. Thus for sufficiently large ν,

$$c_1 = \frac{a^\nu}{1 + a^\nu}$$

has the required property.

According to the argument above, there exist elements $c_1, \ldots, c_n$ in K such that c_i is close to 1 at $|\cdot|_i$, and for every $j \neq i$, c_i is close to 0 at $|\cdot|_j$. The element $x = c_1x_1 + \cdots + c_nx_n$ is then arbitrarily close to x_i at $|\cdot|_i$, for every $i = 1, \ldots, n$, and therefore satisfies the requirements of the theorem. □

We now prove some result about topological vector spaces over a valued field, which will be used later.

Proposition 14.4.15. *Let (K, v) be a valued field with valued group Γ. Let X be a topological vector space over K which is Hausdorff and of dimension 1. Suppose that v is not trivial. For all $x_0 \in X$, the mapping $a \mapsto ax_0$ of K onto X is a topological isomorphism.*

Proof. This mapping is a continuous algebraic isomorphism. It is sufficient to show that it is bicontinuous. Let $\alpha \in \Gamma$. We need to show that there exists a neighbourhood V of 0 in X such that the relation $ax_0 \in V$ implies $v(a) > \alpha$. Let $a_0 \in K^\times$ be such that $v(a_0) = \alpha$. As X is Hausdorff, there exists a neighbourhood W of 0 in X such that $a_0x_0 \notin W$. Since v is not improper, there exist a neighbourhood W' of 0 in X and an element β of Γ such that the relations $y \in W'$ and $v(a) \geq \beta$ imply $ay \in W'$. Let $a_1 \in K^\times$ be such that $v(a_1) = -\beta$. The

relations $ax_0 \in a_1^{-1}W'$ and $v(a) \leq \alpha$ imply $a_1 a x_0 \in W'$ and

$$v(a_0 a^{-1} a_1^{-1}) = v(a_0) - v(a) - v(a_1) = \alpha + \beta - v(a) \geq \beta$$

hence $a_0 x_0 = (a_0 a^{-1} a_1^{-1}) a_1 a x_0 \in W$, which is a contradiction. In other words, the relation $ax_0 \in a_1^{-1}W'$ implies $v(a) > \alpha$, so we are done. □

Proposition 14.4.16. *Suppose that v is not trivial. If M is a closed maximal subspace of a topological vector space X over K then any algebraic complement N of M is a topological complement.*

Proof. Let M be a closed maximal subspace of a topological vector space X. Since M is maximal, $\dim X/M = 1$; hence if N is an algebraic complement of M, $\dim N = 1$. Therefore there must be some $x \neq 0$ such that $N = Kx$. Consequently $X = M \oplus Kx$ and each vector y has a unique representation in the form $y = m + tx$, $m \in M$, $t \in K$. To show that Kx is a topological complement of M, we use the criterion of Corollary 3.3.5: We show that the projection P on Kx along M, $tx + m \mapsto tx$, is continuous.

To this end note that $N(P) = M$. As M is closed and $x \notin M$, there exists a neighborhood U of 0 in X such that $(x + U) \cap M = \varnothing$ and $xU \subseteq U$ whenever $v(x) \geq -\gamma_0$, for some fixed $\gamma_0 \in \Gamma$. Now if $m + tx \in U$ then we must have $v(t) > \gamma_0$: otherwise we have $v(t) \leq \gamma_0$ and so $v(t^{-1}) \geq -\gamma_0$, thus $t^{-1}(m + tx) = m/t + x \in U$, which contradicts $(x + U) \cap M = \varnothing$. Hence if $\gamma > \gamma_0$ and $m + tx \in U_\gamma(0)U$, then $t > \gamma + \gamma_0$.

To establish the continuity of P at 0, suppose that the net $m_\alpha + t_\alpha x \to 0$. As such, for any $\gamma > 0$, $m_\alpha + t_\alpha x \in U_\gamma(0)U$ eventually. Therefore $t_\alpha > \gamma + \gamma_0$ eventually. In other words, $t_\alpha \to 0$ in K, which implies that $t_\alpha x = P(m_\alpha + t_\alpha x) \to 0$, and proves the continuity of P. □

Proposition 14.4.17. *Suppose that v is nontrivial and K is complete. Let X be a topological vector space over K, which is Hausdorff and of finite dimension n. For every basis $(e_i)_{i=1}^n$ of X over K, the mapping $(a_i) \mapsto \sum_{i=1}^n a_i e_i$ from K^n onto X is a topological vector space isomorphism.*

Proof. This follows from induction, using Proposition 14.4.15 and Proposition 14.4.16. □

Corollary 14.4.18. *Suppose that v is nontrivial and K is complete. Let X be a Hausdorff topological vector space over K and F a finite-dimensional vector subspace of X. Then F is closed.*

14.5 Completion of valued fields

Since a non-trivial absolute value v makes K into a topological field, we may consider the completion of K with respect to the additive uniform structure. The next theorem will show that every field K with a non-trivial valuation can be densely embedded into a field complete with respect to a valuation extending the given one on K.

Theorem 14.5.1. *Let K be a field, v a valuation on K and Γ the value group of v with the discrete topology.*

(a) The completion ring $\widehat{K}$ of K (with respect to $\mathcal{T}_v$) is a topological field.

(b) The mapping $v : K^\times \to \Gamma$ can be extended uniquely to a continuous mapping $\hat{v} : \widehat{K}^\times \to \Gamma$. The mapping $\hat{v}$ is a valuation on $\widehat{K}$ with value group Γ.

(c) *The topology on $\widehat{K}$ is the topology defined by the valuation $\hat{v}$.*

(d) *If $U_\gamma(x), V_\gamma(x)$ and $\widehat{U}_\gamma(x), \widehat{V}_\gamma(x)$ are the basic neighborhood of x in (K, v) and $(\widehat{K}, \hat{v})$, then $\widehat{U}_\gamma(x)$ is the closure of $U_\gamma(x)$ in $\widehat{K}$ and $\widehat{V}_\gamma(x)$ is the closure of $V_\gamma(x)$ in $\widehat{K}$.*

(e) *The valuation ring of $\hat{v}$ is the completion $\widehat{A}$ of the valuation ring A of v; the maximal ideal $\widehat{\mathfrak{m}}$ is the completion of the maximal ideal $\mathfrak{m}$ of v.*

(f) *$\widehat{A} = A + \widehat{\mathfrak{m}}$ and the residue field of $\hat{v}$ is canonically identified with that of v.*

Proof. By Proposition 3.3.22, to prove (a), it suffices to show the following: let $\mathfrak{U}$ be a Cauchy filter (with respect to the additive uniform structure) on $K^\times$ for which 0 is not a cluster point; then the image of $\mathfrak{U}$ under the bijection $x \mapsto x^{-1}$ is a Cauchy filter (with respect to the additive uniform structure). For since 0 is not a clustcr point of $\mathfrak{U}$, there exists $V \in \mathfrak{U}$ and $\gamma \in \Gamma$ such that γ is an upper bound of $v(M)$. Let $\alpha \in \Gamma$. If V' is an element of $\mathfrak{U}$ contained in M and such that $v(x - y) > \max\{\alpha + 2\gamma, \gamma\}$ for $x, y \in V'$, then $v(x^{-1} - y^{-1}) > \gamma$ for $x, y \in V$ (see (4.0.1)). Whence (a) follows.

By Proposition 14.4.1, $v : K^\times \to \Gamma$ is a continuous homomorphism from $K^\times$ to Γ and hence can be extended uniquely to a continuous homomorphism $\hat{v}$ from $\widehat{K}^\times$ to Γ. The relation $\hat{v}(x + y) \geq \min\{\hat{v}(x), \hat{v}(y)\}$ holds in $K^\times$ and hence also holds in $\widehat{K}^\times$ by continuity. Thus $\hat{v}$ (extended by $\widehat{K}$ by $\hat{v}(0) = \infty$) is a valuation on $\widehat{K}$ and (b) is proved.

Wc now show (d). Let $\gamma \in \Gamma$ and $x \in \overline{U}_\alpha(0)$. For y in $U_\alpha(0)$ sufficiently close to x, $v(y) = \hat{v}(y) = \hat{v}(x)$ and hence $\hat{v}(x) > \gamma$. Conversely, let $x \in \widehat{K}^\times$ be such that $\hat{v}(x) > \alpha$; for y in $K^\times$ sufficiently close to x, $v(y) = \hat{v}(y) = \hat{v}(x)$ and therefore $y \in U_\gamma(0)$, whence $x \in \overline{U}_\gamma(0)$. Thus $\overline{U}_\gamma(0)$ is the set of $x \in \widehat{K}$ such that $\hat{v}(x) > \gamma$. The general case for $U_\gamma(x)$ now follows from homogeneity, and the result for $V_\gamma(x)$ can be proved similarly.

Taking account of Proposition 3.2.14, assertion (c) is a consequence of (d). Assertion (e) is a special case of (d). Finally let $x \in \widehat{A}$; since $\widehat{A}$ is the closure of A in $\widehat{K}$, there exists $y \in A$ such that $\hat{v}(x - y) > 0$; then $z = x - y \in \widehat{\mathfrak{m}}$ and hence $x = y + z \in A + \widehat{\mathfrak{m}}$; thus $\widehat{A} = A + \widehat{\mathfrak{m}}$ which shows (f). □

14.5.1 Archimedean complete fields

Let K be a field complete with respect to an archimedean absolute value $|\cdot|$. Since the set $\{|n \cdot 1| : n \in \mathbb{Z}\}$ is not bounded, $\mathrm{char} K = 0$. Thus K contains the field $\mathbb{Q}$ of rationals. We shall first show that $|\cdot|$ restricted to $\mathbb{Q}$ is dependent on the usual absolute value of $\mathbb{Q}$. Thus the complete field K contains the completion of $\mathbb{Q}$ with respect to the ordinary absolute value, i.e., K contains $\mathbb{R}$ as a closed subfield. We shall then show that K must be equal to $\mathbb{R}$ or to $\mathbb{C}$. Consequently, every field K admitting an archimedean absolute value may be considered as a subfield of $\mathbb{C}$ or even $\mathbb{R}$ with the absolute value dependent on the induced one from $\mathbb{C}$ (or from $\mathbb{R}$).

Proposition 14.5.2. *Every archimedean absolute value on $\mathbb{Q}$ is dependent on the usual one.*

Proof. Let $|\cdot|$ be an archimedean absolute value on $\mathbb{Q}$. Denote by $|\cdot|_0$ the usual absolute value on $\mathbb{Q}$. Next, for integers $m, n \geq 2$ and $t \geq 1$, expand m^t in powers of n:

$$m^t = c_0 + c_1 n + \cdots + c_s n^s, \quad 0 \leq c_0, \ldots, c_s < n, c_s \neq 0.$$

Since each c_i is integer, we have $|c_i| \le c_i < n$. It follows that

$$|m|^t \le \sum_{i=0}^{s} |c_i||n|^i \le n \sum_{i=0}^{s} |n|^i \le n(s+1)\max\{1, |n|^s\}.$$

As $n^s \le m^t$, $s \le t(\log m)/\log n$. Thus

$$|m|^t \le n\Big(\frac{t\log m}{\log n} + 1\Big)\max\{1, |n|\}^{t(\log m/\log n)}$$

or equivalently,

$$|m| \le n^{1/t}\Big(\frac{t\log m}{\log n} + 1\Big)^{1/t}\max\{1, |n|\}^{\log m/\log n}.$$

Letting t go to infinity and taking limits, one gets

$$|m| \le \max\{1, |n|\}^{\log m/\log n}.$$

Now, if $|n| < 1$ for some $n \in \mathbb{N}$, the above inequality implies $|m| < 1$ for every integer $m \ge 2$, contradicting the archimedeanness of $|\cdot|$. Therefore, $|n| > 1$ for all integers $n \ge 2$, and thus

$$|m| \le |n|^{\log m/\log n}.$$

Interchanging the roles of m and n in the above inequality gives the reverse inequality. Hence

$$|m| = |m|^{\log m/\log n}$$

Therefore, if $m > n \ge 2$, then $\log m/\log n > 1$ and so $|m| > |n|$. Since $|-m| = |m|$ for all $m \in \mathbb{Z}$, it follows that $|m|_0 > |n|_0$ implies $|m| > |n|$, for non-zero $m, n \in \mathbb{Z}$. Consequently, if $m/n \in \mathbb{Q}$ satisfies $|m/n|_0 < 1$, then $|m/n| < 1$. By Proposition 14.4.13, $|\cdot|_0$ and $|\cdot|$ are dependent. □

In case E is a field extension of K, every absolute value $|\cdot|'$ of E that restricts to $|\cdot|$ on K is a norm of E compatible with $|\cdot|$. If E has finite degree over K and K is complete with respect to $|\cdot|$, the next proposition will imply that up to equivalence of norms (and hence up to dependence as absolute values), E admits only one absolute value $|\cdot|'$ restricting to $|\cdot|$ on K. Moreover, E is complete with respect to $|\cdot|'$.

Proposition 14.5.3. *Let K be a field complete with respect to a non-trivial absolute value $|\cdot|$. Then every two norms (compatible with $|\cdot|$) of a finite dimensional K-vector space E are equivalent.*

Proof. We shall prove that any such norm on E is equivalent to the max-norm of E. This will be done by induction on the dimension n of the K-vector space E. For $n = 1$ the statement is obvious. Assume the proposition is proved for $n-1$, $n \ge 2$. One inequality is very simple to prove. Fix a basis $\omega_1, \dots, \omega_n$ of E over K, and for $\xi = x_1\omega_1 + \cdots + x_n\omega_n$, denote $\|\xi\|_{\max} = \max_i |x_i|$. Then

$$\|\xi\| \le \sum_{i=1}^{n} |x_i|\|\omega_i\| \le C\|\xi\|_{\max} \quad \text{where } C = n\max_i \|\omega_i\|.$$

We must now prove that there exists a number $C' > 0$ such that for all $\xi \in E$,

$$\|\xi\|_{\max} \leq C'\|\xi\|.$$

Suppose no such number exists. Then, for every positive integer m there exists $\xi \in E$ such that $\|\xi\|_{\max} > m\|\xi\|$. Let j be such that $|x_j| = \max_{1\leq i\leq n} |x_i|$. Letting $\xi_m = x_j^{-1}\xi$ we get $\|\xi\|_{\max} = 1$ and thus $\|\xi_m\| < 1/m$. For every $m \geq 1$, one of the components of ξ_m equals 1. Thus there must be an infinite subset T of $\mathbb{N}$ and a fixed number j such that the j-th component of ξ_m equals 1 for all $m \in T$. We fix this number j from now until the end of the proof.

Consider the subspace E_1 of E consisting of all vectors whose j-th coordinate is equal to 0, equipped with the norm induced by $\|\cdot\|$. By induction, the restrictions of $\|\cdot\|$ and max-norm $\|\cdot\|_{\max}$ to E_1 are equivalent. In particular, a sequence of elements of E_1 converges to $\zeta \in E_1$ with respect to $\|\cdot\|_{\max}$ if and only if it converges to ζ with respect to $\|\cdot\|$.

For each $m \in T$ we can write $\xi_m = \omega_j + \zeta_m$, for some $\zeta_m \in E_1$. Now, for every $\varepsilon > 0$, take $N \in \mathbb{N}$ such that $2/N < \varepsilon$. If $m, n \geq N$, $m, n \in T$, then

$$\|\zeta_m - \zeta_n\| = \|\zeta_m + \omega_j - \omega_j - \zeta_n\| = \|\xi_m - \xi_n\| \leq \|\xi_m\| + \|\xi_n\| < \frac{1}{m} + \frac{1}{n} \leq \frac{2}{N} < \varepsilon.$$

Consequently, (ζ_m) is a Cauchy sequence with respect to the restriction of $\|\cdot\|$ to E_1. From the induction hypothesis, it follows that this sequence is also a Cauchy sequence with respect to the max-norm. Since E_1 is complete with respect to the max-norm, this sequence converges to some $\zeta \in E_1$ (with respect to the max-norm).

The choice of T implies $\|\omega_j + \zeta_m\| < 1/m$ for each $m \in T$. Since the restrictions of $\|\cdot\|$ and the max-norm to E_1 are equivalent,

$$\|\zeta - \zeta\| \leq C\|\zeta_m - \zeta\|_{\max}$$

for some number $C > 0$. Therefore,

$$\|\omega_j + \zeta\| \leq \|\omega_j + \zeta_m\| + \|\zeta - \zeta_m\| \leq \frac{1}{m} + C\|\zeta - \zeta_m\|_{\max}.$$

Letting $m \in T$ go to infinity, the right-hand side of the preceding inequality tends to 0. Hence $\omega_j + \zeta = 0$. But, this cannot occur, because $\zeta \in E_1$ has the j-th coordinate equal to 0 and $\omega_1, \ldots, \omega_n$ is a basis of E over K. This contradiction finishes the proof of the proposition. □

Theorem 14.5.4. *Let K be a field containing $\mathbb{R}$ and having an absolute value that induces the ordinary one on $\mathbb{R}$. Then $K = \mathbb{R}$ or $K = \mathbb{C}$.*

In particular, the only fields complete with respect to an archimedean absolute value $|\cdot|$ are (up to isomorphism) $\mathbb{R}$ and $\mathbb{C}$ with $|\cdot|$ dependent on the ordinary absolute value.

This theorem is a consequence of the following proposition:

Proposition 14.5.5 (Gelfand-Mazur). *Let A be a commutative normed algebra with identity and assume that A contains an element j such that $j^2 = -1$, and let $\mathbb{C} = \mathbb{R} + j\mathbb{R} \subseteq A$ (identify $\mathbb{R}\cdot 1$ with $\mathbb{R}$). Then for every nonzero element $x_0 \in A$, there exists an element $c \in \mathbb{C}$ such that $x_0 - c$ is not invertible in A.*

Proof. Suppose that $x_0 - z$ is invertible for all $z \in \mathbb{C}$. The map $f : \mathbb{C} \to A$ defined by $f(z) = (x_0 - z)^{-1}$, is then well defined. Moreover, we shall see that taking inverses is a continuous operation on the group of units of A, from which it will follow that f is continuous. In order to show that $x \mapsto x^{-1}$ is continuous on the group of units of A, note that for any units a and x in A,

$$\|x^{-1} - a^{-1}\| = \|(a - x)a^{-1}x^{-1}\| \leq \|x - a\|\|a^{-1}\|\|x^{-1}\|.$$

Thus it remains to show that $\|x^{-1}\|$ is bounded as x varies through units near a. Let $\|a^{-1}\|\|x - a\| \leq 1/2$, and set $w = a^{-1}(x - a)$. Then clearly $\|w\| \leq 1/2$. Hence we get

$$\left\|\frac{1}{1+w}\right\| = \left\|1 - \frac{w}{1+w}\right\| \leq 1 + \frac{\|w\|}{1 + \|w\|} \leq 1 + \frac{1}{2}\left\|\frac{1}{1+w}\right\|.$$

This implies $\|(1 + w)^{-1}\| \leq 1/2$. Thus finally we get

$$\|x^{-1}\| = \|a^{-1}(1 + w)^{-1}\| \leq 2\|a^{-1}\|.$$

Back to the proof of the proposition, observe that for $0 \neq z \in \mathbb{C}$,

$$f(z) = \frac{1}{x_0 - z} = \frac{1}{z}\left(\frac{1}{x_0 z^{-1} - 1}\right).$$

Since z^{-1} and $x_0 z^{-1}$ approach 0 when z goes to infinity in $\mathbb{C}$, it follows that $f(z) \to 0$ when $z \to \infty$. On the other hand, the map $z \mapsto \|f(z)\|$ is continuous, being the composition of two continuous maps. Consequently, $\|f(z)\| \to 0$ when $z \to \infty$. Hence this map may be considered as a real valued continuous map on the one-point compactification $\widehat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ of $\mathbb{C}$. Hence $\|f\|$ has a maximum $M \in \mathbb{R}$, $M > 0$. Let D be the set of elements $z \in \mathbb{C}$ such that $\|f(z)\| = M$. Then D is a non-empty, bounded, and closed subset of $\mathbb{C}$. We shall prove that it is also open, a contradiction.

For $z_0 \in D$, let us write $y = x_0 - z_0$ and let t be a nonzero complex number to be determined later. Consider the polynomial $h(X) = X^n - t^n = \prod_{j=1}^{n}(X - \zeta^j t)$, whence

$$\frac{h'(X)}{h(X)} = \frac{nX^{n-1}}{X^n - t^n} = \sum_{j=1}^{n-1} \frac{1}{X - \zeta_n^j t} + \frac{1}{X - t}.$$

Dividing by n and replacing every occurrence of X by y, taking account of the definitions of f and y, we obtain

$$f(z_0 + t) + \sum_{j=1}^{n-1} f(z_0 + \zeta_n^j t) - nf(z_0) = \frac{ny^{n-1}}{y^n - t^n} - \frac{n}{y} = \frac{n}{y} \cdot \frac{t^n y^{-n}}{1 - t^n y^{-n}}. \tag{5.1.1}$$

If we choose t such that $\|ty^{-1}\| < 1$, then the last expression in (5.1.1) tends to 0 as n tends to ∞; hence

$$\|f(z_0 + t)\| = \lim_{n\to\infty} \|nf(z_0) - \sum_{j=1}^{n-1} f(z_0 + \omega_n^j t)\|. \tag{5.1.2}$$

Now, $\|f(z_0)\| = M$ and $\|f(z_0 + \omega_n^j t)\| \leq M$ by definition of M, whence

$$\|nf(z_0) - \sum_{j=1}^{n-1} f(z_0 + \omega_n^j t)\| \geq n\|f(z_0)\| - \sum_{j=1}^{n-1} \|f(z_0 + \omega_n^j t)\| \geq nM - (n-1)M = M.$$

Therefore by (5.1.2), letting n tend to ∞, $\|f(z_0 + t)\| \geq M$ and by definition of M this implies $\|f(z_0 + t)\| = M$; in other words $z_0 + t \in D$. This proves that the set D is open in $\mathbb{C}$; as it is also closed and non-empty and $\mathbb{C}$ is connected, $D = \mathbb{C}$ and f is therefore constant on $\mathbb{C}$; as this function tends to 0 at the point at infinity, $\|f(z)\| = 0$ in $\mathbb{C}$ and in particular $\|f(0)\| = \|x^{-1}\| = 0$, which is absurd. □

Proof of Theorem 14.5.4. We apply Proposition 14.5.5 to the $\mathbb{R}$-algebra K, and let the given absolute value serve as norm. If K contains $\mathbb{C}$, then $K = \mathbb{C}$, because every element of K is invertible. If K does not contain $\mathbb{C}$, let $L = K(j)$, where $j^2 = -1$. Define a norm on L by putting $\|x + yj\| = \|x\| + \|y\|$ for $x, y \in K$. This clearly makes L a normed $\mathbb{R}$-algebra. Moreover, by standard calculations one proves that $\|1\| = 1$ and $\|zw\| \leq \|z\|\|w\|$. Now, applying Proposition 14.5.5 to $A = L$, we obtain $L = \mathbb{C}$ as before. Thus K must be $\mathbb{R}$. □

14.5.2 Non-archimedean complete fields

As we have already noticed, non-archimedean absolute values corresponds to rank 1 valuations. Therefore, for non-archimedean absolute values, we will use this additive notation and refer non-archimedean absolute values to valuations of rank 1.

Now we prove an important property of a field K complete with respect to a (non-trivial) valuation v. This theorem is widely known as Hensel's Lemma.

Theorem 14.5.6 (Hensel's Lemma). *Let K be a field complete with respect to a non-archimedean absolute value v. Let $f \in A_v[X]$ be a polynomial, and let $a_0 \in A_v$ be such that $v(f(a_0)) > 2v(f'(a_0))$. Then there exists some $a \in A_v$ with $f(a) = 0$ and $v(a_0 - a) > v(f'(a_0))$.*

Proof. The natural way to reach the conclusions of the theorem is to construct a suitable Cauchy sequence which must converge to a root a of f (recall that every polynomial f is a continuous map).

We use the Nowton approximation method: define a sequence (a_n) by

$$a_{n+1} = a_n - \frac{f(a_0)}{f'(a_0)}.$$

We will show that (a_n) has a limit a and this element a satisfies the requirements. In fact, set $r = v(f(a_0)) - 2v(f'(a_0)) > 0$, we will prove by induction that

(a) $v(a_n) \geq 0$.

(b) $v(a_{n+1} - a_n) = v(f(a_n)/f'(a_n)) \geq v(f(a_n)/f'(a_n)^2) \geq 2^n r$.

(c) $v(a_n - a_0) \geq v(f(a_0)/f'(a_0))$.

(d) $v(f'(a_n)) = v(f'(a_0))$.

By hypothesis, (a), (b), and (c) holds for $n = 0$. Now assume these conditions for n, then we can see (a) holds for $n+1$. Since a_n and $f(a_n)/f'(a_n)$ are in A_v, by Talor expansion we have

$$\begin{aligned} v(f(a_{n+1})) &= v\Big(f\Big(a_n - \frac{f(a_n)}{f'(a_n)}\Big)\Big) = v\Big(f(a_n) - f'(a_n)\cdot\frac{f(a_n)}{f'(a_n)} + M\Big(\frac{f(a_n)}{f'(a_n)}\Big)^2\Big) \\ &= v\Big(M\Big(\frac{f(a_n)}{f'(a_n)}\Big)^2\Big) \geq v\Big(\Big(\frac{f(a_n)}{f'(a_n)}\Big)^2\Big) \end{aligned} \tag{5.2.1}$$

where $M \in A_v$. Similarly,

$$\frac{f'(a_{n+1})}{f'(a_n)} = \frac{1}{f'(a_n)}\Big(f'(a_i) + M'\frac{f(a_n)}{f'(a_n)}\Big) = 1 + M'\frac{f(a_n)}{f'(a_n)^2}$$

for some $M' \in A_v$, whence

$$v\Big(\frac{f'(a_{n+1})}{f'(a_n)}\Big) = 0 \tag{5.2.2}$$

and $v(f'(a_{n+1})) = v(f'(a_n)) \neq \infty$. Now by (5.2.1) and (5.2.2),

$$\begin{aligned} v\Big(\frac{f(a_{n+1})}{f'(a_{n+1})^2}\Big) &\geq v\Big(\Big(\frac{f(a_n)}{f'(a_n)}\Big)^2\Big) - v(f'(a_{n+1})^2) = v\Big(\Big(\frac{f(a_n)}{f'(a_n)}\Big)^2\Big) - v(f'(a_n)^2) \\ &= 2v\Big(\frac{f(a_n)}{f'(a_n)^2}\Big) \geq 2^{n+1}r. \end{aligned} \tag{5.2.3}$$

This proves condition (b) for $n+1$. Moreover, by (5.2.3),

$$v\Big(\frac{f(a_{n+1})}{f'(a_{n+1})^2}\Big) \geq v\Big(\frac{f(a_n)}{f'(a_n)^2}\Big).$$

From (5.2.2), this implies

$$v\Big(\frac{f(a_{n+1})}{f'(a_{n+1})}\Big) \geq v\Big(\frac{f(a_n)}{f'(a_n)}\Big) \geq \cdots \geq v\Big(\frac{f(a_0)}{f'(a_0)}\Big)$$

which is to say

$$v(a_{n+1} - a_n) \geq v(a_n - a_{n-1}) \geq \cdots \geq v(a_1 - a_0),$$

and therefore

$$v(a_n - a_0) = v(\sum_{i=1}^{n}(a_n - a_{n-1})) = v(a_1 - a_0) = v\Big(\frac{f(a_0)}{f'(a_0)}\Big).$$

This proves (c), and completes the induction process.

From (a) and (b) we see (a_n) is a Cauchy sequence in K, so admits a limit $a \in K$. Also, since the valuation is continuous, we have $v(a) \geq 0$, whence $a \in A_v$. Taking limit in the recursion formula, we see $f(a) = 0$. Also, by (c), we have $v(a - a_0) \geq v(f(a_0)/f'(a_0)) > v(f'(a_0))$. □

Corollary 14.5.7. *Let K, v be as in Theorem 14.5.6. If $f \in A_v[X]$ has a simple zero a_0 in the residue field κ_v, i.e., $\bar{f}(\bar{a}_0) = 0$ and $\bar{f}'(a_0) \neq 0$, then f has a zero $a \in A_v$ such that $\bar{a} = \bar{a}_0$.*

The proof of Theorem 14.5.6 clearly shows that under the assumption of Theorem 14.5.6, the sequence $(f(a_n))$ converges to 0. At this point, essential use is made of the fact that $v(K^\times)$

is a subgroup of the additive reals. Thus even without the completeness of K, we could still notice:

Proposition 14.5.8. *Let v be a non-archimedean absolute value on K. Then for every $f \in A_v[X]$, if $\bar{f}$ has a simple zero in κ_v, then $f(K)$ approximates* 0.

Now consider the completion $(\widehat{K}, \hat{v})$ of the field with respect to a non-archimedean absolute value v, but now using the additive notation for absolute values. The density of K in $\widehat{K}$ has the following important consequence.

Theorem 14.5.9. *Denote by $\widehat{A}_v$, $\kappa_{\hat{v}}$ and A_v, κ_v the valuation ring and the residue field of $\hat{v}$ and v, respectively. Then the residue fields κ_v and $\kappa_{\hat{v}}$, as well as the groups Γ_v and $\Gamma_{\hat{v}}$, are canonically isomorphic.*

Proof. It follows from the constructions that $A_{\hat{v}} \cap K = A_v$ and $\mathfrak{m}_{\hat{v}} \cap K = \mathfrak{m}$, where $\mathfrak{m}_{\hat{v}}$ and $\mathfrak{m}_v$ are the respective maximal ideals. Thus the map that sends the residue class of $a \in A_v$ to the residue class $\bar{a} \in A_{\hat{v}}/\mathfrak{m}_{\hat{v}}$ is well defined; and it is clearly a ring homomorphism. It remains to be seen that it is surjective. For every $x \in A_{\hat{v}}$, the set $x + \mathfrak{m}_{\hat{v}}$ is an open neighbourhood of x. It consists of all elements z such that $\hat{v}(z - x) > 0$, or $|z - x| < 1$ in terms of the absolute value. Thus the set $(x + \mathfrak{m}_v) \cap K$ is non-empty, by the density property. Hence the residue class of $y \in (x + \mathfrak{m}_{\hat{v}}) \cap K$ is sent by the map above to $\bar{x}$, as required.

Similarly, the map $\Gamma_v \to \Gamma_{\hat{v}}$ sending $v(x)$ to $\hat{v}(x)$ for every $x \in K^\times$ is an order-preserving group monomorphism. In order to show surjectivity, let $x \in \widehat{K}^\times$ be given. By the density of K in $\widehat{K}$ there exists $z \in K$ with $\hat{v}(z - x) > v(x)$, or $|z - x|_{\widehat{K}} < |x|$ in terms of the absolute value. But then $\hat{v}(z) = v(x)$. □

Example 14.5.10. Now consider the p-adic valuation on $\mathbb{Q}$; the completion of $(\mathbb{Q}, v_p)$ is denoted by $\mathbb{Q}_p$, and is called the field of **p-adic numbers**. The valuation ring of $\mathbb{Q}_p$, denoted by $\mathbb{Z}_p$, is the ring of p-adic integers; it is the topological closure of $\mathbb{Z}$ in $\mathbb{Q}_p$, as we shall see below. According to our previous discussion of this example, Theorem 14.5.9 implies that the residue class field of $\mathbb{Z}_p$ is $\mathbb{F}_p$. Observe also that p is a local parameter for v_p in both fields, $\mathbb{Q}$ and $\mathbb{Q}_p$.

Example 14.5.11. If we fix X as the irreducible polynomial p, then the completion of $(k(X), v_X)$ is the field $k((X))$ of formal Laurent series over k, and the valuation ring is $k[\![X]\!]$, the ring of formal power series.

The last two examples above are special cases of the following more general result:

Proposition 14.5.12. *Let v be a discrete absolute value on the field K, with uniformizer π. Then every element $x \in K^\times$ can be written uniquely as a convergent series*

$$x = \sum_{i=\nu}^{\infty} r_i \pi^i$$

where $\nu = v(x)$, $r_\nu \neq 0$, and the coefficients r_i are taken from a set $R \subseteq A_v$ of representatives of the residue classes in the field κ_v (i.e., the canonical map $A_v \to \kappa_v$ induces a bijection of R onto κ_v). In particular, the valuation ring of $\widehat{K}$ is a complete discrete valuation ring with uniformizer π, and we have an isomorphism of topological rings $\widehat{A} \cong \varprojlim A/\pi^n A$.

Proof. We proceed by induction. As observed above, $u = x\pi^{-\nu}$ is a unit in A_v. Choose $r_\nu \in R$ such that $\bar{r}_\nu = \bar{u}$. Then clearly $v(x\pi^{-\nu} - r_\nu) > 0$ or, equivalently,

$$v(x - r_\nu \pi^\nu) > v(\pi^\nu) = \nu.$$

Let $x_1 = x - r_\nu \pi^\nu$ and $\nu_1 = v(x_1) > \nu$. Then by the same argument we get $r_{\nu_1} \in R$ such that

$$v(x - (r_\nu \pi^\nu + r_{\nu_1}\pi^{\mu_1})) = v(x_1 - r_{\mu_1}\pi^{\mu_1}) > \nu_1.$$

Repeating this argument and adding "zero coefficients" (i.e. a representative for zero in κ_v) if necessary, we obtain the existence of the "series"

$$r_\nu \pi^\nu + r_{\nu+1}\pi^{\nu+1} + \cdots$$

At the same time we see that it converges to x.

The uniqueness of the coefficients is clear. Indeed, otherwise 0 would have a representation

$$0 = (r_\nu - r'_\nu)\pi^\nu + (r_{\nu+1} - r'_{\nu+1})\pi^{\nu+1} + \cdots$$

with $r_\nu \neq r'_\nu \in R$, and hence $r_\nu - r'_\nu \neq 0$ in κ_v. But $v(0) = \infty$, a contradiction.

Let $\widehat{A}$ be the valuation ring of $\hat{v}$. Then $\widehat{A}$ is complete (it is closed in $\widehat{K}$) and contains A. For each $n \geq 1$ we define a ring homomorphism $\phi_n : \widehat{A} \to A/\pi^n A$ as follows: for each $x = \sum_{i=0}^{\infty} r_i \pi^i$ let $\phi_n(x)$ be the n-th truncation $\sum_{i=0}^{n-1} r_i \pi^i$. We thus obtain an infinite sequence of surjective maps $\phi_n : \widehat{A} \to A/\pi^n A$ that are compatible in that for all $n \geq m > 0$ and all $x \in \widehat{A}$ the image of $\phi_n(x)$ in $A/\pi^m A$ is $\phi_m(x)$. This defines a surjective ring homomorphism $\phi : \widehat{A} \to \varprojlim A/\pi^n A$. Now note that $\ker \phi = \bigcap_n \pi^n \widehat{A} = \{0\}$ so ϕ is injective and therefore an isomorphism.

To show that ϕ is also a homeomorphism, it suffices to note that if $x + \pi^m A$ is a coset of $\pi^m A$ in A and U is the corresponding open set in $\varprojlim A/\pi^n A$, then $\phi^{-1}(U)$ is the closure of $x + \pi^m A$ in $\widehat{A}$, which is the coset $x + \pi^m \widehat{A}$, an open subset in $\widehat{A}$ (as explained in the discussion above, every open set in the inverse limit corresponds to a finite union of cosets $x + \pi^m A$ for some m). Conversely ϕ maps open sets $x + \pi^m \widehat{A}$ to open sets in $\varprojlim A/\pi^n A$. □

Example 14.5.13. Returning once more to our typical examples, any p-adic number $z \in \mathbb{Q}_p^\times$ has a unique representation in the form

$$z = \sum_{i=\nu}^{\infty} a_i p^i$$

where $\nu = v_p(z)$, $0 \leq a_i < p$ for every i, and $a_\nu \neq 0$. The set of representatives chosen here is then $R = \{0, \ldots, p-1\}$. If $z \in \mathbb{Z}_p$, i.e., if $v(z) \geq 0$, then $z = \sum_{i=0}^{\infty} a_i p^i$. This shows, in particular, that $\mathbb{Z}$ is dense in $\mathbb{Z}_p$. The reader should be aware of the fact that addition of two "series" of the form $\sum_{i=\nu} a_i p^i$ is not coefficient-wise, as the set R is not closed under addition. As a simple example observe that (choosing $p = 7$)

$$5p^i + 4p^i = p^{i+1} + 2p^i$$

Example 14.5.14. For the X-adic valuation of $k(X)$, we can take the elements of k itself as

representatives of the residue field. In this case every $z \in k(X))^\times$ has a unique representation in the form

$$z = \sum_{i=\nu}^{\infty} a_i X^i$$

where $v_X(z) = \nu \in \mathbb{Z}$ and $a_i \in k$ for every i. This time, addition of two such series is coefficient-wise. These series are called formal Laurent series. They form a field $k((X))$, the field of formal Laurent series. The canonical discrete absolute value on $k((X))$ is just given by

$$v\Big(\sum_{i=\nu}^{\infty} a_i X^i\Big) = \nu \quad \text{if } \nu \neq 0.$$

Clearly its valuation ring consists of the ring $k[\![X]\!]$ of formal power series, i.e., series of the type $\sum_{i=0}^{\infty} a_i X^i$.

14.6 Extensions of valuation rings

In this part we consider valuation rings in different fields. In particular, we will see how different valuation rings relate in a field extension, and we will prove a fundamental inequality in this situation.

14.6.1 Ramification index and inertial degree

Let $K \subseteq L$ be a field extension and w a valuation of L. Then it is easy to see $v = w|_K$ is a valuation of K and for maximal ideals we have

$$\mathfrak{m}_v = \mathfrak{m}_w \cap K.$$

That is, A_v is dominated by A_w. Conversely, if v is a valuation of K, then by Theorem 14.1.7 we can find a valuation ring of L dominating A_v. If w is the valuation of this ring, then the valuation v is given by the restriction of w on K and for value groups we have $\Gamma_v \subseteq \Gamma_w$. Also, since A_w dominates A_v, we also have an extension of residue fields : $\kappa_v \subseteq \kappa_w$. Now we make the following definition.

Definition 14.6.1. *The index $[\Gamma_w : \Gamma_v]$ is called the **ramification index** of w over v and denoted by $e(w/v)$. If this index equals 1 then w is called **unramified** over v.*

Definition 14.6.2. *The index $[\kappa_w : \kappa_v]$ is called the **inertial degree** of w over v and denoted by $f(w/v)$.*

In particular, if $e(w/v) = 1$ and $f(w/v) = 1$, the extension w/v is called **immediate**. We follow the usual convention that both e and f can be either finite or infinite, without distinguishing between different infinite cardinalities. With this convention, we have the following transitivity due to that of group index and field degree.

Proposition 14.6.3. *Let $K \subseteq L \subseteq L'$ be field extension, w' an extension of L' and w, v the restriction of w' to L' and L. Then*

$$e(w'/v) = e(w'/w)e(w/v), \quad f(w'/v) = f(w'/w)f(w/v).$$

Now, before we prove anything about the quantities e and f, we first provide some examples.

Example 14.6.4. Let (K, v) be a valued field with value group Γ_v and Γ a totally ordered group with $\Gamma_v \subseteq \Gamma$. Consider some t transcendental over K and any $\gamma \in \Gamma$. Define a valuation w on $K(t)$ with values in Γ via

$$w\Big(\sum_{i=0}^{n} a_i t^i\Big) = \min\{v(a_i) + i\gamma : 0 \le i \le n\}$$

for $f = \sum_{i=0}^{n} a_i t^i \in K[t]$ and extend w to all of $K(t)$. Then w is a well-defined valuation extending v with value group $\Gamma_w = \Gamma_v + \gamma\mathbb{Z}$.

The following inequality is fundamental for extension of valuations.

Proposition 14.6.5. *Let K be a field, L a extension of K of degree n, w a valuation on L and v its restriction to K. Choose $x_1, \dots, x_e \in L^\times$ and $y_1, \dots, y_f \in A_w$ such that*

(a) the values $w(x_1), \dots, v(x_e)$ are representatives of the distinct cosets of Γ_w/Γ_v.

(b) the residues $\bar{y}_1, \dots, \bar{y}_f \in \kappa_w$ are linearly independent over κ_v;

Then for all $a_{ij} \in K$, we have

$$w\Big(\sum_{ij} a_{ij} x_i y_j\Big) = \min_{ij}\{w(a_{ij} x_i y_j)\}$$

In particular, the products $x_i y_j$ are linearly independent over K.

Proof. Let $a_{ij} \in K$, not all zero, and $I \in \{1, \dots, e\}$ and $J \in \{1, \dots, f\}$ such that

$$w(a_{IJ} x_I) = \min_{ij}\{w(a_{ij} x_i)\}.$$

and observe first that $w(a_{IJ} x_I) < w(a_{ij} x_i)$ for all $i \neq I$ since otherwise

$$w(x_I) - w(x_i) = w(a_{ij}) - w(a_{IJ}) = v(a_{ij}/a_{IJ}) \in \Gamma_v,$$

which contradicts our assumption on x.

Next, write $z = \sum_{ij} a_{ij} x_i y_j$. Since $w(y_j) \ge 0$ for each j, for the sake of obtaining a contradiction, we assume that $w(z) > w(a_{IJ} x_I)$. Then $z(a_{IJ} x_I)^{-1} \in \mathfrak{m}_w$. Also, according to the previous paragraph we have $a_{ij} x_i (a_{IJ} x_I)^{-1} \in \mathfrak{m}_w$ for all $i \neq I$. Dividing everything by $a_{IJ} x_I$ one gets

$$\sum_j \frac{a_{Ij}}{a_{IJ}} y_j = \frac{z}{a_{IJ} x_I} - \sum_{j=1}^{f} \sum_{i \neq I} \frac{a_{ij} x_i}{a_{IJ} x_I} y_j \in \mathfrak{m}_w$$

which gives a relation $\sum_j \bar{a}_{Ij} (\bar{a}_{IJ})^{-1} \bar{y}_j = 0$, this contradicts the hypothesis made on y_j. □

Corollary 14.6.6. *Let K be a field, L a finite extension of K of degree n, w a valuation on L and v its restriction to K. Then the $e(w/v) f(w/v) \le n$. In particular, $e(w/v)$ and $f(w/v)$ are finite.*

Theorem 14.6.7. *Let K be a field, L an algebraic extension of K, w a valuation on L, v its restriction to K. Then Γ_w/Γ_v is torsion and κ_w/κ_v is algebraic.*

Proof. Pick $x \in L$ such that $w(x) = \gamma \in \Gamma_w$. If $L' = K(x)$ and v' is the restriction of w on L' then by Corollary 14.6.6, since L'/K is finite degree, the group $\Gamma_{v'}/\Gamma_v$ is finite, whence torsion. It then follows that Γ_w/Γ_v is torsion.

Similarly, for $x \in A_w$ we take L' and v' as above. It follows from Corollary 14.6.6 that the residue class field $\kappa_{v'}$ is a finite extension of κ_v. Therefore $\bar{x} \in \kappa_{v'} \subseteq \kappa_w$ is algebraic over κ_v. □

Corollary 14.6.8. *Let K be a field, L an algebraic extension of K, w a valuation on L, v its restriction to K. Then the map $\Delta \mapsto \Delta \cap \Gamma_v$ is a one-to-one correspondence between isolated subgroups of Γ_w and Γ_v. In particular,* $\operatorname{rank}(w) = \operatorname{rank}(v)$.

Proof. It is clear that $\Delta \cap \Gamma_v$ is an isolated subgroup, if Δ is. Now let $\Delta \subseteq \Gamma_v$ be an isolated subgroup and Δ' denote the set of $\alpha \in \Gamma_w$ such that there exists $\beta \in \Delta$ satisfying $-\beta \leq \alpha \leq \beta$; it is immediately verified that Δ' is an isolated subgroup of Γ_v with $\Delta' \cap \Delta = \Delta$ (since Δ is isolated); hence the mapping $\Delta \mapsto \Delta \cap \Gamma_v$ is surjective. Finally, let Δ_1 and Δ_2 be two isolated subgroups of Γ_w such that $\Delta := \Delta_1 \cap \Gamma_v = \Delta_2 \cap \Gamma_v$ and assume, for example, $\Delta_1 \subseteq \Delta_2$; then Δ_2/Γ_1 is a totally ordered group and is isomorphic to a quotient group of Δ_2/Δ which itselfis identified with a subgroup of Γ_w/Γ_v. Hence Δ_2/Δ_1 is a torsion group and therefore reduces to 0. □

Corollary 14.6.9. *Suppose that L is a finite extension of K. For w to be discrete, it is necessary and sufficient that v be discrete.*

Proof. If w is discrete, then Γ_v is isomorphic to a non-zero subgroup of $\mathbb{Z}$ and hence to $\mathbb{Z}$. Conversely, if v is discrete, Γ_v is isomorphic to $\mathbb{Z}$ and Γ_w/Γ_v is a finite group. Hence Γ_w is a finitely generated commutative group of rank 1 and torsion-free. Consequently it is isomorphic to $\mathbb{Z}$. □

14.6.2 Prolongations of a valuation

Given a valuation ring $A \subseteq K$, and an extension L/K, any valuation ring B of L dominating A is called a **prolongation** of A to L. Equivalently, if v is the valuation corresponding to K, then prolongations of A corresponds to extensions of v to L. In this part, we consider the connection bewteen these prolongations.

The following lemma will be used throughout this part, and it states that two distinct prolongations of A to an algebraic extension L/K are incomparable.

Lemma 14.6.10. *Suppose L/K is an algebraic extension of fields, A is a valuation ring of K, and B_1, B_2 are two prolongations of A to L. If $B_1 \subseteq B_2$, then $B_1 = B_2$.*

Proof. The valuation ring B_1 maps to a valuation ring $\bar{B}_1 = B_1/\mathfrak{m}_{B_2}$ of the residue field $\kappa_{B_2} = B_2/\mathfrak{m}_{B_2}$. Since B_1 is an extension of A, it follows that $\bar{B}_1$ is also an extension of κ_v. According to Theorem 14.6.7, κ_{B_2} is an algebraic extension of κ_v, so it follows that $\bar{B}_1$ is also a field. But $\bar{B}_1$ is a valuation ring of κ_{B_2}, so it follows that $\bar{B}_1 = \kappa_{B_2}$ whence $B_1 = B_2$. □

There may exist infinitely many valuation rings of L lying over A, of course. But sometimes, their number has a natural bound. This is the content of the next result.

Theorem 14.6.11. *Let L be algebraic over K and $[L : K]_s < \infty$. Let A be a valuation ring of K. Then the number n of all prolongations of A to L is finite, and $n \leq [L : K]_s$.*

Proof. Let $B_1, \ldots, B_n$ be the distinct prolongations of A to L, with maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$, respectively. Also, by Lemma 14.6.10 these prolongations are pairwise incomparable. Therefore, by Corollary 14.4.7 there exist $x_1, \ldots, x_n \in L$ such that for all $i, j \in \{1, \ldots, n\}$,

$$x_i - 1 \in \mathfrak{m}_i, \quad x_i \in \mathfrak{m}_j \text{ for } i \neq j.$$

If K has characteristic $p > 0$, pick k large enough to guarantee that $x_i^{p^k} \in K^s$, the separable closure of K in L. Then we claim that these n elements $x_i^{p^k}$ are lineraly independent over K. Consequently, $n \leq [K^s : K] = [L : K]_s$, and the result follows.

We shall prove the claim by contradiction. For $a_1, \ldots, a_n \in K$, not all zero, such that $\sum_{i=1}^n a_i x_i^{p^k} = 0$, pick j such that

$$v(a_j) = \min\{v(a_1), \ldots, v(a_n)\}.$$

Then $a_j \neq 0$ and we have

$$x_j^{p^k} = -\sum_{i \neq j} a_i x_i^{p^k} \in \mathfrak{m}_j.$$

Since this would imply $x_j \in \mathfrak{m}_j$ and hence $1 \in \mathfrak{m}_j$, we get the desired contradiction. □

Corollary 14.6.12. *If the extension L/K is purely inseparable, then every valuation ring of K has a unique prolongation to L.*

With Theorem 14.6.11 in hand, we now classifies all prolongations of a given valuation ring to L: they corresponds to maximal ideals of the integral closure of A in L.

Theorem 14.6.13. *Let L be an algebraic extension of a field K, A be a valuation ring of K, and R the integral closure of A in L.*

(a) If B is a prolongation of A to L then $\mathfrak{m} = \mathfrak{m}_B \cap R$ is a maximal ideal of R.

(b) If $\mathfrak{m}$ is a maximal ideal of R then $R_\mathfrak{m}$ is a prolongation of A to L.

(c) The map $B \mapsto \mathfrak{m}_B \cap R$ gives a one-to-one correspondence between maximal ideals of R and prolongations of A to L, and its inverse is given by $\mathfrak{m} \mapsto R_\mathfrak{m}$.

Proof. Note that any prolongation B of A to L must contains R, by Theorem 14.1.8. Since $\mathfrak{m}_B$ is maximal in B, $\mathfrak{m}$ is also maximal in R. Conversely, since a contraction of maximal ideal is maximal, we see $R_\mathfrak{m}$ is a prolongation of A for every maximal ideal $\mathfrak{m}$ in R.

In remains to prove that, for a prolongation B of A to L we have $B = R_\mathfrak{m}$, where $\mathfrak{m} = \mathfrak{m}_B \cap R$. The inclusion $R_\mathfrak{m} \subseteq B$ is clear. We first consider the case where the extension L/K is finite. In this case, there are finitely many prolongations of A to L by Theorem 14.6.11, say $B_1, \ldots, B_n$ with maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$. Then by Proposition 14.4.5 we have $B_i = R_{\mathfrak{m}_i}$, where $\mathfrak{m}_i = \mathfrak{m}_{B_i} \cap R$, whence the claim holds in this case.

Now consider the general case. Let L' be a subfield of L such that L'/K is finite. Then we see $R' = R \cap L'$ is the integral closure of A in L' and $B' = B \cap L'$ is a prolongation of A

to L' with maximal ideal $\mathfrak{m}_{B'} = \mathfrak{m}_B \cap L'$. By the argument above, we get $B' = R'_{\mathfrak{m}'}$, where $\mathfrak{m}' = \mathfrak{m} \cap L' = \mathfrak{m}_{B'} \cap R'$. Since the subfield L' is arbitrary, it follows that $B = R_{\mathfrak{m}}$. □

Next we shall consider the set of all prolongations of a fixed valuation ring of a field K to normal extensions of K. It turn out that the automorphism group $\mathrm{Aut}(L/K)$ plays an important rule.

Theorem 14.6.14. *Suppose L/K is a normal extension of fields, with $G = \mathrm{Aut}(L/K)$. Suppose A is a valuation ring of K, and B_1 and B_2 are valuation rings in L extending A. Then B_1 and B_2 are conjugate over K, i.e., there exists $\sigma \in G$ with $\sigma(B_1) = B_2$.*

Proof. First, split the extension L/K into the steps $K \subseteq K^s \subseteq L$. Corollary 14.6.12 implies that every extension of A to K^s has just one prolongation to L. Furthermore, $\mathrm{Aut}(K^s/K)$ and G can be canonically identified. Therefore, we see that it is enough to consider the case where L is separable over K.

We may assume $[L : K] < \infty$, and the general case follows by considering the compactness of Galois groups. In this case let

$$H_1 = \{\sigma \in G : \sigma(B_1) = B_1\}, \quad H_2 = \{\tau \in G : \tau(B_2) = B_2\}.$$

Then H_1 and H_2 are subgroups of G. Moreover, for every $\sigma \in H_1$, it follows that $\sigma(\mathfrak{m}_1) = \mathfrak{m}_1$, for the maximal ideal of B_1. Indeed, it is enough to observe that $\sigma(\mathfrak{m}_1)$ must be the maximal ideal of $\sigma(B_1)$. Analogously for the maximal ideal $\mathfrak{m}_2$ of B_2, it follows that $\tau(\mathfrak{m}_2) = \mathfrak{m}_2$ for all $\tau \in H_2$. Next write G as disjoint unions of cosets of H_1 and H_2, respectively:

$$G = \bigcup_{i=1}^{n} H_1\sigma_i^{-1}, \quad G = \bigcup_{k=1}^{m} H_2\tau_k^{-1}.$$

Suppose now, for the sake of contradiction, that $\sigma_i(B_1) \not\subseteq \tau_k(B_2)$ and $\tau_k(B_2) \not\subseteq B_1$ for all i, k. Since $\sigma_1^{-1}, \dots, \sigma_n^{-1}$ is a complete set of representatives of cosets of H_1, for all $i \neq j$, $\sigma_i(B_1) \not\subseteq \sigma_j(B_1)$. Similarly, $\tau_k(H_2) \not\subseteq \tau_l(B_2)$ for every $k \neq l$. Now take

$$C = \bigcap_{i=1}^{n} \sigma_i(H_1) \cap \bigcap_{k=1}^{m} \tau_j(H_2).$$

According to Corollary 14.4.7, there exists an $x \in C$ such that, for each i, k,

$$x - 1 \in \sigma_i(\mathfrak{m}_1), \quad x \in \tau_k(\mathfrak{m}_2)$$

As a consequence, for $\sigma \in G$, writing $\sigma = \rho\sigma_i^{-1}$ and $\rho \in H_1$, it follows that

$$\sigma(x - 1) \in \rho\sigma_i^{-1}(\sigma_i(\mathfrak{m}_1)) = \rho(\mathfrak{m}_1) = \mathfrak{m}_1.$$

Analogously, $\sigma(x) \in \mathfrak{m}_2$ for every $\sigma \in G$. Taking norms, it then follows

$$N_{L/K}(a) = \prod_{\sigma \in G} \sigma(a) \in (\mathfrak{m}_1 + 1) \cap K = \mathfrak{m} + 1$$

and

$$N_{L/K}(a) = \prod_{\sigma \in G} \sigma(a) \in \mathfrak{m}_2 \cap K = \mathfrak{m}.$$

This contradiction implies $\sigma_i(\mathfrak{m}_1) \subseteq \tau_j(\mathfrak{m}_2)$ or $\tau_j(\mathfrak{m}_2) \subseteq \sigma_i(\mathfrak{m}_1)$. Thus the claim holds in this case by Lemma 14.6.10. □

Now, since we now all prolongations of A are conjugate under $\mathrm{Aut}(L/K)$, we are ready to prove the following theorem.

Theorem 14.6.15. *Let L be a normal extension of a field K, A a valuation ring of K, and B a prolongation of A to L. Let v and w be valuations corresponding to A and B.*

(a) For $\sigma \in \mathrm{Aut}(L/K)$, the map $w \circ \sigma$ is the unique valuation of L that corresponds to $\sigma^{-1}(B)$. In particular, if $\sigma(B) = B$, then $w \circ \sigma = w$.

(b) κ_B is a normal extension of κ_v.

(c) The map $x \mapsto \overline{\sigma(x)}$ induces a K-isomorphism from $\sigma^{-1}(B)/\sigma^{-1}(\mathfrak{m}_B)$ onto κ_B. In particular, if $\sigma(B) = B$ then $\bar{\sigma} \in \mathrm{Aut}(\kappa_B/\kappa_v)$.

(d) For every $\sigma \in \mathrm{Aut}(L/K)$ we have $e(\sigma^{-1}(B)/A) = e(B/A)$ and $f(\sigma^{-1}(B)/A) = f(B/A)$.

Proof. Part (a), (b), (d) are easily verified, so we concentrate on (b). Let $\bar{f} \in \kappa_v[X]$ be an irreducible polynomial with a root $\bar{x} \in \kappa_v$. Let R be the integral closure of A in L and write $\mathfrak{m} = \mathfrak{m}_B \cap R$. By Theorem 14.6.13, we have $B = R_{\mathfrak{m}}$. Observe next that R is fixed by $\mathrm{Aut}(L/K)$. Now let $x \in R$ be a preimage of $\bar{x}$, and let $g \in A[X]$ be the minimal polynomial of x over K. Since L/K is normal, g splits completely as $g(X) = \prod_{i=1}^{n}(X - x_i)$ with $x_i \in R$. From $\bar{g}(\bar{x}) = 0$, it follows that $\bar{f}$ divides $\bar{g}$. But $\bar{g} = \prod_{i=1}^{n}(X - \bar{x}_i)$ in κ_B, hence $\bar{f}$ has all its roots in κ_B, proving (b). □

14.6.3 Henselian fields

In this part we introduce the basic concepts of a Henselian field. These will be used when we establish the structure theorem about extension of valuations.

We have seen that every rank-one valuation v of a complete field K has a unique prolongation to each algebraic extension of K. By Corollary 14.6.12, also every valuation of a separably closed field K has this property. Valuation rings, or valuations, with this property are very important. They are the so-called "Henselian" valuation rings. We shall see that they are the suitable substitute for rank-one valuation rings of complete fields. In particular, they are the valuation rings for which Hensel's Lemma holds.

A valued field (K, v) is called **Henselian** if v has a unique extension to every algebraic extension L of K. We see from the definition that the property of being Henselian is hereditary. Let $\bar{K}$ be an algebraic closure and K^s be the separable closure of K in $\bar{K}$. We then have the following apparently easier characterization of Henselian valuations.

Proposition 14.6.16. *A valued field (K, v) is Henselian if and only if it extends uniquely to K^s.*

Proof. By definition, if (K, v) is Henselian then v extends uniquely to K^s. Conversely, take an algebraic extension L of K. By Corollary 14.6.12, every extension of v to $L \cap K^s$ has an extension to K^s. By assumption, v extends uniquely to $L \cap K^s$, so v has a unique prolongation to L. □

The next theorem will highlight the importance of Henselian valuation rings. Comparing with completions we see that rank-one complete valuation rings are a particular case of Henselian valuation rings. Before stating the theorem we need a little preparation.

Let $v : K^\times \to \Gamma$ be a valuation of the field K. The **Gauss extension** w of v to the rational function field $K(X)$ is given by

$$w(\sum_{i=0}^{n} a_i X^i) = \min_i \{v(a_i)\}.$$

We say a polynomial is primitive if $w(f) = 0$. The following properties of primitive polynomials hold, which can be seen as a generalization of the well known Gauss's lemma.

Lemma 14.6.17. *Let $v : K^\times \to \Gamma$ be a valuation with valuations ring A.*

(a) If two polynomials f and g are primitive, then so is their product fg.

(b) Every $f \in K[X]$ admits a decomposition $f = a\tilde{f}$ with $a \in K$ and $\tilde{f} \in K[X]$ primitive.

(c) If $f \in A[X]$ decomposes as $f = \prod_{i=1}^m g_i$ with irreducible factors $g_1, \dots, g_m \in K[X]$, then there are $h_1, \dots, h_m \in A[X]$, irreducible in $K[X]$, such that $f = \prod_{i=1}^m h_i$.

Proof. Part (a) and (b) are easy to prove. To see (c), write $f = a\tilde{f}$ and $g_i = b_i \tilde{g}_i$, where $a, b_1, \dots, b_m \in K$ and $\tilde{f}, \tilde{g}_1, \dots, \tilde{g}_m$ are primitive. Then

$$v(a) = w(f) = \sum_{i=1}^{n} w(g_i) = w(b_1 \cdots b_m).$$

Since $f \in A[X]$, we have $v(a) \geq 0$, whence $b_1 \cdots b_m \in A$. Define $h_1 = b_1 \cdots b_m \tilde{g}_1$ and $h_i = \tilde{g}_i$, we see the desired decomposition. □

Theorem 14.6.18. *Let (K, v) be a valued field with valuation ring A and $\mathfrak{m}$ its maximal ideal. The following statements are equivalent:*

(i) (K, v) is Henselian.

(ii) For each irreducible polynomial $f \in A[X]$ with $\bar{f} \notin (\kappa_v)[X]$, there exists $g \in A[X]$ such that $\bar{g}$ is irreducible in $(\kappa_v)[X]$ and $\bar{f} = \bar{g}^s$, for some $s \geq 1$.

(iii) Let $f, g, h \in A[X]$ satisfy $\bar{f} = \bar{g}\bar{h}$, with $\bar{g}, \bar{h}$ relatively prime in $(\kappa_v)[X]$. Then there exist $g_1, h_1 \in A[X]$ such that

$$f = g_1 h_1, \quad \bar{g}_1 = \bar{g}, \bar{h}_1 = \bar{h}, \quad \deg g_1 = \deg g, \deg h_1 = \deg h.$$

(iv) For each $f \in A[X]$ and $a \in A$ with $\bar{f}(\bar{a}) = 0$ and $\bar{f}'(\bar{a}) \neq 0$, there exists an $\alpha \in A$ with $f(\alpha) = 0$ and $\bar{\alpha} = \bar{a}$.

(v) For each $f \in A[X]$ and $a \in A$ with $v(f(a)) > 2v(f'(a))$, there exists an $\alpha \in A$ with $f(\alpha) = 0$ and $v(a - \alpha) > v(f'(\alpha))$.

(vi) Every polynomial $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in A[X]$ with $a_{n-1} \in\notin \mathfrak{m}$ and $a_{n-2}, \dots, a_0 \in \mathfrak{m}$ has a zero in K.

(vii) Every polynomial $f(X) = X^n + X^{n-1} + \cdots + a_1X + a_0 \in A[X]$ with $a_{n-2}, \ldots, a_0 \in \mathfrak{m}$ has a zero in K.

Proof. Let (K, v) be Henselian, denote by w the unique extension of v to $\overline{K}$, the algebraic closure of K. Write B the valuation ring of w and $\mathfrak{m}_B$ for the maximal ideal, and κ_B for the residue class field of B. Since w is the unique extension of v, for every K-automorphism σ of $\overline{K}$ we have $\sigma(B) = B$ and $\sigma(\mathfrak{m}_B) = \mathfrak{m}_B$. Let f an be irreducible polynomial $f \in A[X]$ with $\bar{f} \notin (\kappa_v)[X]$. Write

$$f(X) = \prod_{i=1}^{n}(aX - x_j)$$

where $a, x_1, \ldots, x_n \in K$ and a is an n-th root of the leading coefficient of f. Then $a \in B$ since $w(a) = v(a)/n \geq 0$. Also, $(-1)^n x_1 \ldots x_n = f(0) \in A$.

The roots $x_1/a, \ldots, x_n/a$ of f are all K-conjugate, and w is invariant under $\mathrm{Aut}(\overline{K}/K)$. Consequently, there exists $\gamma \in \Gamma_w$ such that $w(x_j/a) = \gamma$ for all j. So, for $\delta = \gamma + w(a)$, we have that $w(x_j) = \delta$ for each j. Therefore, $x_1, \ldots, x_n \in A$ implies $\delta \geq 0$, and thus $x_1, \ldots, x_n \in \mathfrak{m}_B$ or $x_1, \ldots, x_n \in B - \mathfrak{m}_B$.

In the first case, $\bar{f} = (\bar{a}X)^n$ and the claim (b) follows. In the second case, we obtain

$$\bar{f} = \prod_{i=1}^{n}(\bar{a}X - \bar{x}_i)$$

with $\bar{x}_i \neq 0$. Since $\bar{f} \notin (\kappa_v)[X]$, we also have $\bar{a} \neq 0$. For the sake of seeking a contradiction, let us assume that $\bar{f} = \bar{g}\bar{h}$ for some relatively prime polynomials $\bar{g}$ and $\bar{h}$ with $g, h \in A[X]$. Let $\bar{x_i}/a$ be a root of $\bar{g}$ and take some $x_j \neq x_i$ such that $\bar{x_j}/a$ is a root of $\bar{h}$. Hence $g(x_i/a) \in \mathfrak{m}_A$ and $h(x_j/a) \in \mathfrak{m}_A$. Take $\sigma \in \mathrm{Aut}(\overline{K}/K)$ such that $\sigma(x_i/a) = x_j/a$. Then

$$g(x_j/a) = g(\sigma(x_i/a)) = \sigma(g(x_i/a)) \in \sigma(\mathfrak{m}_B) = \mathfrak{m}_B$$

which means $\bar{x_j}/a$ is also a root of $\bar{g}$, contradiction. This proves $(i) \Rightarrow (ii)$.

Now assume (ii), and let $f = gh$ with $f, g, h \in A[X]$ and g, h coprime. By Lemma 14.6.17, let $f = \prod_{i=1}^{m} g_i$ be a factorization of f with irreducible factors $g_1, \ldots, g_m \in A[X]$. By condition (ii), for every i, either $g_i \in K$ or there exists $p_i \in A[X]$ such that p_i is irreducible and $g_i = p_i^{t_i}$ for some $t_i \geq 1$. Clearly, we may assume that p_i has no non-zero coefficient in $\mathfrak{m}_A$. Renumbering the polynomials $g_1, \ldots, g_m$, we may assume that

$$\bar{g} = \bar{a}\prod_{i=1}^{k}\bar{p}_i^{t_i}, \quad \bar{b} = \bar{h}\prod_{i=k+1}^{\ell}\bar{p}_i^{t_i}, \quad \bar{c} = \prod_{i=\ell+1}^{m}\bar{p}_i^{t_i}$$

for some $a, b, c \in A - \mathfrak{m}$, since $\bar{g}$ and $\bar{h}$ are coprime. Define now

$$g_1 = a\prod_{i=1}^{k}p_i^{t_i}, \quad h_1 = \Big(b\prod_{i=k+1}^{\ell}p_i^{t_i}\Big)\Big(c^{-1}\prod_{i=\ell+1}^{m}p_i^{t_i}\Big)$$

then the polynomials g_1 and h_1 satisfies the requirements in (iii), so we have shown $(ii) \Rightarrow (iii)$.

Next, we will deduce (iv) from (iii). If $f \in A[X]$ and $a \in A$ with $\bar{f}(\bar{a}) = 0$ and $\bar{f}'(\bar{a}) \neq 0$, set $g(X) = X - a$ and $\bar{h} = \bar{f}/\bar{g}$, then $\bar{f} = \bar{g}\bar{h}$. Since $\bar{f}'(\bar{a}) \neq 0$, $\bar{g}$ and $\bar{h}$ are coprime, so by condition

(iii) there exist polynomials g_1 and h_2 such that

$$f = g_1 h_1, \quad \bar{g}_1 = \bar{g} = X - \bar{a}, \bar{h}_1 = \bar{h}, \quad \deg g_1 = \deg g = 1, \deg h_1 = \deg h.$$

It then follows that $g_1 = u(X - b)$ for some $u \in A^\times$ and $b \in A$, with $\bar{u} = 1$ and $\bar{b} = \bar{a}$. Clearly $f(b) = 0$, so this proves (iv).

For each $f \in A[X]$ and $a \in A$ with $v(f(a)) > 2v(f'(a))$, we have $f'(a) \neq 0$. Now by a simple computation we know $f(a - X) = f(a) - f'(a)X + X^2 g(X)$ for some $g \in A[X]$, and by a change of variable $X = f'(a)Y$ we can define

$$h(Y) := \frac{f(a - f'(a)Y)}{f'(a)^2} = \frac{f(a)}{f'(a)^2} - Y + Y^2 g(f'(a)Y).$$

Since $v(f(a)) > 2v(f'(a))$ we have $h \in A[Y]$. Note that $f(a)/f'(a)^2 \in \mathfrak{m}_A$, so $\bar{h}$ has a simple root $\bar{0}$ in κ_v. If condition (iv) holds, this will give a root $b \in \mathfrak{m}$ of h. Then by the construction of h, $\alpha = a - f'(a)b$ will a root of f. Moreover, since $v(b) > 0$, we have $v(a - \alpha) > v(f'(a))$. This shows $(iv) \Rightarrow (v)$.

The implication $(v) \Rightarrow (vi)$ is immediate. In fact, let $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$ be as in (vi). Then

$$\bar{f}(X) = X^n + \bar{a}_{n-1}X^{n-1} = X^{n-1}(X + \bar{a}_{n-1}).$$

Hence $-\bar{a}_{n-1}$ is a nonzero simple zero of $\bar{f}$. In particular, $f(-a_{n-1}) > 0$ and $f'(-a_{n-1}) \in A - \mathfrak{m}$. This means

$$v(f(-a_{n-1})) > 0 = 2v(f'(-a_{n-1}))$$

thus f has a root in A, by (v).

It is clear that $(vi) \Rightarrow (vii)$. Conversely, if (vii) holds and $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$ is a polynomial as in (vi), then the changing $X = a_{n-1}Y$ and dividing by a_{n-1}^n, we obtain

$$g(Y) = Y^n + Y^{n-1} + \frac{a_{n-2}}{a_{n-1}^2}Y^{n-2} + \cdots + \frac{a_1}{a_{n-1}^n}Y + \frac{a_0}{a_{n-1}^n}.$$

It is clear that a root of $g(Y)$ gives a root of f, so (vi) and (vii) are equivalent.

Finally, we prove $(vii) \Rightarrow (i)$. Suppose (K, v) were not henselian. Then there would be a finite Galois extension L/K with Galois group $\mathrm{Gal}(L/K)$ in which v has more than one extension. Let B be a prolongation of A to L and set $H = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(B) = B\}$. As B is not the only prolongation of A to L, the group H is a proper subgroup of $\mathrm{Gal}(L/K)$, and thus the fixed field $L' := L^H$ of H is a proper extension of K. Let $B_1, \ldots, B_n$ be all conjugates of B in L with maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ and consider the subring

$$R = \bigcap_{i=1}^{m} (B_i \cap L')$$

of L'. By Corollary 14.4.7, we find $\alpha \in R$ such that $\alpha - 1 \in \mathfrak{m}_1$ and $\alpha \in \mathfrak{m}_i$ for $i = 2, \ldots, n$. Since $n > 1$, α cannot lie in K, so its minimal polynomial

$$f = \min(\alpha, K) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$$

cannot have a zero in K. However, if $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_n$ are conjugates of α in L, we have

$$a_{n-i} = (-1)^i e_i(\alpha_1, \dots, \alpha_n), \tag{6.3.1}$$

where e_i is the i-th symmetric function. For each $i \geq 2$, we have $\alpha_i \neq \alpha$, so $\alpha_i = \tau(\alpha)$ for some $\tau \in \mathrm{Gal}(L/K) \setminus H$ (note that $\alpha \in L'$). Hence $\tau^{-1}(B) = B_j$ for some $j \geq 2$. Since by the approximation condition we have $\alpha \in \mathfrak{m}_j = \tau^{-1}(\mathfrak{m}_1)$, we then get $\alpha_i = \tau(\alpha) \in \mathfrak{m}_1$. By (6.3.1), this implies $1 + a_{n-1} \in \mathfrak{m}_1$ and $a_{n-2}, \dots, a_1, a_0 \in \mathfrak{m}_1$. Thus by (vi) the polynomial f has a root in K, contradiction. □

Corollary 14.6.19. *Let (K, w) be a composition of valuations (K, v) and $(\kappa_v, \bar{v})$. Then (K, w) is Henselian if and only if both (K, v) and $(\kappa_v, \bar{v})$ are Henselian.*

Proof. Suppose (K, w) is Henselian. Then (K, v) is also Henselian, using $\mathfrak{m}_v \subseteq \mathfrak{m}_w \subseteq A_w \subseteq A_v$ and Theorem 14.6.18. To show that $(\kappa_v, \bar{v})$ is Henselian, let $\bar{f} = X^n + X^{n-1} + \cdots + \bar{a}_0$, with $a_i \in \mathfrak{m}_{\bar{v}}$ we must show that $\bar{f}$ has a zero in κ_v (again using Theorem 14.6.18). The polynomial

$$f = X^n + X^{n-1} + \cdots + a_0 \in A_w[X]$$

has a zero $x \in A_w$ (yet again by Theorem 14.6.18), since $a_i \in \mathfrak{m}_v \subseteq \mathfrak{m}_w$); therefore $\bar{x} \in A_{\bar{v}}$ is a zero of $\bar{f}$.

Now we prove the converse. Let $f = X_n + a_{n-1}X^{n-1} \cdots + a_0 \in A_w[X]$, and suppose that $\bar{f}$ has a simple zero in the residue field κ_w. As κ_w is also the residue field of $\bar{v}$, and $\bar{v}$ is Henselian, this simple zero of $\bar{f}$ lifts to κ_v. As the field (K, v) is also Henselian, the zero (which is again simple) can be lifted further to K. □

Let (K, v) be a valued field. Assume L/K is a Galois extension. We then say (K, v) is ***L*-Henselian** if v has exactly one extension to L. By taking $L = K^s$, the separable closure of K, we return to our usual definition of Henselian field. Just as Theorem 14.6.18, we can also obtain many equivalent characterizations of L-Henselian fields. One need only go through the proof of Theorem 14.6.18 and restrict consideration to those polynomials f that split in L. The corresponding condition for the Galois extension K^s/K is always satisfied, hence, of course, was not mentioned in Theorem 14.6.18.

14.6.4 The fundamental inequality

Definition 14.6.20. *Let K be a field, v a valuation on K and L an extension of K. A family $(w_i)_{i \in I}$ of valuations on L which extend v and such that every valuation on L extending v is equivalent to a unique w_i is called a* ***complete system of extensions of v to L****.*

We have already proved that the completion is an immediate extension of a given valued field. Now we go deeper to this result and consider the case of a extension of valued fields.

Proposition 14.6.21. *Let (K, v) be a valued field and $(\widehat{K}, \hat{v})$ its completion of K. Let L be a finite extension of K of degree n.*

(a) Let w be a valuation on L extending v and $(\widehat{L}_w, \hat{w})$ denote the completion of (L, w). Identity $\widehat{K}$ with the closure of K in $\widehat{L}_w$, then

$$e(\hat{w}/\hat{v}) = e(w/v), \quad f(\hat{w}/\hat{v}) = f(w/v), \quad e(w/v)f(w/v) \leq [\widehat{L}_w : \widehat{K}] \leq n.$$

(b) *Every set of pairwise independent valuations on L extending a nontrivial valuation v is finite. Let $(w_i)_{1\le i\le s}$ denote pairwise independent valuations on L extending v such that every valuation on L extending v is dependent on one of the w_i; let L_i be the field L with the topology defined by w_i and $\widehat{L}_i$ its completion. Then the canonical mapping*

$$\phi : \widehat{K} \otimes_K L \to \prod_{i=1}^{s} \widehat{L}_i$$

(extending by continuity the diagonal mapping $L \to \prod_{i=1}^{s} L_i$) is surjective, its kernel is the Jacobson radical of $\widehat{K} \otimes_K L$. In particular, $\sum_{i=1}^{s}[\widehat{L}_i : \widehat{K}] \le n$.

Proof. Let us first prove (a). Suppose that v is nontrivial. As v and $\hat{v}$ (resp. w and $\hat{w}$) have the same order group and the same residue field, we see $e(\hat{w}/\hat{v}) = e(w/v)$ and $e(\hat{w}/\hat{v}) = e(w/v)$. In particular, $e(w/v)f(w/v) \le [\widehat{L}_w : \widehat{K}]$ by Corollary 14.6.6. Finally the vector sub-$\widehat{K}$-space of $\widehat{L}_w$ generated by L is closed in $\widehat{L}_w$ (by Corollary 14.4.18) and also dense in $\widehat{L}_w$ so it equals to $\widehat{L}_w$. This shows $[\widehat{L}_w : \widehat{K}] \le n$ and completes the proof of (a).

We now pass to (b). We may still assume that v is not trivial. Let $(w_1, \dots, w_r)$ be any finite family of pairwise independent valuations on L extending v. The image of L in $\prod_{i=1}^{r} L_i$ under the diagonal mapping is dense by the approximation theorem, and $\prod_i L_i$ is dense in $\prod_{i=1}^{r} \widehat{L}_i$. Hence the canonical Image of $\widehat{K} \otimes_K L$ in $\prod_{i=1}^{r} \widehat{L}_i$ is dense. On the other hand this image is a vector sub-$\widehat{K}$-space of $\prod_{i=1}^{r} \widehat{L}_i$; as $\prod_{i=1}^{r} \widehat{L}_i$ is of finite dimension over $\widehat{K}$ by (a), every subspace of $\prod_{i=1}^{r} \widehat{L}_i$ is closed. Thus the image of $\widehat{K} \otimes_K L$ is closed and equal to $\prod_{i=1}^{r} \widehat{L}_i$. As the dimension of $K \otimes_K L$ over K is n, we see $\sum_{i=1}^{s}[\widehat{L}_i : \widehat{K}] \le n$. This shows in particular that the integer r is bounded above by n and shows the first assertion of (b).

We now take $(w_1, \dots, w_s)$ as in the statement. The fact that

$$\phi : \widehat{K} \otimes_K L \to \prod_{i=1}^{s} \widehat{L}_i$$

is suriective have already been shown. It remains to verify that the kernel of ϕ is the Jacobsen radical J of $K \otimes_K L$. As $\prod_{i=1}^{s} \widehat{L}_i$ is semi-simple, we see $J \subseteq \ker \phi$. On the other hand, for every maximal ideal $\mathfrak{m}$ of $\widehat{K} \otimes_K L$, the quotient field $L(\mathfrak{m}) = (\widehat{K} \otimes_K L)/\mathfrak{m}$ is a composite extension of $\widehat{K}$ and L over K (Proposition 9.1.94). There exists a valuation μ on $L(\mathfrak{m})$ extending $\hat{v}$; the restriction w of μ to L then extends v. As $[L(\mathfrak{m}) : \widehat{K}]$ is finite, $L(\mathfrak{m})$ is complete with respect to μ (Proposition 14.4.17). Now the closure of L in $L(\mathfrak{m})$ is a field containing $\widehat{K}$ and L and hence is equal to $L(\mathfrak{m})$. Consequently $L(\mathfrak{m})$ is identified with the completion $\widehat{L}_w$ and $\mathfrak{m}$ is the kemel of the canonical mapping of $\widehat{K} \otimes_K L$ onto $\widehat{L}_w$. Now, by hypothesis, there exists an index i such that w and w_i are dependent; whence $\widehat{L}_w = \widehat{L}_i$. Thus $\ker \phi \subseteq \mathfrak{m}$, which proves that $\ker \phi \subseteq J$ and completes the proof. □

Corollary 14.6.22. *If K is complete with respect to v and v is nontrivial, two valuations on L extending v are dependent.*

Proof. In this case we have $\widehat{K} \otimes_K L = K \otimes_K L = L$, so the claim follows by Proposition 14.6.21(b). □

Corollary 14.6.23. *If the extension L/K or $\widehat{K}/K$ is separable then the map ϕ is an isomorphism.*

Proof. In this case the Jacobsen radical of $\widehat{K} \otimes_K L$ is zero. □

Theorem 14.6.24 (The Fundamental Inequality). *Let (K, v) be a valued field and L a finite extension of K of degree n. Then every complete system $(w_i)_{i\in I}$ of extensions of v to L is finite and we have*

$$\sum_{i\in I} e(w_i/v)f(w_i/v) \leq n.$$

Proof. Since the theorem is trivial if v is trivial, we shall assume that v is nontrivial. Let $(w_1, \dots, w_s)$ be any finite family of valuations on L extending v, no two of which are equivalent. We shall show that $\sum_{i=1}^{s} e(w_i/v)f(w_i/v) \leq n$. This will prove the theorem.

We argue by induction on s and suppose therefore that the inequality has been established for the case of valuations of number smaller than s. We distinguish two cases.

Suppose that there exist at least two independent valuations of w_i. Then there exists a partition $[1, s] = I_1 \cup \cdots \cup I_t$ of $[1, s]$ such that:

(i) for w_i and w_j to be dependent, it is necessary and suflicient that i and j belong to the same I_k;

(ii) $|I_k| < s$ for all k.

We choose in each I_k an index i_k. Let $\widehat{L}_k$ denote the completion of L with respect to v_{i_k} and $n_k = [\widehat{L}_k : \widehat{K}]$. For all $i \in I_k$, w_i defines on L the same topology as w_{i_k} and hence may be extended to a valuation $\hat{w}_i$ on $\widehat{L}_k$ whose restriction to $\widehat{K}$ is $\hat{v}$. Since no two of the w_i for $i \in I_k$ are equivalent, the same is true of the $\hat{w}_i$. The induction hypothesis applied to the ordered pair $(\widehat{K}, \widehat{L}_k)$ shows

$$\sum_{i\in I_k} e(w_i/v)f(w_i/v) \leq n_k.$$

As $\sum_k n_k \leq n$ by Proposition 14.6.21, we see the claim follows in this case.

We now pass to the case where any two of the w_i are dependent. In this case there is a nontrivial valuation w' of L such that $w_i = w \circ \bar{w}_i$, where $\bar{w}_i$ is a valuation of the residue field $\kappa_{w'}$. Denote by v' the restriction of w' to K, then v is also a composition of v', say $v = v' \circ \bar{v}$, where $\bar{v}$ is a valuation of $\kappa_{v'}$. If we choose w such that the valuation rings A_{w_i} generates $A_{w'}$, then the valuation rings of $\bar{w}_i$ generates $\kappa_{w'}$, so that they are not all dependent. From the first part of the proof, we then have

$$\sum_{i=1}^{s} e(\bar{w}_i/\bar{v})f(\bar{w}_i/\bar{v}) \leq [\kappa_{w'} : \kappa_{v'}] = f(w'/v')$$

and hence

$$\sum_{i=1}^{s} e(w'/v')e(\bar{w}_i/\bar{v})f(\bar{w}_i/\bar{v}) \leq e(w'/v')f(w'/v') \leq n.$$

Now it suffices to prove that

$$f(w_i/v) = f(\bar{w}_i/\bar{v}), \quad e(w'/v')e(\bar{w}_i/\bar{v}) = e(w_i/v). \tag{6.4.1}$$

For this, we note that v and $\bar{v}$ (resp. w_i and $\bar{w}_i$) have the same residue field, so the first equality holds. For the second there is, by Proposition 14.3.3 and Proposition 14.3.1, the following

commutative diagram, where the rows are exact sequences and the vertical arrows represent canonical injections:

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \Gamma_{\bar{v}} \arrow[r] \arrow[d] & \Gamma_v \arrow[r] \arrow[d] & \Gamma_{v'} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \Gamma_{\bar{w}_i} \arrow[r] \arrow[d] & \Gamma_{w_i} \arrow[r] \arrow[d] & \Gamma_{w'} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \Gamma_{\bar{w}_i}/\Gamma_{\bar{v}} \arrow[r] \arrow[d] & \Gamma_{w_i}/\Gamma_v \arrow[r] \arrow[d] & \Gamma_{w'}/\Gamma_{v'} \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

From this we see the second equality is valid, therefore the proof is completed. □

Now we preceed a step further to investigate when the equality in Theorem 14.6.24 holds. For this, we need the following definition.

Definition 14.6.25. *Let Γ be a totally ordered group. A subset of Γ is called **major** if the relations $\alpha \in M$, $\beta \in \Gamma$ and $\beta \geq \alpha$ imply $\beta \in M$.*

Example 14.6.26. Let Δ be a isolated subgroup of a totally ordered group Γ. Then the set

$$M = \{\alpha \in \Gamma : \alpha \geq \gamma \text{ for all } \gamma \in \Delta\}$$

is a major subset of Γ.

Let K be a field, v a valuation on K, and A the ring of v and Γ the order group of v. For every major subset $M \subseteq G$, let $\mathfrak{a}(M)$ be the set of $x \in K$ such that $v(x) \in M \cup \{\infty\}$. Clarly $\mathfrak{a}(M)$ is a sub-A-module of K.

Proposition 14.6.27. *The mapping $M \mapsto \mathfrak{a}(M)$ is an increasing bijection of the set of major subsets of Γ onto the set of sub-A-modules of K.*

Proof. Let $\mathfrak{b}$ be a sub-A-module of K. The set of $v(x)$ for $x \in \mathfrak{b} \setminus \{0\}$ is a major subset $M(\mathfrak{b})$ of Γ. We now show the following equations are satisfied:

(a) $M(\mathfrak{a}(N)) = N$ for every major subset N of Γ;

(b) $\mathfrak{a}(M(\mathfrak{b})) = \mathfrak{b}$ for every sub-A-module $\mathfrak{b}$ of K.

Part (a) is easy, since, for all $\alpha \in N$, there exists $x \in K$ such that $v(x) = \alpha$. Then obviously $\mathfrak{b} \subseteq \mathfrak{a}(M(\mathfrak{b}))$; conversely, let $x \in \mathfrak{a}(M(\mathfrak{b}))$ and suppose $x \neq 0$, then $v(x) \in M(\mathfrak{b})$ and therefore there exists $y \in \mathfrak{b}$ such that $v(x) = v(y)$; whence $x = uy$ where $v(u) = 0$, which proves that $x \in \mathfrak{b}$ and completes the proof. □

Corollary 14.6.28. *Let Γ_+ be the set of positive elements in Γ. The mapping $M \mapsto \mathfrak{a}(M)$ is a bijection of the set of major subsets of Γ_+ onto the set of ideals of A.*

Proof. As $A = \mathfrak{a}(\Gamma_+)$, $\mathfrak{a}(M) \subseteq A$ is equivalent to $M \subseteq \Gamma_+$. □

Definition 14.6.29. *Let Γ be a totally ordered group and Δ a subgroup of Γ of finite index. The number of major subsets of Γ consisting of strictly positive elements and containing all strict positive elements of Δ is called the **initial index** of Δ in Γ and denoted by $\varepsilon(\Gamma, \Delta)$.*

This initial index is a natural number by virtue of the following proposition:

Proposition 14.6.30. *Let Γ be a totally ordered group and Δ a subgroup of Γ of finite index. If Γ has no least positive element, then $\varepsilon(\Gamma, \Delta) = 1$ for all Δ. If there exists a least positive element of Γ and Γ_0 denotes the subgroup it generates, then*

$$\varepsilon(\Gamma, \Delta) = [\Gamma_0 : \Gamma_0 \cap \Delta].$$

Proof. In the first case, let α be a strict positive element in Γ. The set of $\alpha \in \Gamma$ such that $0 < \beta < \alpha$ is infinite and hence there exist two elements of this set which are distinct and congruent modulo Δ; their difference is an element γ of Γ such that $0 < \gamma < \alpha$. Hence every major subset which contains all the strictly positive elements of Δ contains α and hence all strict positive elements of Γ.

In the second case, let δ be the least strict positive element of Γ and let n be the least positive integer such that $mx \in \Delta$. Clearly $n = [\Gamma_0 : \Gamma_0 \cap \Delta]$. On the other hand, writing $M(\alpha)$ for the set of $\beta \in \Gamma$ such that $\beta > \alpha$, it is immediately seen that the admissible major sets are just $M(\delta)$, $M(2\delta), \ldots, M(n\delta)$. □

Corollary 14.6.31. *The initial index $\varepsilon(\Gamma, \Delta)$ divides the index $[\Gamma : \Delta]$ and is equal to it if Γ is isomorphic to $\mathbb{Z}$.*

Definition 14.6.32. *Let K be a field, L a finite extension of K, w a valuation on L, v its restriction to K and Γ_v and Γ_w their order groups. The initial index of Γ_v in Γ_w is called the* ***initial ramification index*** *of w with respect to v (or with respect to K) and denoted by $\varepsilon(w/v)$.*

From the above corollary, $\varepsilon(w/v)$ divides $e(w/v)$ with equality in the case of a discrete valuation.

Proposition 14.6.33. *Let K be a field, L a finite extension of K, w a valuation on L, v its restriction to K. Then*

$$\dim_{\kappa_v}(A_w/\mathfrak{m}_v A_w) = \varepsilon(w/v) f(w/v).$$

Proof. The ideals of A_w containing $\mathfrak{m}_v$ and distinct from A_w correspond to the major subsets of Γ_w, consisting of strict positive elements and containing the elements strict positive of Γ_v. They are therefore equal in number to $\varepsilon(w/v)$ and, as they form a totally ordered set under inclusion, this number is equal to the length of the quotient ring $A_w/\mathfrak{m}_v A_w$. Now a module of length 1 over A_w is a 1-dimensional vector space over κ_w and hence a module of length $f(w/v)$ over A; hence, as $A_w/\mathfrak{m}_v A_w$ is of length $\varepsilon(w/v)$ over A_w, it is of length $\varepsilon(w/v) f(w/v)$ over A_v, that is over κ_v. □

Theorem 14.6.34. *Let K be a field, v a valuation on K, A its ring, $\mathfrak{m}$ its maximal ideal, L a finite extension of K of degree n, B the integral closure of A in L and $(w_i)_{1 \le i \le s}$ a complete system of extensions of v to L. Then*

$$\dim_{\kappa_v}(B/\mathfrak{m}B) = \sum_{i=1}^{s} \varepsilon(w_i/v) f(w_i/v) \le \sum_{i=1}^{s} e(w_i/v) f(w_i/v) \le n.$$

Proof. Let B_i be the ring of w_i; then $B_i = B_{\mathfrak{m}_i}$, where $\mathfrak{m}_i$ runs through the family of maximal ideals of B. Let $\mathfrak{q}_i$ be the saturation of $\mathfrak{m}B$ with respect to $\mathfrak{m}_i$. By Corollary 13.1.66, the canonical homomorphism $B/\mathfrak{m}B \to \prod_{i=1}^{s} B/\mathfrak{q}_i$ is an isomorphism and $\mathfrak{m}_i$ is the only maximal ideal

containing $\mathfrak{q}_i$. Hence $B/\mathfrak{q}_i$ is canonically isomorphic to $(B/\mathfrak{q}_i)_{\mathfrak{m}_i}$. On the other hand, we note that

$$(B/\mathfrak{q}_i)_{\mathfrak{m}_i} = B_{\mathfrak{m}_i}/\mathfrak{m}B_{\mathfrak{m}_i} = B_i/\mathfrak{m}B_i,$$

therefore there is a canonical isomorphism $B/\mathfrak{m}B \to \prod_{i=1}^{s} B_i/\mathfrak{m}B_i$, whence the result in view of Proposition 14.6.33. □

Theorem 14.6.35. *With the hypotheses and notation of Theorem 14.6.34, the following conditions are equivalent:*

(a) B is a finitely generated A-module;

(b) B is a free A-module;

(c) $\dim_{\kappa_v}(B/\mathfrak{m}B) = n$;

(d) the equality in Theorem 14.6.34 holds and $\varepsilon(w_i/v) = e(w_i/v)$ for all i.

Proof. The equivalence of (a) and (b) follows from Proposition 14.1.5. Also, the equivalence of (c) and (d) follows from Theorem 14.6.34. It remains to show that (c) and (b) are equivalent.

First, assume that B is a free A-module. From the proof of Theorem 13.1.48, we see for any $x \in L$ there exists $s \in A$ such that sx is integral over K, hence in B. Since K is the fraction field of A, any independent set of B over A is an independent subset of L over K. These together show that any basis of B over A is also a basis of L over K, hence $\operatorname{rank}_A(B) = n$. Next, we prove that $\dim_{\kappa_v}(B/\mathfrak{m}B)$ also equals to n. Let $\{x_1, \dots, x_n\}$ be a basis of B over A. If $\bar{x}_i$ denotes the image of x_i in $B/\mathfrak{m}B$ then $\bar{x}_1, \dots, \bar{x}_n$ span the vector space $B/\mathfrak{m}B$ over κ_v. We assert that the n vectors are independent, hence the claim. For this, it suffices to show that if we have a relation of the form $\sum_{i=1}^{n} a_i x_i \in \mathfrak{m}B$, $a_i \in A$, then the a_i's necessarily belong to A. But this follows at once from the linear independence of the x_i over A, for we have, by assumption: $\sum_{i=1}^{n} a_i x_i = \sum_{i=1}^{n} b_i x_i$, where the y_i are suitable elements of $\mathfrak{m}$, and this relation implies $a_i = b_i$ for each i.

Conversely, assume that $\dim_{\kappa_v}(B/\mathfrak{m}B) = n$. Let $x_1, \dots, x_n$ be elements of B whose canonical images in $B/\mathfrak{m}B$ form a basis of $B/\mathfrak{m}B$ and let $M \subseteq B$ be the sub-Amodule which they generate. As M is torsion-free ($M \subseteq B$ and B is an integral domain) and finitely generated, it is free by Proposition 14.1.5. We shall see that $B = M$. Let $y \in B$; we write $N = M + Ay$; this is also a free A-module. The canonical injections $M \to N \to B$ give canonical homomorphisms

$$M/\mathfrak{m}M \to N/\mathfrak{m}N \to B/\mathfrak{m}B.$$

Now, by hypothesis, $M/\mathfrak{m}M \to B/\mathfrak{m}B$ is surjective and $B/\mathfrak{m}B$ is n-dimensional, hence $M/\mathfrak{m}M$ and $N/\mathfrak{m}N$ are n-dimensional and $M/\mathfrak{m}M \to N/\mathfrak{m}N$ is surjective. As N is finitely generated, $M \to N$ is then surjective by Proposition 7.1.5, whence $M = N$ and $B = M$. Hence B is free. □

Corollary 14.6.36. *With the same hypotheses and notation, suppose further that v is discrete and L separable. Then*

$$\sum_{i=1}^{s} e(w_i/v) f(w_i/v) = n.$$

Proof. In this case B is a free A-module of rank n by Theorem 13.1.48, since A is a PID. □

Corollary 14.6.37. *Let (K, v) be a discrete valued complete field and L a finite extension of K of degree n. Then v admits a unique (up to equivalence) extension w to L, the ring B of w is a finitely generated free module over the ring A of v and $e(w/v)f(w/v) = n$.*

Proof. All the extensions of v to L are dependent by Corollary 14.6.22. Since they are discrete by Corollary 14.6.9, they are therefore equivalent. This shows the uniqueness of w. The integral closure of A in L is therefore B. As v is discrete, the topology induced on A by that on K is the $\mathfrak{m}$-adic topology (where $\mathfrak{m} = \mathfrak{m}_A$); the ring A is complete, for it is closed in K. We conclude that, since $B/\mathfrak{m}B$ is a finite-dimensional vector $(A/\mathfrak{m})$-space (Proposition 14.6.33), B is a finitely generated A-module (Corollary 11.3.36). It is therefore free and $e(v'/v)f(v'/v) = n$ by Theorem 14.6.35. □

Corollary 14.6.38. *Suppose that v is of rank 1 and that the equivalent conditions of Theorem 14.6.35 hold. If $\widehat{L}_i$ is the completion of L with respect to w_i, then the degree $n_i = [\widehat{L}_i : \widehat{K}]$ is equal to $e(w_i/v)f(w_i/v)$ for all i and the canonical homomorphism*

$$\phi : \widehat{K} \otimes_K L \to \prod_{i=1}^{s} \widehat{L}_i$$

is bijective. For all $x \in L$, the characteristic polynomial $\min_{L/K}(x)$ is equal to the product of the characteristic polynomials $\min_{\widehat{L}_i/\widehat{K}}(x)$. In particular, we have

$$\mathrm{tr}_{L/K}(x) = \sum_{i=1}^{s} \mathrm{tr}_{\widehat{L}_i/\widehat{K}}(x), \quad N_{L/K}(x) = \prod_{i=1}^{s} N_{\widehat{L}_i/\widehat{K}}(x), \quad v(N_{L/K}(x)) = \sum_{i=1}^{s} n_i w_i(x). \tag{6.4.2}$$

Proof. As no two of the w_i are equivalent and they are of rank 1 by Corollary 14.6.8, they are independent and Theorem 14.6.24 therefore shows that $e(w_i/v)f(w_i/v) \le n_i$ for all i and $\sum_i n_i \le n$. The first assertion therefore follows from these inequalities and the relation $\sum_i e(w_i/v)f(w_i/v) = n$. Under the isomorphism ϕ the endomorphism $z \mapsto z(1 \otimes x)$ of $\widehat{K} \otimes_K L$ (for $x \in L$) is transformed into the endomorphism of $\prod_{i=1}^{s} \widehat{L}_i$, leaving invariant each of the factors and reducing on each factor to multiplication by x (L_i being canonically imbedded in its completion $\widehat{L}_i$); whence the assertion relating to the characteristic polynomial of x and the first two formulae of (6.4.2). Finally, let E be a finite quasi-Galois extension of $\widehat{K}$ containing $\widehat{L}_i$. As $\widehat{K}$ is complete and v has rank 1, there exists only one valuation (up to equivalence) w on E extending $\hat{v}$ (Corollary 14.6.22). Then for every $\widehat{K}$-automorphism σ of E we have $w(\sigma(x)) = w(x)$ and therefore

$$\hat{v}(N_{\widehat{L}_i/\widehat{K}}(x)) = n_i w_i(x)$$

which proves the formula. □

14.7 Exercise

Exercise 14.7.1. If A is a valuation ring of dimension ≥ 2 then the formal power series ring $A[\![X]\!]$ is not integrally closed.

Proof. Let $0 \subset \mathfrak{p}_1 \subset \mathfrak{p}_2$ be a strict chain. Let $b \in \mathfrak{p}_1$, $a \in \mathfrak{p}_2 - \mathfrak{p}_1$, then $a^n/b \notin A$ for all n:

$$a^n/b \in A \Rightarrow a^n = (a^n/b) \cdot b \in \mathfrak{p}_1 \Rightarrow a \in \mathfrak{p}_1 (\mathfrak{p}_1 \text{ is prime})$$

Now A is a valuation ring so $ba^{-n} \in A$ for all n.

Let $f = \sum_{n=0}^{\infty} u_n x^n$ be a solution of

$$f^2 + af + x = 0$$

We shall take $u_0 = -a$, then from the equation

$$f^2 + af = \sum_{n=0}^{\infty} (u_0 u_n + \cdots + u_n u_0 + a u_n) x^n$$

we claim that $u_n \in a^{-2n+1}A$ for all $n \geq 1$. In fact, we can compute $u_1 = a^{-1}$. And assume this holds for $u_1, \ldots, u_{n-1}$, for u_n we have an equation

$$u_0 u_n + u_1 u_{n-1} + \cdots + u_{n-1} u_1 + u_n u_0 + a u_n = 0$$

For $1 \leq i \leq n-1$, since $u_i \in a^{-2i+1}A$ we have

$$u_i u_{n-i} = a^{-2i+1} r_1 \cdot a^{-2(n-i)+1} r_2 = a^{-2n+2} r_1 r_2 \in a^{-2n+2} A$$

Hence

$$u_n = -(a + 2u_0)^{-1}(u_1 u_{n-1} + \cdots + u_{n-1} u_1) \in a^{-1} \cdot a^{-2n+2} A = a^{-2n+1} A.$$

Now we only need to prove that f is in the field of fractions of $A[\![X]\!]$. By our observation we have $bf \in A[\![X]\!]$, so $f \in b^{-1} A[\![X]\!] \subseteq \mathrm{Frac}(A[\![X]\!])$. But since $a \in \mathfrak{p}_2$, $a^{-1} \notin A$, which means $f \notin A[\![X]\!]$. So $A[\![X]\!]$ is not integrally closed. □

Exercise 14.7.2. If v is an additive valuation of a field K and $\alpha_1, \ldots, \alpha_n \in K$ are such that $\alpha_1 + \cdots + \alpha_n = 0$ then there exist two indices i, j such that $i \neq j$ and $v(\alpha_i) = v(\alpha_j)$.

Proof. If all $\alpha_i = 0$ then $v(\alpha_i) = \infty$ for all i, and the claim holds. Hence we may assume that $a_n \neq 0$, and from $\alpha_1 + \cdots + \alpha_n = 0$ we get

$$1 = -\left(\frac{\alpha_1}{\alpha_n} + \cdots + \frac{\alpha_{n-1}}{\alpha_n}\right).$$

Now, since $1 \notin \mathfrak{m}$, there exist an index $1 \leq i \leq n-1$ such that α_i/α_n is not in $\mathfrak{m}$, hence is a unit. Then by our definition $v(\alpha_i/\alpha_n) = 0$, so $v(\alpha_i) = v(\alpha_n)$. □

Exercise 14.7.3. Let k be a field, x and y indeterminates, and supposeth α is a positive irrational number. Then the map $v : k[x, y] \to \mathbb{R} \cup \{\infty\}$ defined by

$$\sum_{n,m} c_{n,m} x^n y^m \mapsto \min\{n + m\alpha \mid c_{n,m} \neq 0\}$$

determines a valuation of $k(x, y)$ with value group $\mathbb{Z} + \alpha\mathbb{Z}$.

Proof. For $f = \sum_{n,m} a_{n,m} x^n y^m$, $g = \sum_{n,m} b_{n,m} x^n y^m$, we have

$$v(fg) = \min\{n_1 + n_2 + (m_1 + m_2)\alpha \mid a_{n_1,m_1} \neq 0, b_{n_2,m_2} \neq 0\}$$

which is easily seen to be equal to $v(f) + v(g)$.

For $v(f+g)$, it is also easy to verify $v(f+g) \geq \min\{v(f), v(g)\}$. Also, $v(0) = \infty$. Thus by the previous exercise, v extends to a valuation $k(x, y) \to \mathbb{R} \cup \{\infty\}$. It is clear that $\Gamma_v = \mathbb{Z} + \alpha\mathbb{Z}$. □

Exercise 14.7.4. Let A be a DVR and $\mathfrak{m}$ its maximal ideal; then the $\mathfrak{m}$-adic completion $\widehat{A}$ of A is again a DVR.

Proof. Let $\mathfrak{m} = (x)$, then every element in A has a form rx^n for r a unit. Hence we can think the complition of A as the power series ring $(A - \mathfrak{m})[\![t]\!]$. Thus, we can define a valuation for $f = \sum_{n=0}^{\infty} u_n t^n$:

$$v : \widehat{A} \to \mathbb{Z}, \quad v(f) = \{n \mid u_n \neq 0\}$$

Since $f = \sum_{n=0}^{\infty} u_n t^n$ is a unit if and only if u_0 is a unit, this is well defined, and extending it to the field of fractions of $\widehat{A}$ gives makes $\widehat{A}$ a valuation ring. □

Chapter 15

Krull domains and divisors

15.1 Krull domains

15.1.1 Fractional ideals

Definition 15.1.1. *Let A be an integral domain and K its field of fractions. A sub-A-module $\mathfrak{a}$ of K such that there exists a nonzero element $d \in A$ for which $d\mathfrak{a} \subseteq A$ is called a* ***fractional ideal*** *of A (or of K, by an abuse of language).*

Every finitely generated sub-A-module $\mathfrak{a}$ of K is a fractional ideal: for if $a_1, \ldots, a_n$ is a system of generators of $\mathfrak{a}$, we may write $a_i = x_i/y_i$, where $x_i, y_i \in A$ and $y_i \neq 0$. If $d = y_1 \cdots y_n$ then clearly $d\mathfrak{a} \subseteq A$. In particular the principal sub-A-modules of K are fractional ideals. It is clear that every ideal of A is a fractional ideal. To avoid confusion, these will also be called the **integral ideals** of A. We denote by $\mathfrak{F}(A)$ the set of non-zero fractional ideals of A. Given two elements $\mathfrak{a}, \mathfrak{b}$ of $\mathfrak{F}(A)$, we shall write $\mathfrak{a} \preceq \mathfrak{b}$ for the relation "every fractional principal ideal containing $\mathfrak{a}$ also contains $\mathfrak{b}$. Clearly this relation is a **preordering** on $\mathfrak{F}(A)$ (it is reflexive and transitive). Consider the associated equivalence relation "$\mathfrak{a} \preceq \mathfrak{b}$ and $\mathfrak{b} \preceq \mathfrak{a}$" and let $\mathfrak{D}(A)$ be the equivalent class of this relation. We shall say that the elements of $\mathfrak{D}(A)$ are the **divisors** of A and, for every fractional ideal $\mathfrak{a} \in \mathfrak{F}(A)$, we shall denote by $\operatorname{div}(\mathfrak{a})$ (or $\operatorname{div}_A(\mathfrak{a})$) the canonical image of $\mathfrak{a}$ in $\mathfrak{D}(A)$ and we shall say that $\operatorname{div}(\mathfrak{a})$ is the **divisor of** $\mathfrak{a}$. If $a = Ax$ is a fractional principal ideal, we write $\operatorname{div}(x)$ instead of $\operatorname{div}(Ax)$ and $\operatorname{div}(x)$ is called the **divisor of** $\boldsymbol{x}$. The elements of $\mathfrak{D}(A)$ of the form $\operatorname{div}(x)$ are called **principal divisors**. By taking the quotient, the preordering $\preceq$ on $\mathfrak{F}(A)$ defines on $\mathfrak{D}(A)$ an ordering which we shall denote by $\leq$.

For any $\mathfrak{a} \in \mathfrak{F}(A)$ there exists by hypothesis some $d \in A$ such that $\mathfrak{a} \subseteq Ad^{-1}$. The intersection $\tilde{\mathfrak{a}}$ of the fractional principal ideals containing $\mathfrak{a}$ is therefore an element of $\mathfrak{F}(A)$. Clearly the relation $\mathfrak{a} \preceq \mathfrak{b}$ is equivalent to the relation $\tilde{\mathfrak{a}} \supseteq \tilde{\mathfrak{b}}$, which is the case if $\mathfrak{a} \supseteq \mathfrak{b}$. For two elements $\mathfrak{a}$, $\mathfrak{b}$ of $\mathfrak{F}(A)$ to be equivalent modulo R, it is necessary and sufficient that $\tilde{\mathfrak{a}} = \tilde{\mathfrak{b}}$.

Definition 15.1.2. *Every element $\mathfrak{a}$ of $\mathfrak{F}(A)$ such that $\mathfrak{a} = \tilde{\mathfrak{a}}$ is called a* ***divisorial fractional ideal*** *of A.*

In other words a divisorial ideal is just a non-zero intersection of a non-empty family of fractional principal ideals. Every non-zero intersection of divisorial ideals is a divisorial ideal. If $\mathfrak{a}$ is divisorial, so is $\mathfrak{a}x$ for all $x \in K$, the mapping $\mathfrak{b} \mapsto \mathfrak{b}x$ being a bijection of the set of fractional principal ideals onto itself. By definition, for all $\mathfrak{a} \in \mathfrak{F}(A)$, $\tilde{\mathfrak{a}}$ is then the least divisorial ideal containing $\mathfrak{a}$ and is equivalent to $\mathfrak{a}$ modulo R. Moreover, if $\mathfrak{b}$ is a divisorial ideal

equivalent to $\mathfrak{a}$ modulo R, then $\tilde{\mathfrak{a}} = \tilde{\mathfrak{b}} = \mathfrak{b}$. Hence $\tilde{\mathfrak{a}}$ is the unique divisorial ideal $\mathfrak{b}$ such that $\operatorname{div}(\mathfrak{a}) = \operatorname{div}(\mathfrak{b})$ (in other words, the restriction of the mapping $\mathfrak{a} \mapsto \operatorname{div}(\mathfrak{a})$ to the set of divisorial ideals is bijective).

Let $\mathfrak{a}$ and $\mathfrak{b}$ be two fractional ideals of K. Recall that $(\mathfrak{b} : \mathfrak{a})$ denotes the set of $x \in K$ such that $x\mathfrak{a} \subseteq \mathfrak{b}$. This is obviously an A-module. Note that $(\mathfrak{b} : \mathfrak{a})$ is also a fractional ideal, for if d is a non-zero element of A such that $d\mathfrak{b} \subseteq A$ and $d\mathfrak{a} \subseteq A$ and a is a non-zero element of $A \cap \mathfrak{a}$, then $da(\mathfrak{b} : \mathfrak{a}) \subseteq A$. On the other hand, if $b \neq 0$ belongs to $\mathfrak{b}$, then $bd\mathfrak{a} \subseteq \mathfrak{b}$, hence $bd \in (\mathfrak{b} : \mathfrak{a})$ and $(\mathfrak{b} : \mathfrak{a}) \neq 0$. Note that the definition of $(\mathfrak{b} : \mathfrak{a})$ can also be written as

$$(\mathfrak{b} : \mathfrak{a}) = \bigcap_{x \in \mathfrak{a}, x \neq 0} \mathfrak{b}x^{-1}. \tag{1.1.1}$$

Proposition 15.1.3. *Let $\mathfrak{a}, \mathfrak{b}$ be fractional ideals of A.*

(a) If $\mathfrak{b}$ is a divisorial ideal then $(\mathfrak{b} : \mathfrak{a})$ is divisorial.

(b) In order that $\operatorname{div}(\mathfrak{a}) = \operatorname{div}(\mathfrak{b})$, it is necessary and sufficient that $(A : \mathfrak{a}) = (A : \mathfrak{b})$.

(c) We have $\tilde{\mathfrak{a}} = (A : (A : \mathfrak{a}))$.

Proof. Assertion (a) follows immediately from equation (1.1.1) since, if $\mathfrak{b}$ is divisorial, so is $\mathfrak{b}x^{-1}$ for all $x \neq 0$. To show (b), let $P(\mathfrak{a})$ denote the set of fractional principal ideals containing $\mathfrak{a}$. The relation $Ax \in P(\mathfrak{a})$ is equivalent to $x^{-1}\mathfrak{a} \subseteq A$ and hence to $x^{-1} \in (A : \mathfrak{a})$. As the relation $\operatorname{div}(\mathfrak{a}) = \operatorname{div}(\mathfrak{b})$ is by definition equivalent to $P(\mathfrak{a}) = P(\mathfrak{b})$, it is also equivalent to $(A : \mathfrak{a}) = (A : \mathfrak{b})$.

Finally, as $\mathfrak{a}(A : a) \subseteq A$, we see $\mathfrak{a} \subseteq (A : (A : \mathfrak{a}))$. Replacing $\mathfrak{a}$ by $(A : \mathfrak{a})$ in this formula, it is seen that $(A : \mathfrak{a}) \subseteq (A : (A : (A : \mathfrak{a})))$. On the other hand, the relation $\mathfrak{a} \subseteq (A : (A : \mathfrak{a}))$ implies

$$(A : \mathfrak{a}) \supseteq (A : (A : (A : \mathfrak{a})))$$

Therefore $(A : \mathfrak{a}) = (A : (A : (A : \mathfrak{a})))$ and it follows from (b) that $\operatorname{div}(\mathfrak{a}) = \operatorname{div}(A : (A : \mathfrak{a}))$. As $(A : (A : \mathfrak{a}))$ is divisorial by (a), certainly $\tilde{\mathfrak{a}} = (A : (A : \mathfrak{a}))$, which proves (c). □

Proposition 15.1.4 (Lattice Structure in $\mathfrak{D}(A)$).

(a) In $\mathfrak{D}(A)$ every non-empty set bounded above admits a least upper bound. Moreprecisely, if $(\mathfrak{a}_i)$ is a non-empty family of elements of $\mathfrak{F}(A)$ which is bounded above, then

$$\sup_i(\operatorname{div}(\mathfrak{a}_i)) = \operatorname{div}(\bigcap_i \tilde{\mathfrak{a}}_i).$$

(b) In $\mathfrak{D}(A)$ every non-empty set bounded below admits a greatest lower bound. More precisely, if $(\mathfrak{a}_i)$ is a non-empty family of elements of $\mathfrak{F}(A)$ which is bounded below, then

$$\inf_i(\operatorname{div}(\mathfrak{a}_i)) = \operatorname{div}(\sum_i \tilde{\mathfrak{a}}_i).$$

(c) $\mathfrak{D}(A)$ is a lattice.

Proof. Let $(\mathfrak{a}_i)$ be a non-empty family of elements of $\mathfrak{F}(A)$ which is bounded above. To say that a divisorial ideal $\mathfrak{b}$ bounds this family above amounts to saying that it is contained in all the $\tilde{\mathfrak{a}}_i$. Hence $\bigcap_i \tilde{\mathfrak{a}}_i \neq 0$ and $\sup_i(\operatorname{div}(\mathfrak{a}_i)) = \operatorname{div}(\bigcap_i \tilde{\mathfrak{a}}_i)$.

Now let $(\mathfrak{a}_i)$ be a non-empty family of elements of $\mathfrak{F}(A)$ which is bounded below. To say that a divisorial ideal $\mathfrak{b}$ bounds this family below means that it contains all the $\tilde{\mathfrak{a}}_i$, so we see $\inf_i(\mathrm{div}(\mathfrak{a}_i)) = \mathrm{div}(\sum_i \tilde{\mathfrak{a}}_i)$.

Finally, it is sufficient to note that, if $\mathfrak{a}$, $\mathfrak{b}$ are in $\mathfrak{F}(A)$, then $\mathfrak{a} \cap \mathfrak{b}$ and $\mathfrak{a} + \mathfrak{b}$ are both nonzero fractional ideals, so the claim follows. □

Corollary 15.1.5. *If $x, y, x + y \in K^\times$ then* $\mathrm{div}(x + y) \geq \inf\{\mathrm{div}(x), \mathrm{div}(y)\}$.

Proof. We have $A(x + y) \subseteq Ax + Ay$ and hence $\mathrm{div}(x + y) \geq \mathrm{div}(Ax + Ay)$. □

15.1.2 The monoid structure on $\mathfrak{D}(A)$

Proposition 15.1.6. *Let $\mathfrak{a}$, $\mathfrak{a}'$, $\mathfrak{b}$, $\mathfrak{b}'$ be elements of $\mathfrak{F}(A)$. Then the relations $\mathfrak{a} \geq a'$ and $\mathfrak{b} \geq \mathfrak{b}'$ imply $\mathfrak{a}\mathfrak{b} \geq \mathfrak{a}'\mathfrak{b}'$.*

Proof. We may restrict our attention to the case where $\mathfrak{b} = \mathfrak{b}'$, by transitivity. Then let Ax be a fractional principal ideal containing $\mathfrak{a}'\mathfrak{b}$. For every non-zero element y of $\mathfrak{b}$, $Ax \supseteq \mathfrak{a}'y$ and hence $Axy^{-1} \supseteq \mathfrak{a}'$, whence $Axy^{-1} \supseteq \mathfrak{a}$ and $Ax \supseteq \mathfrak{a}y$. Varying y, it is seen that $Ax \supseteq \mathfrak{a}\mathfrak{b}$, whence $\mathfrak{a}\mathfrak{b} \geq \mathfrak{a}'\mathfrak{b}$. □

It follows from Proposition 15.1.6 that multiplication on $\mathfrak{F}(A)$ defines, by passing to the quotient, a law of composition on $\mathfrak{D}(A)$ which is obviously associative and commutative. It is written additively so that we may write:

$$\mathrm{div}(\mathfrak{a}\mathfrak{b}) = \mathrm{div}(\mathfrak{a}) + \mathrm{div}(\mathfrak{b})$$

for $\mathfrak{a}$, $\mathfrak{b}$ in $\mathfrak{F}(A)$. Clearly $\mathrm{div}(1)$ is an identity element for this addition. This element is denoted by 0. Proposition 15.1.6 proves further that the order structure on $\mathfrak{D}(A)$ is compatible with this addition:

$$\begin{aligned}\inf(\mathrm{div}(\mathfrak{a}) + \mathrm{div}(\mathfrak{b}), \mathrm{div}(\mathfrak{a}) + \mathrm{div}(\mathfrak{c})) &= \inf(\mathrm{div}(\mathfrak{a}\mathfrak{b}), \mathrm{div}(\mathfrak{a}\mathfrak{c})) = \mathrm{div}(\mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c}) \\ &= \mathrm{div}(\mathfrak{a}(\mathfrak{b} + \mathfrak{c})) = \mathrm{div}(\mathfrak{a}) + \mathrm{div}(\mathfrak{b} + \mathfrak{c}) \\ &= \mathrm{div}(\mathfrak{a}) + \inf(\mathrm{div}(\mathfrak{b}), \mathrm{div}(\mathfrak{c})).\end{aligned}$$

For a fractional ideal $\mathfrak{a}$ to be such that $\mathrm{div}(\mathfrak{a}) \geq 0$ in $\mathfrak{D}(A)$, it is necessary and sufficient that $\mathfrak{a} \subseteq A$ (in other words, that $\mathfrak{a}$ be an integral ideal of A).

For two elements x, y of $K^\times$, the relation $\mathrm{div}(x) = \mathrm{div}(y)$ is equivalent to $Ax = Ay$. Therefore the set of principal divisors of A with the order relation and the monoid law induced by that on $\mathfrak{D}(A)$ is an ordered group canonically isomorphic to the multiplicative group of fractional principal ideals ordered by the opposite order relation to inclusion. The relation S between two elements P, Q of $\mathfrak{D}(A)$:

$$\text{there exists } x \in K^\times \text{ such that } P = Q + \mathrm{div}(x)$$

is therefore an equivalence relation since the relation $P = Q + \mathrm{div}(x)$ is equivalent to $Q = P + \mathrm{div}(x^{-1})$. If P and Q are congruent modulo S, they are called **equivalent divisors** of A. Clearly moreover the relation S is compatible with the law of the monoid $\mathfrak{D}(A)$ and the latter

therefore defines, by taking quotients, a monoid structure on $\mathfrak{D}(A)/S$. This monoid is called the **divisor class monoid** of A.

Proposition 15.1.7. *Let $\mathfrak{a}$, $\mathfrak{b}$ be two divisorial fractional ideals of A. Then* $\operatorname{div}(\mathfrak{a})$ *and* $\operatorname{div}(\mathfrak{b})$ *are equivalent divisors if and only if there exists $x \in K^\times$ such that $\mathfrak{b} = x\mathfrak{a}$.*

Proof. If $\operatorname{div}(\mathfrak{b}) = \operatorname{div}(\mathfrak{a}) + \operatorname{div}(x)$ for some $x \in K^\times$, then $\operatorname{div}(\mathfrak{b}) = \operatorname{div}(x\mathfrak{a})$ and, as $\mathfrak{b}$ and $x\mathfrak{a}$ are divisorial, $\mathfrak{b} = x\mathfrak{a}$, which proves the proposition. □

Let $\mathfrak{a}$ be an invertible fractional ideal; then $\mathfrak{a} = (A : (A : \mathfrak{a}))$ by Proposition 10.5.22(b) and hence $\mathfrak{a}$ is divisorial by Proposition 15.1.3. The group $\mathfrak{I}(A)$ of invertible fractional ideals is therefore identified with a subgroup of the monoid $\mathfrak{D}(A)$ and the canonical image of $\mathfrak{I}(A)$ in $\mathfrak{D}(A)/S$ with the group of classes of projective A-modules of rank 1 (Proposition 10.5.26).

Proposition 15.1.8. *Let A be an integral domain. For the monoid $\mathfrak{D}(A)$ of divisors of A to be a group, it it necessary and sufficient that A be completely integrally closed.*

Proof. Suppose that $\mathfrak{D}(A)$ is a group. Let $x \in K$ and suppose that $A[x]$ is contained in a finitely generated sub-A-module of K. Then we have seen that $\mathfrak{a} = A[x]$ is an element of $\mathfrak{F}(A)$. Then $x\mathfrak{a} \subseteq \mathfrak{a}$ and hence $\operatorname{div}(x) + \operatorname{div}(\mathfrak{a}) \geq \operatorname{div}\mathfrak{a}$. Since $\mathfrak{D}(A)$ is an ordered group, we conclude that $\operatorname{div}(x) \geq 0$, whence $x \in A$. Thus A is completely integrally closed.

Conversely, suppose that A is completely integrally closed. Let $\mathfrak{a}$ be a divisorial ideal. We shall show that $\operatorname{div}(\mathfrak{a}(A : \mathfrak{a})) = 0$, which will prove that $\mathfrak{D}(A)$ is a group. As $\mathfrak{a}(A : \mathfrak{a}) \subseteq A$, it suffices to verify that every fractional principal ideal Ax^{-1} which contains $\mathfrak{a}(A : \mathfrak{a})$ also contains A. Now, for $y \in K^\times$, the relation $Ay \supseteq \mathfrak{a}$ implies $y^{-1} \in (A : \mathfrak{a})$, whence $y^{-1}\mathfrak{a} \subseteq \mathfrak{a}(A : \mathfrak{a}) \subseteq Ax^{-1}$ and hence $x\mathfrak{a} \subseteq Ay$. As $\mathfrak{a}$ is divisorial, we then deduce that $x\mathfrak{a} \subseteq \mathfrak{a}$, whence $x^n\mathfrak{a} \subseteq \mathfrak{a}$ for all $n \in \mathbb{N}$. Since $\mathfrak{a}$ is divisorial, there exist elements x_0, x_1 of $K^\times$ such that $Ax_0 \subseteq \mathfrak{a} \subseteq Ax_1$; therefore $x^n x_0 \in Ax_1$, whence $x^n \in Ax_1x_0^{-1}$. As A is completely integrally closed, $x \in A$, that is $Ax^{-1} \supseteq A$, which completes the proof. □

Remark 15.1.1. Note that, if A is completely integrally closed (and even Noetherian), a divisorial ideal of A is not necessarily invertible, in other words, in general $\mathfrak{I}(A) \neq \mathfrak{D}(A)$.

Corollary 15.1.9. *Let A be a completely integrally closed domain and $\mathfrak{a}$ a divisorial fractional ideal of A. Then, for every nonzero fractional ideal $\mathfrak{b}$ of A,* $\operatorname{div}(\mathfrak{a} : \mathfrak{b}) = \operatorname{div}(\mathfrak{a}) - \operatorname{div}(\mathfrak{b})$.

Proof. By the formula (1.1.1),

$$\operatorname{div}(\mathfrak{a} : \mathfrak{b}) = \operatorname{div}\Big(\bigcap_{y\in\mathfrak{b},y\neq 0} y^{-1}\mathfrak{a}\Big) = \sup_{y\in\mathfrak{b},y\neq 0} \operatorname{div}(y^{-1}\mathfrak{a})$$

taking account of Proposition 15.1.4 and the fact that the fractional ideals $y^{-1}\mathfrak{a}$ are divisorial. But since $D(A)$ is an ordered group,

$$\sup_{y\in\mathfrak{b},y\neq 0} \operatorname{div}(y^{-1}\mathfrak{a}) = \sup_{y\in\mathfrak{b},y\neq 0} (\operatorname{div}(\mathfrak{a}) - \operatorname{div}(y)) = \operatorname{div}(\mathfrak{a}) - \inf_{y\in\mathfrak{b},y\neq 0} \operatorname{div}(y) = \operatorname{div}(\mathfrak{a}) - \operatorname{div}(\mathfrak{b})$$

so the claim follows. □

15.1.3 Krull domains

Definition 15.1.10. *An integral domain A is called a* ***Krull domain*** *if there exists a family $(v_i)_{i\in I}$ valuations on the field of fractions K of A with the following properties:*

(K1) the valuations v_i are discrete;

(K2) the intersection of the rings of the v_i is A;

(K3) for all $x \in K^\times$, the set of indices $i \in I$ such that $v_i(x) \neq 0$ is finite.

Such a family $(v_i)_{i\in I}$ is called a ***defining family of valuations****.*

Example 15.1.11.

(a) Every discrete valuation ring is a Krull domain.

(b) More generally, every PID A is a Krull domain. For let $(p_i)_{i\in I}$ be a representative system of irreducible elements of A and let v_i be the valuation on the field of fractions of A defined by p_i. It is immediately seen that the family $(v_i)_{i\in I}$ satisfies properties (K1), (K2) and (K3).

Let A be a Krull domain and let $(v_i)_{i\in I}$ be a family of valuations on the field of fractions K of A satisfying (K1), (K2) and (K3). The v_i may be assumed to be normed. For all $\mathfrak{a} \in I(A)$, we shall write:

$$v_i(\mathfrak{a}) = \sup_{\mathfrak{a}\subseteq Ax} v_i(x).$$

Then $v_i(\mathfrak{a}) \in \mathbb{Z}$, for, if a is a non-zero element of $\mathfrak{a}$, the relation $Ax \supseteq Aa$ implies that $v_i(x) \leq v_i(a)$ (by (K2)), which shows that the family $\{v_i(x) : \mathfrak{a} \subseteq Ax\}$ is bounded above. We establish the following properties.

Proposition 15.1.12. *Let A be a Krull domain, $(v_i)_{i\in I}$ a family of normed valuations on K satisfying (K1), (K2) and (K3), and $v_i(\mathfrak{a})$ be defined above.*

(a) If $x \in K^\times$ then $v_i(Ax) = v_i(x)$.

(b) Let $\mathfrak{a}$ and $\mathfrak{b}$ be two divisorial fractional ideals of A. In order that $\mathfrak{a} \subseteq \mathfrak{b}$, it is necessary and sufiicient that $v_i(\mathfrak{a}) \geq v_i(\mathfrak{b})$ for all $i \in I$.

(c) For all $\mathfrak{a} \in I(A)$, the indices $i \in I$ such that $v_i(\mathfrak{a}) \neq 0$ are finite in number.

Proof. If $Ay \supseteq Ax$, then $v_i(y) \leq v_i(x)$ by (K2) and the minimum value of $v_i(y)$ is taken at $y = x$. This proves (a). For a divisorial ideal $\mathfrak{a}$ be, the relation $y \in \mathfrak{a}$ is equivalent to the relation "$\mathfrak{a} \subseteq Ax$ implies $y \in Ax$". Now, by (K2), the relation $y \in Ax$ is equivalent to $v_i(y) \geq v_i(x)$ for all $i \in I$, whence we see $y \in \mathfrak{a}$ if and only if $v_i(y) \geq v_i(\mathfrak{a})$ for all i, and (b) follows.

Finally, for $\mathfrak{a} \in I(A)$ there exist x, y in K^* such that $Ax \subseteq \mathfrak{a} \subseteq Ay$. By properties (a) and (b), $v_i(x) \geq v_i(\mathfrak{a}) \geq v_i(y)$ for all $i \in I$. It then follows from (K3) that (c) holds. □

Corollary 15.1.13. *If A is a Krull domain and $(v_i)_{i\in I}$ is a defining family of normed valuations on K, the mapping $\mathfrak{a} \mapsto (v_i(\mathfrak{a}))_{i\in I}$ is a decreasing injective mapping of the set of divisorial integer ideals of A (ordered by inclusion) to the set of positive elements of the ordered group the direct sum $\mathbb{Z}^{\oplus I}$. In particular every non-empty family of divisorial integral ideals of A admits a maximal element.*

The condition in Corollary 15.1.13 is also suffcient. In fact, we have the following characterization for Krull domains.

Theorem 15.1.14. *Let A be an integral domain. For A to be a Krull domain, it is necessary and sufficient that the two following conditions be satisfied:*

(a) A is completely integrally closed.

(b) every non-empty family of divisorial integral ideals of A admits a maximal element (with respect to inclusion).

Moreover, if $P(A)$ is the set of irreducible elements of $\mathfrak{D}(A)$, then $P(A)$ is a basis of the $\mathbb{Z}$-module $\mathfrak{D}(A)$ and the positive elements of $\mathfrak{D}(A)$ are the linear combinations of the elements of $P(A)$ with positive coefficients.

Proof. A Krull domain is completely integrally closed by Corollary 14.2.12, and it satisfies (b) by Corollary 15.1.13. Conversely, let A be an integral domain satisfying properties (a) and (b) of the statement. Since A is completely integrally closed, $\mathfrak{D}(A)$ is an ordered group and a lattice. By condition (b) of the statement, every non-empty family of positive elements of $\mathfrak{D}(A)$ has a minimal element. Let $P(A)$ be the set of irreducible elements of $\mathfrak{D}(A)$. Then by **??** $P(A)$ is a basis of the $\mathbb{Z}$-module $\mathfrak{D}(A)$ and the positive elements of $\mathfrak{D}(A)$ are the linear combinations with positive integer coefficients of the elements of $P(A)$. Thus, for $x \in K^\times$, integers $v_P(x)$ are defined (for $P \in P(A)$) by writing:

$$\operatorname{div}(x) = \sum_{P \in P(A)} v_P(x) P. \tag{1.3.1}$$

From the relations $\operatorname{div}(xy) = \operatorname{div}(x) + \operatorname{div}(y)$ and $\operatorname{div}(x+y) \geq \inf\{\operatorname{div}(x), \operatorname{div}(y)\}$ for $x, y, x+y \in K^\times$, we deduce that the v_P are discrete valuations on K. In order that $x \in A$, it is necessary and sufficient that $\operatorname{div}(x) \geq 0$, that is that $v_P(x) \geq 0$ for all $P \in P(A)$. Thus the v_P satisfy conditions (K1) and (K2) and obviously also (K3). □

Corollary 15.1.15. *For a Noetherian ring to be a Krull domain, it is necessary and sufieient that it be an integrally closed domain.*

Proof. An integrally closed Noetherian domain is completely integrally closed. □

Note that there are non-Noetherian Krull domains, for example the polynominal ring $K[X_n]_{n \in \mathbb{N}}$ over a field K in an infinity of indeterminates.

15.1.4 Essential valuations for a Krull domain

Let A be a Krull domain and K its field of fractions. The valuations defined by formula (1.3.1) (for $x \in K^\times$) are called the **essential valuations** of K (or A). We have remarked in the course of the proof of Theorem 15.1.14 that the valuations (v_P) satisfy properties (K1), (K2) and (K3). Moreover, these discrete valuations v_P are normed: for every irreducible divisor $P \in P(A)$, $P < 2P$ and hence, if $\mathfrak{a}$ and $\mathfrak{b}$ are the divisorial ideals corresponding to P and $2P$, then $\mathfrak{a} \supsetneq \mathfrak{b}$. For $x \in \mathfrak{a} - \mathfrak{b}$, $\operatorname{div}(x) \geq P$ and $\operatorname{div}(x) \not\geq 2P$, whence $v_P(x) = 1$, which proves our assertion.

Proposition 15.1.16. *Let A be a Krull domain, K its field of fractions and $(v_P)_{P\in P(A)}$ the family of its essential valuations. Let $(n_P)_{P\in P(A)}$ be a family of integers with finite support. Then the set of $x \in K$ such that $v_P(x) \geq n_P$ for all $P \in P(A)$ is the divisorial ideal $\mathfrak{a}$ of A such that* $\operatorname{div}(\mathfrak{a}) = \sum_P n_P P$.

Proof. Let $x \in K^\times$ and $\mathfrak{a}$ the divisorial ideal such that $\operatorname{div}(\mathfrak{a}) = \sum_P n_P P$. In order that $x \in \mathfrak{a}$, it is necessary and sufficient that $Ax \subseteq \mathfrak{a}$, hence that $\operatorname{div}(x) \geq \operatorname{div}(\mathfrak{a})$ and hence, by (1.3.1), that $v_P(x) \geq n_P$ for all $P \in P(A)$. □

Proposition 15.1.17. *Let A be a Krull domain, K its field of fractions, $(v_i)_{i\in I}$ a defining family of valuations on K and A_i the ring of v_i. Let S be a multiplicative subset of A not containing* 0, *then*

$$S^{-1}A = \bigcap_{S^{-1}A\subseteq A_i} A_i.$$

In particular $S^{-1}A$ is a Krull domain.

Proof. Let $J = \{i \in I : S^{-1}A \subseteq A_i\}$ and write $B = \bigcap_{i\in J} A_i$, then we see $i \in J$ if and only if v_i is zero on S. Let $x \in B$ and $J(x)$ denote the finite set of indices $i \in I$ such that $v_i(x) < 0$. For each $i \in J(x)$ we have $x \notin A_i$, hence $i \notin J$ and so there exists $s_i \in S$ such that $v_i(s_i) > 0$. Let n_i be a positive integer such that $v_i(s_i^{n_i}x) \geq 0$ and we write $s = \prod_{i\in J} s_i^{n_i}$. Then $v_i(s_i x) \geq 0$ for all $i \in I$ and hence $sx \in A$ and $x \in s^{-1}A$. Thus $B = S^{-1}A$. □

Corollary 15.1.18. *Let P be an irreducible divisor of A and $\mathfrak{p}$ the corresponding divisorial ideal. Then $\mathfrak{p}$ is a prime ideal of height* 1, *the ring of v_P is $A_\mathfrak{p}$ and the residue field of v_P is identified with the field of fractions of $A/\mathfrak{p}$.*

Proof. By Proposition 15.1.16 we see v_P is zero on $S = A - \mathfrak{p}$ and positive on $\mathfrak{p}$, hence $\mathfrak{p} = \mathfrak{m}_{v_P} \cap A$ and $\mathfrak{p}$ is prime. On the other hand, since P is irreducible, for every divisor $Q \neq P$, $Q \not\geq P$ and hence the divisorial ideal $\mathfrak{q}$ corresponding to Q is not contained in $\mathfrak{p}$. This proves $\operatorname{ht}\mathfrak{p} = 1$ and the corollary then follows from Proposition 15.1.17 and Proposition 10.2.39 □

Corollary 15.1.19. *Let A be a Krull domain, K its field of fractions and $(v_i)_{i\in I}$ a defining family of valuations. Then every essential valuation of A is equivalent to one of the v_i.*

Proof. Let P be an irreducible divisor of A and $\mathfrak{p}$ the corresponding divisorial ideal. By Proposition 15.1.17 we have

$$A_\mathfrak{p} = \bigcap_{A_\mathfrak{p}\subseteq A_i} A_i = \bigcap_{\mathfrak{m}_i\cap A\subseteq\mathfrak{p}} A_i.$$

If $\mathfrak{m}_i \cap A = \{0\}$ then $A_i = K$ which is a contradiction, so $\mathfrak{m}_i \cap A \neq \{0\}$, and since $\mathfrak{p}$ is of height 1 we must have $\mathfrak{m}_i \cap A = \mathfrak{p}$. Since $\mathfrak{p}$ in nonzero, we then see there are only finitely many $i \in I$ such that $A_\mathfrak{p} \subseteq A_i$ by (K3). Now $A_\mathfrak{p}$ is an intersection of finitely many valuation rings and we can apply Proposition 14.4.6 Proposition 14.4.5 to claim that there is a unique $i \in I$ such that $A_\mathfrak{p} = A_i$, so v_P is equivalent to v_i. □

Proposition 15.1.20. *Let A be a Krull domain, $(v_P)_{P\in P(A)}$ the family of its essential valuations and $\mathfrak{a} \in \mathfrak{F}(A)$. Then the coefficient of P in* $\operatorname{div}(\mathfrak{a})$ *is* $\inf_{x\in\mathfrak{a}}(v_P(x))$. *If $\mathfrak{p}$ is the divisorial prime ideal corresponding to the irreducible divisor P, then $\mathfrak{a}A_\mathfrak{p} = \tilde{\mathfrak{a}}A_\mathfrak{p}$.*

Proof. As $\mathfrak{a} = \sum_{x\in\mathfrak{a}} Ax$, Proposition 15.1.4 shows that $\operatorname{div}(\mathfrak{a}) = \inf_{x\in\mathfrak{a}} \operatorname{div}(Ax)$, whence our first assertion. The second follows immediately, since $\operatorname{div}(\tilde{\mathfrak{a}}) = \operatorname{div}(\mathfrak{a})$ and $A_\mathfrak{p}$ is the ring of the discrete valuation v_P. □

Proposition 15.1.21. *Let A be an integrally closed Noetherian domain.*

(a) Let P be an irreducible divisor of A and $\mathfrak{p}$ the corresponding divisorial prime ideal. Then the n-th ***symbolic power*** *$\mathfrak{p}^{(n)}$ (that is, the saturation of $\mathfrak{p}^n$ with respect to $S = A - \mathfrak{p}$) is the set of $x \in A$ such that $v_P(x) \geq n$ and is a $\mathfrak{p}$-primary ideal.*

(b) Let $\mathfrak{a}$ be a divisorial integral ideal and $\operatorname{div}(\mathfrak{a}) = \sum_{i=1}^r n_i P_i$, with $\mathfrak{p}_i$ the corresponding prime ideal of P_i. Then

$$\mathfrak{a} = \bigcap_{i=1}^r \mathfrak{p}_i^{(n_i)}$$

is the unique reduced primary decomposition of $\mathfrak{a}$ and the $\mathfrak{p}_i$ are isolated primes of $\mathfrak{a}$.

Proof. By Corollary 15.1.18, the relation $x \in \mathfrak{p}^n A_\mathfrak{p} = (\mathfrak{p}A_\mathfrak{p})^n$ is equivalent to $v_P(x) \geq n$. On the other hand, as $A_\mathfrak{p}$ is a discrete valuation ring, $(\mathfrak{p}A_\mathfrak{p})^n$ is $(\mathfrak{p}A_\mathfrak{p})$-primary and hence $\mathfrak{p}^{(n)}$ is $\mathfrak{p}$-primary; this shows (a). Proposition 15.1.16 certainly shows that $\mathfrak{a} = \bigcap_{i=1}^r \mathfrak{p}_i^{(n_i)}$. As $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ are primes of height 1, this primary decomposition is reduced. The uniqueness follows from Proposition 12.2.10. □

15.1.5 Approximation theorem for essential valuations

As the essential valuations of a Krull domain are discrete and normed, no two of them are equivalent and hence they are independent. Corollary 14.4.11 to the approximation theorem may therefore be applied to them: given some $n_i \in \mathbb{Z}$ and some essential valuations v_i finite in number and distinct, there exists $x \in K$ such that $v_i(x) = n_i$ for all i. But here there is a more precise result:

Proposition 15.1.22. *Let $v_1, \dots, v_r$ be essential valuations of a Krull domain A and $n_1, \dots, n_r$ integers. There exists an element x of the field of fractions K of A such $v_i(x) = n_i$ for all i and $v(x) \geq 0$ for every essential valuation v of A distinct from $v_1, \dots, v_r$.*

Proof. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ be the divisorial ideals of A corresponding to the valuations $v_1, \dots, v_r$. There exists $y \in K$ such that $v_i(y) = n_i$ for all i by Corollary 14.4.11. The essential valuations $w_1, \dots, w_s$ of A distinct from the v_i for which the integer $w_i(y) = -m_j < 0$ are finite in number. Let $\mathfrak{q}_1, \dots, \mathfrak{q}_s$ be the corresponding ideals. There exists no inclusion relation between $\mathfrak{p}_1, \dots, \mathfrak{p}_r, \mathfrak{q}_1, \dots, \mathfrak{q}_s$ since these ideals correspond to irreducible divisors and these ideals are prime. Hence the integral ideal $\mathfrak{a} = \mathfrak{q}_1^{m_1} \cdots \mathfrak{q}_s^{m_s}$ is contained in none of the $\mathfrak{p}_i$ and is therefore not contained in their union. Therefore there exists $z \in \mathfrak{a}$ such that $z \notin \mathfrak{p}_i$ for all i. Then $v_i(z) = 0$ for all i and $w_j(z) \geq m_j$ for all j; hence the element $x = yz$ solves the problem. □

Corollary 15.1.23. *Let A be a Krull domain, K its field of fractions and $\mathfrak{a}$, $\mathfrak{b}$ and $\mathfrak{c}$ three divisorial fractional ideals of A such that $\mathfrak{a} \subseteq \mathfrak{b}$. Then there exists $x \in K$ such that $\mathfrak{a} = \mathfrak{b} \cap x\mathfrak{c}$.*

Proof. Let $(v_i)_{i\in I}$ be the family of essential valuations of A and let (m_i) (resp. (n_i), (p_i)) be the family of integers (zero except for a finite number of indices) such that $\mathfrak{a}$ (resp. $\mathfrak{b}$, $\mathfrak{c}$) is the set of

$x \in K$ for which $v_i(x_i) \geq m_i$ (resp. n_i, p_i) for all $i \in I$ (Proposition 15.1.16). The set J of $i \in I$ such that $m_i > n_i$ is finite. As $p_i = m_i = 0$ except for a finite number of indices, Proposition 15.1.22 shows that there exists $x \in K^\times$ such that $v_i(x^{-1}) + m_i = p_i$ for $i \in J$ and

$$v_i(x^{-1}) + m_i \geq p_i$$

for $i \in I - J$. Then, for all $i \in I$, $m_i = \sup(n_i, v_i(x) + p_i)$. Whence $\mathfrak{a} = \mathfrak{b} \cap x\mathfrak{c}$. □

Corollary 15.1.24. *Let A be a Krull domain. For a fractional ideal $\mathfrak{a}$ of A to be divisorial, it is necessary and sufficient that it be the intersection of two fractional principal ideals.*

Proof. The sufficiency is obvious. The necessity follows from Corollary 15.1.23 by taking $\mathfrak{b}$ and $\mathfrak{c}$ to be principal and such that $\mathfrak{b} \supseteq \mathfrak{a}$. □

15.1.6 Prime ideals of height 1 in a Krull domain

We have seen in Corollary 15.1.18 that irreducible divisors corresponds to prime ideals of height 1. Now we show that the converse also holds.

Theorem 15.1.25. *Let A be a Krull domain and $\mathfrak{p}$ an integral ideal of A. For $\mathfrak{p}$ to be the divisorial ideal corresponding to an irreducible divisor, it is necessary and suficient that $\mathfrak{p}$ be a prime ideal of height 1.*

Proof. If $\mathfrak{p}$ is the divisorial ideal corresponding to an irreducible divisor, we know that $\mathfrak{p}$ is prime of height 1. Conversely, let $\mathfrak{p}$ be a nonzero prime ideal. As $A_\mathfrak{p} \neq K$, by Proposition 15.1.17 $A_\mathfrak{p}$ is the intersection of a non-empty family (A_i) of essential valuation rings, each A_i being of the form $A_{\mathfrak{q}_i}$ (Corollary 15.1.18) and from $A_\mathfrak{p} \subseteq A_{\mathfrak{q}_i}$ we deduce that $\mathfrak{q}_i \subseteq \mathfrak{p}$. Thus, if $\mathfrak{p}$ is of height 1, then $\mathfrak{p} = \mathfrak{q}$, which shows that $\mathfrak{p}$ is the divisorial ideal corresponding to an irreducible divisor. □

Corollary 15.1.26. *In a Krull domain every non-zero prime ideal $\mathfrak{p}$ contains a prime ideal of height 1. If $\mathfrak{p}$ is not of height 1, then $\operatorname{div}(\mathfrak{p}) = 0$ and $(A : \mathfrak{p}) = A$.*

Proof. The first assertion is clear. If $\mathfrak{p}$ is not of height 1 and $\mathfrak{q}$ is a prime ideal of height 1 contained in $\mathfrak{p}$, then $\mathfrak{q} \subseteq \tilde{\mathfrak{p}}$ and $\mathfrak{q} \neq \tilde{\mathfrak{p}}$. As $\operatorname{div}(\mathfrak{q})$ is irreducible, necessarily $\operatorname{div}(\mathfrak{p}) = \operatorname{div}(\tilde{\mathfrak{p}}) = 0$; hence $\operatorname{div}(A : \mathfrak{p}) = 0$ and, as $(A : \mathfrak{p})$ is divisorial, we get $(A : \mathfrak{p}) = A$. □

Corollary 15.1.27. *Let A be a Krull domain, K its field of fractions, v a valuation on K which is positive on A and $\mathfrak{p}$ the set of $x \in A$ such that $v(x) > 0$. If the prime ideal $\mathfrak{p}$ is of height 1, v is equivalent to an essential valuation of A.*

Proof. Let B be the ring of v and $\mathfrak{m}$ its ideal. Then $\mathfrak{m} \cap A = \mathfrak{p}$ and hence $A_\mathfrak{p} \subseteq B$. Now $A_\mathfrak{p}$ is a DVR by Theorem 15.1.25 and $B \neq K$, thus $B = A_\mathfrak{p}$. □

Theorem 15.1.28. *Let A be an integral domain. For A to be a Krull domain, it is necessary and suficient that the following properties are satisfied:*

(a) For all prime ideal $\mathfrak{p}$ of A of height 1, $A_\mathfrak{p}$ is a DVR.

(b) $A = \bigcap_{\operatorname{ht}\mathfrak{p}=1} A_\mathfrak{p}$.

(c) For all $x \neq 0$ in A, there exists only a finite number of prime ideals $\mathfrak{p}$ of height 1 such that $x \in \mathfrak{p}$.

Moreover, in the admissible case, the valuations corresponding to the A for prime ideals of height 1 *are the essential valuations of A.*

Proof. The conditions are trivially sufficient. Their necessity follows immediately from Theorem 15.1.25, Corollary 15.1.18 and the fact that the essential valuations of A is a defining family. □

Proposition 15.1.29. *Let A be an integrally closed Noetherian domain and $\mathfrak{a}$ an integral ideal of A. Then $\mathfrak{a}$ is divisorial if and only if the prime ideals associated with $A/\mathfrak{a}$ are of height* 1.

Proof. Recall that, if $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ is a reduced primary decomposition of $\mathfrak{a}$ and $\mathfrak{p}_i$ denotes the prime ideal corresponding to $\mathfrak{q}_i$, the prime ideals associated with $A/\mathfrak{a}$ are just the $\mathfrak{p}_i$. The necessity then follows from Proposition 15.1.21. Conversely, if, in the above notation, the $\mathfrak{p}_i$ are of height 1, then $A_{\mathfrak{p}_i}$ is a DVR and each $\mathfrak{p}_i$ is isolated, so $\mathfrak{q}_i = \mathfrak{q}_i A_{\mathfrak{p}_i} \cap A$ (Proposition 12.2.4). Denoting by v_i the essential valuation corresponding to $\mathfrak{p}_i$, there therefore exists an integer n_i such that $\mathfrak{q}_i$ is the set of $x \in A$ such that $v_i(x) \geq n_i$ (n_i is just the integer such that $\mathfrak{q}_i A_{\mathfrak{p}_i} = (\mathfrak{p}_i A_{\mathfrak{p}_i})^{n_i}$ in $A_{\mathfrak{p}_i}$). This shows the $\mathfrak{q}_i$ are divisorial by Proposition 15.1.16, hence also is $\mathfrak{a}$. □

Proposition 15.1.30. *Let A be a local Krull domain (in particular an integrally closed local Noetherian domain) and $\mathfrak{m}$ its maximal ideal. The following conditions are equivalent:*

(i) *A is a DVR;*

(ii) *$\mathfrak{m}$ is invertible;*

(iii) *$(A : \mathfrak{m}) \neq A$;*

(iv) *$\mathfrak{m}$ is divisorial;*

(v) *$\mathfrak{m}$ is the only non-zero prime ideal of A.*

Proof. As every non-zero ideal of a DVR is principal, it is invertible and hence (i) implies (ii). If $\mathfrak{m}$ is invertible, its inverse is $(A : \mathfrak{m})$ and hence $(A : \mathfrak{m}) \neq A$, hence (ii) implies (iii). If $(A : \mathfrak{m}) \neq A$, then $(A : (A : \mathfrak{m})) \neq A$. Now $\mathfrak{m} \subseteq (A : (A : \mathfrak{m}))$, hence $\mathfrak{m} = (A : (A : \mathfrak{m}))$ since $\mathfrak{m}$ is maximal, so that $\mathfrak{m}$ is divisorial. Thus (iii) implies (iv). The fact that (iv) implies (v) follows from Theorem 15.1.25, Finally, if $\mathfrak{m}$ is the only non-zero prime ideal of A, it is of height 1 and hence $A_{\mathfrak{m}}$ is a DVR by Theorem 15.1.28. As A is local, $A_{\mathfrak{m}} = A$, which shows that (v) implies (i). □

15.1.7 Permanence properties of Krull domains

Proposition 15.1.31. *Let A be a Krull domain, K its field of fractions, L a finite extension of K and R the integral closure of A in L. Then R is a Krull domain. The essential valuations of R are the normed discrete valuations on L which are equivalent to the extensions of the essential valuations of A.*

Proof. Let $(v_i)_{i \in I}$ be a complete family of extensions to L of the essential valuations of A. Since the degree $n = [L : K]$ is finite, the v_i are discrete valuations on L by Corollary 14.6.9. Let B_i be the ring of v_i. Then $R \subseteq \bigcap_{i \in I} B_i$ by Theorem 14.1.8. Conversely, every element of $x \in \bigcap_i B_i$ is integral over each of the essential valuation rings of A by Corollary 14.1.10, hence the coefficients of the minimal polynomial of x over K belong to A (Corollary 13.1.28), so that

$x \in R$; thus $R = \bigcap_i B_i$. Now let x be a non-zero element of R. It satisfies an equation of the form

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

where $a_i \in A$ and $a_0 \neq 0$. If $v_i(x) > 0$, then $v_i(a_0) > 0$. Now the essential valuations v of A such that $v(a_0) > 0$ are finite in number and the valuations on L extending a given valuation on K are also finite in number, hence $v_i(x) = 0$ except for a finite number of indices $i \in I$. Thus it has been proved that R is a Krull domain.

It remains to show that the v_i are equivalent to essential valuations of R, that is, that the prime ideal $\mathfrak{p}_i$ consisting of the $x \in R$ such that $v_i(x) > 0$ is of height 1. If this were not so, there would exist a prime ideal $\mathfrak{q}$ of R such that $(0) \subseteq \mathfrak{q} \subseteq \mathfrak{p}_i$ distinct from (0) and $\mathfrak{p}_i$. Then $(0) \subseteq \mathfrak{q} \cap A \subseteq \mathfrak{p}_i \cap A$ and $\mathfrak{q} \cap A$ would be distinct from (0) and $\mathfrak{p}_i \cap A$ by Corollary 13.1.64. The prime ideal $\mathfrak{p}_i \cap A$ would therefore not be of height 1, which contradicts the fact that it corresponds to an essential valuation of A. □

Corollary 15.1.32. *Let $\mathfrak{p}$ (resp. $\mathfrak{P}$) be a prime ideal of A (resp. R) of height 1 and v (resp. w) the essential valuation of A (resp. R) corresponding to it. For $\mathfrak{P}$ to lie over $\mathfrak{p}$, it is necessary and sufficient that the restriction of w to K be equivalent to v.*

Proof. The valuation w is equivalent to the extension of an essential valuation v' of A. Let $\mathfrak{q} = \mathfrak{P} \cap A$, which is a prime ideal of A of height 1. For the restriction of w to K to be equivalent to v, it is necessary and suflicient that $v' = v$ and hence that $\mathfrak{q} = \mathfrak{p}$. □

Lemma 15.1.33. *Let A be an integral domain, K its field of fraction and L an extension of K. If $(A_i)_{i\in I}$ is a family of Krull domains contained in L satisfying the following two conditions:*

(a) $A = \bigcap_i A_i$.

(b) Each nonzero element of A is a nonunit in only finitely many A_i.

Then A is a Krull doamin.

Proof. For each $i \in I$ let $(v_{ij})_{j\in J_i}$ be a defining family of valuations of A_i. Let $x \in A$ be nonzero, then x is not a unit for only finitely many A_i's. Also, for each i, since A_i is a Krull domain, $v_{ij}(x) \neq 0$ for only finitely many $j \in J_i$, whence we see the family $(v_{ij})_{i\in I, j\in J_i}$ satisfies the condition (K3) and hence A is a Krull domain. □

Proposition 15.1.34. *Let A be a Krull domain, then the ring $A[X_1, \ldots, X_n]$ is a Krull domain.*

Proof. Arguing by induction on n, it is sufficient to show that, if X is an indeterminate, $A[X]$ is a Krull domain. Let K be the field of fractions of A. The field of fractions of $A[X]$ is $K(X)$. The ring $K[X]$ is a PID and therefore a Krull ring. Moreover, for every prime ideal $\mathfrak{p}$ of A of height 1, let $\bar{v}_\mathfrak{p}$ be the extension of v to $K(X)$ defined by

$$\bar{v}_\mathfrak{p}\Big(\sum_j a_j X^j\Big) = \inf_j v_\mathfrak{p}(a_j)$$

for $\sum_j a_j X^j \in K[X]$. Then the valuation ring of $\bar{v}_\mathfrak{p}$ in $K(X)$ is $A[X]_{\mathfrak{p}A[X]}$. We also note that $K \cap A[X]_{\mathfrak{p}A[X]} = A_\mathfrak{p}[X]$, in fact, for $\sum_j a_j X^j \in K[X]$, the relation $\bar{v}_\mathfrak{p}(\sum_j a_j X^j) \geq 0$ is equivalent

to $v_{\mathfrak{p}}(a_j) \geq 0$ for all j, hence equivalent to $\sum_j a_j X^j \in A_{\mathfrak{p}}[X]$. With this, we have

$$A[X] = K[X] \cap \bigcap_{\mathrm{ht}\mathfrak{p}=1} A[X]_{\mathfrak{p}A[X]}$$

Since A is Krull we see every nonzero element in $A[X]$ is a nonunit in only finitely many $A_{\mathfrak{p}}[X]$, so the condition of Lemma 15.1.33 is satisfied and we see $A[X]$ is a Krull domain. □

Corollary 15.1.35. *Let A be a Krull domain, then the prime ideals of $A[X]$ of height 1 are:*

(a) the prime ideals of the form $\mathfrak{p}A[X]$, where $\mathfrak{p}$ is a prime ideal of A of height 1;

(b) the prime ideals of the form $\mathfrak{m} \cap A[X]$, where $\mathfrak{m}$ is a (necessarily principal) prime ideal of $K[X]$.

Proof. This follows from the observation that that the prime ideals of height 1 in $K[X]$ are exactly maximal ideals. □

Proposition 15.1.36. *Let A be a Krull domain, then the ring $A[\![X_1, \ldots, X_n]\!]$ is a Krull domain.*

Proof. By induction we only need to show $A[\![X]\!]$ is Krull. Since A is Krull we have $A = \bigcap_{\mathrm{ht}\mathfrak{p}=1} A_{\mathfrak{p}}$, and therefore $A[\![X]\!] = \bigcap_{\mathrm{ht}\mathfrak{p}=1} A_{\mathfrak{p}}[\![X]\!]$. Also, each $A_{\mathfrak{p}}$ is a DVR and thus $A_{\mathfrak{p}}[\![X]\!]$ is integrally closed and Noetherian, hence a Krull domain. However, as X is a non-unit of all the rings $A_{\mathfrak{p}}[\![X]\!]$, we can not apply Lemma 15.1.33 directly. On the other hand, note that

$$A[\![X]\!] = K[\![X]\!] \cap \bigcap_{\mathrm{ht}\mathfrak{p}=1} (A_{\mathfrak{p}}[\![X]\!][X^{-1}]).$$

Now the hypothesis in Lemma 15.1.33 is easily verified for the rings $A_{\mathfrak{p}}[\![X]\!][X^{-1}]$. Indeed, an element $f(X) = \sum_{i=r}^{\infty} a_i X^i$ (with $a_r \neq 0$) in $A[\![X]\!]$ is a nonunit in $A_{\mathfrak{p}}[\![X]\!][X^{-1}]$ if and only if a_r is a nonunit of $A_{\mathfrak{p}}$, and there finitely many such $\mathfrak{p}$. Therefore $A[\![X]\!]$ is a Krull domain. □

15.1.8 Divisor classes in a Krull domain

Let A be a Krull domain. Recall that the group $\mathfrak{D}(A)$ of divisors of A is the free commutative group generated by the set $P(A)$ of its irreducible elements and that $P(A)$ is identified with the set of prime ideals of A of height 1. For $\mathfrak{p} \in P(A)$ we shall denote by $v_{\mathfrak{p}}$ the normed essential valuation corresponding to $\mathfrak{p}$. Recall that the ring of $v_{\mathfrak{p}}$ is $A_{\mathfrak{p}}$. We shall denote by $\mathfrak{P}(A)$ the subgroup of $\mathfrak{D}(A)$ consisting of the principal divisors and by $\mathfrak{C}(A) = \mathfrak{D}(A)/\mathfrak{P}(A)$ the divisor class group of A.

Proposition 15.1.37. *Let A be a Krull domain and B a Krull domain containing A. Suppose that the following condition holds*

(PD) For every prime ideal $\mathfrak{P}$ of B of height 1, the prime ideal $\mathfrak{P} \cap A$ is zero or of height 1.

For $\mathfrak{p} \in P(A)$ the $\mathfrak{P} \in P(B)$ such that $\mathfrak{P} \cap A = \mathfrak{p}$ are finite in number. We write

$$i(\mathfrak{p}) = \sum_{\mathfrak{P} \in P(B), \mathfrak{P} \cap A = \mathfrak{p}} e(\mathfrak{P}/\mathfrak{p})\mathfrak{P},$$

where $e(\mathfrak{P}/\mathfrak{p})$ denotes the ramification index of $v_{\mathfrak{P}}$ over $v_{\mathfrak{p}}$. Then i defines, by linearity, an increasing homomorphism of $\mathfrak{D}(A)$ to $\mathfrak{D}(B)$, which enjoys the following properties:

(a) for every non-zero element x of the field of fractions of A,

$$i(\mathrm{div}_A(x)) = \mathrm{div}_B(x),$$

(b) for all D_1, D_2 in $\mathfrak{D}(A)$,

$$i(\sup\{D_1, D_2\}) = \sup\{i(D_1), i(D_2)\}.$$

Proof. Let $\mathfrak{p} \in P(A)$, consider a non-zero element a of $\mathfrak{p}$; the $\mathfrak{P} \in P(B)$ which contain a are finite in number by Theorem 15.1.28. A fortiori the $\mathfrak{P} \in P(B)$ such that $\mathfrak{P} \cap A = \mathfrak{p}$ are finite in number. We now show (a). By additivity, it may be assumed that $x \in A - \{0\}$. By definition, $\mathrm{div}_B(x) = \sum_{\mathfrak{P}\in P(B)} v_{\mathfrak{P}}(x)\mathfrak{P}$. For all $\mathfrak{P} \in P(B)$ such that $v_{\mathfrak{P}}(x) > 0$, $\mathfrak{P} \cap A$ is non-zero (for x is in it) and is therefore of height 1 by (PD). Setting $\mathfrak{p} = \mathfrak{P} \cap A$, by definition of the ramification index, $v_{\mathfrak{P}}(x) = e(\mathfrak{P}/\mathfrak{p})v_{\mathfrak{p}}(x)$ (since $v_{\mathfrak{P}}$ and $v_{\mathfrak{p}}$ are normed). As $\mathrm{div}_A(x) = \sum_{\mathfrak{p}\in P(A)} v_{\mathfrak{p}}(x)\mathfrak{p}$, and $i(\mathfrak{q}) = 0$ for all $\mathfrak{q} \in P(A)$ wich is not of the form $\mathfrak{Q} \cap A$ for some $\mathfrak{Q} \in P(B)$, we deduce (a).

To prove (b) we write

$$D_1 = \sum_{\mathfrak{p}\in P(A)} n_1(\mathfrak{p})\mathfrak{p}, \quad D_2 = \sum_{\mathfrak{p}\in P(A)} n_2(\mathfrak{p})\mathfrak{p}$$

the coefficient of $\mathfrak{p}$ in $\sup\{D_1, D_2\}$ is $\sup\{n_1(\mathfrak{p}), n_2(\mathfrak{p})\}$. Let $\mathfrak{P}$ be an element of $P(B)$. If $\mathfrak{P} \cap A = (0)$, the coefficients of $\mathfrak{P}$ in $i(D_1)$, $i(D_2)$, and hence also in $\sup\{i(D_1), i(D_2)\}$ are zero. Also the coefficient of $\mathfrak{P}$ in $i(\sup\{D_1, D_2\})$ is zero. If $\mathfrak{P} \cap A \neq (0)$, it is a prime ideal $\mathfrak{p}$ of height 1 (by (PD)); writing $e = e(\mathfrak{P}/\mathfrak{p})$, the coeflicients of $\mathfrak{P}$ in $i(D_1)$, $i(D_2)$ and $i(\sup\{D_1, D_2\})$ are respectively $en_1(\mathfrak{p})$, $en_2(\mathfrak{p})$ and $e \sup\{n_1(\mathfrak{p}), n_2(\mathfrak{p})\}$. That of $\sup\{i(D_1), i(D_2)\}$ is

$$\sup\{en_1(\mathfrak{p}), en_2(\mathfrak{p})\} = e \sup\{n_1(\mathfrak{p}), n_2(\mathfrak{p})\}.$$

This proves (b). □

Under the hypotheses of Proposition 15.1.37, it follows from (a) that i defines, by taking quotients, a canonical homomorphism $\bar{i}$ of $\mathfrak{C}(A)$ to $\mathfrak{C}(B)$.

Example 15.1.38. Let A, B be Krull domains and B be integral over A. In this case, for the prime ideal $\mathfrak{P}$ of B to be of height 1, it is necessary and sufficient that $\mathfrak{p} = \mathfrak{P} \cap A$ be of height 1 (Corollary 13.1.64), so the condition (PD) is satisfied.

Proposition 15.1.39. *Let A and B be Krull domains such that B contains A and is a flat A-module. Then:*

(a) the condition (PD) is satisfied;

(b) for every divisorial ideal $\mathfrak{a}$ of A, $B\mathfrak{a}$ is the divisorial ideal of B which corresponds to the divisor $i(\mathrm{div}_A(\mathfrak{a}))$.

Proof. To show (a), suppose that there exists a prime ideal $\mathfrak{P}$ of B of height 1 such that $\mathfrak{P} \cap A$ is neither 0 nor of height 1. Take an elemcnt $x \neq 0$ in $\mathfrak{P} \cap A$. The ideals $\mathfrak{p}_i$ of A of height 1 which contain x are finite in number and none contains $\mathfrak{P} \cap A$. There therefore exists an element y of $\mathfrak{P} \cap A$ such that $y \notin \mathfrak{p}_i$ for all i. Thus $\mathrm{div}_A(x)$ and $\mathrm{div}_A(y)$ are relatively prime elements of the

ordered group $\mathfrak{D}(A)$, so that

$$\sup\{\mathrm{div}_A(x), \mathrm{div}_A(y)\} = \mathrm{div}_A(x) + \mathrm{div}_A(y) = \mathrm{div}_A(xy).$$

As $\sup\{\mathrm{div}_A(x), \mathrm{div}_A(y)\} = \mathrm{div}(Ax \cap Ay)$ and the ideals $Ax \cap Ay$ and Axy are divisorial, we deduce that $Ax \cap Ay = Axy$. Since B is a flat A-module, this implies $Bx \cap By = Bxy$ (Proposition 7.3.16), and therefore

$$\sup\{v_{\mathfrak{P}}(x), v_{\mathfrak{P}}(y)\} = v_{\mathfrak{P}}(Bx \cap By) = v_{\mathfrak{P}}(xy) = v_{\mathfrak{P}}(x) + v_{\mathfrak{P}}(y).$$

Since $v_{\mathfrak{P}}(x)$ and $v_{\mathfrak{P}}(y)$ are positive integers (which hold since x and y are in $\mathfrak{P}$), this is a contradiction. Thus (a) has been proved by reductio ad absurdum.

We now show (b). If $\mathfrak{a}$ is a divisorial ideal of A, it is the intersection of two fractional principal ideals (Corollary 15.1.24), say

$$\mathfrak{a} = d^{-1}(Aa \cap Ab)$$

where a, b, d are in A and nonzero. As B is flat over A, $Ba = d^{-1}(Ba \cap Bb)$, which shows that $B\mathfrak{a}$ is divisorial. This shows also that $\mathrm{div}_B(B\mathfrak{a}) = \sup\{\mathrm{div}_B(a), \mathrm{div}_B(b)\} - \mathrm{div}_B(d)$, using Proposition 15.1.37 (a) and (b), it is seen that

$$\begin{aligned}\mathrm{div}_B(B\mathfrak{a}) &= \sup\{i(\mathrm{div}_A(a)), i(\mathrm{div}_A(b))\} - i(\mathrm{div}_A(d))\\ &= i(\sup\{\mathrm{div}_A(a), \mathrm{div}_A(b)\}) - i(\mathrm{div}_A(d))\\ &= i(\mathrm{div}_A(Aa \cap Ab)) - i(\mathrm{div}_A(d))\\ &= i(\mathrm{div}_A(d^{-1}(Aa \cap Ab))) = i(\mathrm{div}_A(a))\end{aligned}$$

which completes the proof. □

Corollary 15.1.40. *Let A be a local Krull domain and B a DVR such that B dominates A and is a flat A-module. Then A is a field or a DVR.*

Proof. Let $\mathfrak{M}$ be the maximal ideal of B. By (PD), $\mathfrak{M} \cap A$ is zero or of height 1. As it is, by hypothesis the maximal ideal of A, our assertion follows from Proposition 15.1.30. □

Remark 15.1.2. As the elements of $P(B)$ form a basis of $\mathfrak{D}(B)$ and two distinct ideals of $P(A)$ cannot be the traces on A of the same ideal of $P(B)$, for the injectivity of i it amounts to verifying that $i(\mathfrak{p}) \neq 0$ for all $\mathfrak{p} \in P(A)$. Now this is equivalent to say every $\mathfrak{p} \in P(A)$ is the contraction of an element in $P(B)$, and in particular this holds if B is a faithfully flat A-algebra or B is a superring of A and integral over A.

In what follows, we propose to study the canonical homomorphism i from $\mathfrak{C}(A)$ to $\mathfrak{C}(B)$ for certain ordered pairs of Krull domains A, B.

Proposition 15.1.41. *Let A be a Zariski ring such that its completion $\widehat{A}$ is a Krull domain. Then A is a Krull domain and the canonical homomorphism $\bar{i}$ from $\mathfrak{C}(A)$ to $\mathfrak{C}(\widehat{A})$ (which is defined since $\widehat{A}$ is a flat A-module) is injective.*

Proof. As $\widehat{A}$ is an integral domain and $A \subseteq \widehat{A}$, A is an integral domain. Let L be the field of fractions of $\widehat{A}$ and $K \subseteq L$ that of A. As $A = \widehat{A} \cap K$ (Corollary 11.4.30), A is a Krull domain. The

fact that $\bar{i} : \mathfrak{C}(A) \to \mathfrak{C}(\widehat{A})$ is injective follows from Proposition 15.1.39 and the fact that, if $\mathfrak{b}\widehat{A}$ is principal, $\mathfrak{b}$ is principal (Corollary 11.4.29) □

Now let A be a Krull domain and S a multiplicative subset of A not containing 0. The group $\mathfrak{D}(A)$ (resp. $\mathfrak{D}(S^{-1}A)$ is the free commutative group with basis the set of $\operatorname{div}(\mathfrak{p})$ (resp. $\operatorname{div}(S^{-1}\mathfrak{p})$), where $\mathfrak{p}$ runs through the set of prime ideals of A of height 1 (resp. the set of prime ideals of A of height 1 such that $\mathfrak{p} \cap S = \varnothing$) and, if $\mathfrak{p} \cap S = \varnothing$, then $i(\operatorname{div}(\mathfrak{p})) = \operatorname{div}(S^{-1}\mathfrak{p})$. Thus $\mathfrak{D}(S^{-1}A)$ is identified with the direct factor of $\mathfrak{D}(A)$ generated by the elements $\operatorname{div}(\mathfrak{p})$ such that $\mathfrak{p} \cap S = \varnothing$ and admits as complement the free commutative subgroup of $\mathfrak{D}(A)$ with basis the set of $\operatorname{div}(\mathfrak{p})$ such that $\mathfrak{p} \cap S \neq \varnothing$. We shall denote this complement by $\mathfrak{G}(S)$. As the map $i : \mathfrak{D}(A) \to \mathfrak{D}(S^{-1}A)$ is suijective, so is the induced map $\bar{i} : \mathfrak{C}(A) \to \mathfrak{C}(S^{-1}A)$ and

$$\ker \bar{i} = (\mathfrak{G}(S) + \mathfrak{P}(A))/\mathfrak{P}(A) = \mathfrak{G}(S)/(\mathfrak{G}(S) \cap \mathfrak{P}(A)). \tag{1.8.1}$$

In fact, if an element of $\mathfrak{D}(S^{-1}A)$ is equal to $\operatorname{div}_{S^{-1}A}(x/s)$, where $x \in A$ and $s \in S$, it is then the image under i of the principal divisor $\operatorname{div}_A(x/s)$ (Proposition 15.1.37).

Proposition 15.1.42. *Let A be a Krull domain and S a multiplicative subset of A not containing 0. Then the canonical homomorphism $\bar{i}$ from $\mathfrak{C}(A)$ to $\mathfrak{C}(S^{-1}A)$ is suijective. If further S is generated by a family of elements p_i such that the principal ideals Ap_i are all prime, then $\bar{i}$ is bijective.*

Proof. Suppose now that S is generated by a family of elements $(p_i)_{i\in I}$ of A such that the principal ideals Ap_i are all prime. Then, if $\mathfrak{p}$ is a prime ideal of A of height 1 such that $p \cap S \neq \varnothing$, $\mathfrak{p}$ contains a product of powers of the p_i and therefore one of the p_i, say p_0. As Ap_0 is non-zero and prime and $\mathfrak{p}$ is of height 1, it follows that $\mathfrak{p} = Ap_0$. In the above notation, we then have $\mathfrak{G}(S) \subseteq \mathfrak{P}(A)$ and the kernel of $\bar{i}$ is zero. □

Proposition 15.1.43. *Let R be a Krull domain and consider the polynomial ring $R[X]$. The canonical homomorphism of $\mathfrak{C}(R)$ to $\mathfrak{C}(R[X])$ is bijective.*

Proof. Let R be a Krull domain; take A to be the polynomial ring $A = R[X]$ and S to be the set $R - (0)$ of non-zero constant polynomials of A. The prime ideals $\mathfrak{p}$ of A of height 1 such that $\mathfrak{p} \cap S \neq \varnothing$ are those of the form $\mathfrak{p}_0 A$, where $\mathfrak{p}_0$ is a prime ideal of R of height 1. Hence, in the notation introduced above, $\mathfrak{G}(S)$ is identified with $\mathfrak{D}(R)$ by identifying $\operatorname{div}_A(\mathfrak{p}_0 A)$ with $\operatorname{div}_R(\mathfrak{p}_0)$. On the other hand $\mathfrak{G}(S) \cap \mathfrak{P}(A)$ is identified with $\mathfrak{P}(R)$: for if an ideal $\mathfrak{a}_0$ of R generates a principal ideal $f(X)A$ in $A = R[X]$, then $f(0) \in \mathfrak{a}_0 A$ since $\mathfrak{a}_0 A$ is a graded ideal of the ring A (graded by the usual degree of polynomials) and hence $f(0) \in \mathfrak{a}_0$. Further, for any $a \in \mathfrak{a}_0$ we have $a = f(X)g(X)$ where $g(X) \in R$, whence $a = f(0)g(0)$. It follows that $\mathfrak{a}_0$ is the principal ideal of R generated by $f(0)$. Finally, denoting by K the field of fractions of R, $S^{-1}A$ is identified with the polynomials ring $K[X]$, which is a principal ideal domain; hence $\mathfrak{C}(S^{-1}A) = (0)$. Thus $\mathfrak{C}(A) = \ker \bar{i}$ is identified with $\mathfrak{C}(R)$ and we have proved the proposition. □

15.1.9 Dedekind domains

Let A be an integral domain. Clearly the following conditions are equivalent:

(i) no two of the non-zero prime ideals of A are comparable with respect to inclusion;

(ii) the non-zero prime ideals of A are maximal;

(iii) the non-zero prime ideals of A are of height 1.

A Krull domain which satisfies the above equivalent conditions is called a **Dedekind domain**.

Example 15.1.44 (Examples of Dedekind domains).

(a) Every principal ideal domain is a Dedekind domain.

(b) Let K be a finite extension of $\mathbb{Q}$ and A the integral closure of $\mathbb{Z}$ over K. The ring A is a Krull domain by Proposition 15.1.31. Let $\mathfrak{p}$ be a non-zero prime ideal of A. Then by the going down theorem $\mathfrak{p} \cap Z$ is non-zero and hence is a maximal ideal of $\mathbb{Z}$. Hence $\mathfrak{p}$ is a maximal ideal of A. Therefore, A is a Dedekind domain. In general, A is not a principal ideal domain.

(c) Let V be an affine algebraic variety and A the ring of functions regular on V. Suppose that A is not a field (i.e. that V is not reduced to a point). For A to be a Dedekind domain, it is necessary and sufficient that V be an irreducible curve with no singular point: for to say that A is an integral domain amounts to saying that V is irreducible; to say that every non-zero prime ideal of A is maximal amounts to saying that $\dim A = 1$, so A is a curve; finally, as A is Noetherian, to say that it is a Krull domain amounts to saying that it is integrally closed, that is, V is a normal curve, or also that it has no singular point.

(d) A ring of fractions $S^{-1}A$ of a Dedekind domain A is a Dedekind domain if $0 \notin S$. For $S^{-1}A$ is a Krull domain and every nonzero prime ideal of $S^{-1}A$ is maximal.

Theorem 15.1.45. *Let A be an integral domain and K its field of fractions. Then the following conditions are equivalent:*

(i) A is a Dedekind domain;

(ii) A is a Krull domain and every nontrivial valuation on K which is positive on A is equivalent to an essential valuation of A;

(iii) A is a Krull domain and every nonzero fractional ideal $\mathfrak{a}$ of A is divisorial;

(iv) every nonzero fractional ideal $\mathfrak{a}$ of A is invertible;

(v) A is a Noetherian integrally closed domain and every non-zero prime ideal of A is maximal;

(vi) A is Noetherian and, for every maximal ideal $\mathfrak{m}$ of A, $A_{\mathfrak{m}}$ is either a field or a DVR;

(vii) A is Noetherian and, for every maximal ideal $\mathfrak{m}$ of A, $A_{\mathfrak{m}}$ is a PID.

Proof. We show first the equivalence of (i) and (ii). Corollary 15.1.27 shows immediately that (i) implies (ii). Conversely, (ii) implies (i), since, for every prime ideal $\mathfrak{p}$ of A, there exists a valuation ring of K which dominates $A_{\mathfrak{p}}$, and (ii) this implies that $\mathfrak{p}$ has height 1, so A is a Dedekind domain.

If A is a Dedekind domain and $\mathfrak{a}$ is a non-zero fractional ideal, then $\mathfrak{a}A_{\mathfrak{m}} = \tilde{\mathfrak{a}}A_{\mathfrak{m}}$ for every maximal ideal $\mathfrak{m}$ (by Proposition 15.1.20) and hence $\mathfrak{a} = \tilde{\mathfrak{a}}$; thus (i) implies (iii).

We now show that (iii) implies (iv). If (iii) holds, the mapping $\mathfrak{a} \mapsto \operatorname{div}(\mathfrak{a})$ is a bijection of $\mathfrak{F}(A)$ onto $\mathfrak{D}(A)$, as it is a homomorphism and $\mathfrak{D}(A)$ is a group, every element of $\mathfrak{F}(A)$ is invertible.

We show that (iv) implies (v). If (iv) holds, every integral ideal of A is finitely generated and hence A is Noetherian. As $\mathfrak{F}(A)$ is a group, $\mathfrak{D}(A)$ is a group and A is therefore completely integrally closed. Finally, if $\mathfrak{p}$ is a non-zero prime ideal of A and $\mathfrak{m}$ is a maximal ideal of A containing $\mathfrak{p}$, the ring $A_\mathfrak{m}$ is a PID by Theorem 10.5.23. As $\mathfrak{p}A_\mathfrak{m}$ is prime and non-zero, necessarily $\mathfrak{p}A_\mathfrak{m} = \mathfrak{m}A_\mathfrak{m}$, whence $\mathfrak{p} = \mathfrak{m}$ and $\mathfrak{p}$ is maximal.

We now show that (v) implies (vi). If $\mathfrak{m}$ is a maximal ideal of A and (v) holds, $A_\mathfrak{m}$ is an integrally closed Noetherian domain and its maximal ideal $\mathfrak{m}A_\mathfrak{m}$ is, either (0), or the only non-zero prime ideal of $A_\mathfrak{m}$. Hence $A_\mathfrak{m}$ is a field or a DVR by Proposition 15.1.30.

The fact (vi) implies (vii) is obvious. We show finally that (vii) implies (i). As A is the intersection of the $A_\mathfrak{m}$ where $\mathfrak{m}$ runs through the set of maximal ideals (Proposition 10.3.25), (vii) implies that A is integrally closed and Noetherian and hence that A is a Krull domain. On the other hand, it can be shown that every non-zero prime ideal of A is maximal as in the proof that (iv) implies (v). □

Proposition 15.1.46. *A semi-local Dedekind domain is a PID.*

Proof. Let A be a semi-local Dedekind domain, K its field of fractions, $\mathfrak{m}_1, \dots, \mathfrak{m}_n$ its maximal ideals and $v_1, \dots, v_n$ the corresponding essential valuations. These are the only essential valuations of A. Let $\mathfrak{a}$ be a non-zero integral ideal of A. Since it is divisorial, there exists integers $q_1, \dots, q_r$ such that $\mathfrak{a}$ is the set of $x \in K$ such that $v_i(x) \geq \mathfrak{q}_i$ for all i (Proposition 15.1.21). Let x_0 be an element of K such that $v_i(x_0) = q_i$ for all i (Proposition 15.1.22). Then $\mathfrak{a}$ is the set of $x \in K$ such that $v_i(xx_0^{-1}) \geq 0$ for all i and thus $\mathfrak{a} = Ax_0$. □

If A is a Dedekind domain, it has been seen, in Theorem 15.1.45, that the group $\mathfrak{D}(A)$ of divisors of A is identified with the group $\mathfrak{F}(A)$ of nonzero fractional ideals $\mathfrak{a}$ (as A is Noetherian, every non-zero fractional ideal is finitely generated). The divisor class group $\mathfrak{C}(A)$ of A is then identified with the group of class of nonzero ideals of A.

Let A be a Dedekind domain, $\mathfrak{F}(A)$ the ordered multiplicative group of nonzero fractional ideals of A and $\mathfrak{D}(A)$ the group of divisors of A. The isomorphism $\mathfrak{a} \mapsto \operatorname{div}(\mathfrak{a})$ of $\mathfrak{F}(A)$ onto $\mathfrak{D}(A)$ maps the non-zero prime ideals of A to irreducible divisors and hence the multiplicative group $\mathfrak{F}(A)$ admits as basis the set of non-zero prime ideals of A. In other words, every non-zero fractional ideal $\mathfrak{a}$ of A admits a unique decomposition of the form:

$$\mathfrak{a} = \prod \mathfrak{p}^{n_\mathfrak{p}} \tag{1.9.1}$$

where the product extends to the non-zero prime ideals of A, and the exponents $n_\mathfrak{p}$ equals $v_\mathfrak{p}(\mathfrak{a})$, where $v_\mathfrak{p}$ denotes the essential valuation corresponding to $\mathfrak{p}$. Further $\mathfrak{a}$ is integral if and only if the $n_\mathfrak{p}$ are all positive. The relation (1.9.1) is called the **decomposition of $\mathfrak{a}$ into prime factors**. For $\mathfrak{a}, \mathfrak{b} \in \mathfrak{F}(A)$, write

$$\mathfrak{a} = \prod \mathfrak{p}^{n_\mathfrak{p}}, \quad \mathfrak{b} = \prod \mathfrak{p}^{m_\mathfrak{p}}$$

then we have

$$\mathfrak{a}\mathfrak{b} = \prod \mathfrak{p}^{n_\mathfrak{p}+m_\mathfrak{p}}, \quad (\mathfrak{a} : \mathfrak{b}) = \mathfrak{a}\mathfrak{b}^{-1} = \prod \mathfrak{p}^{n_\mathfrak{p}-m_\mathfrak{p}},$$

$$\mathfrak{a} + \mathfrak{b} = \prod \mathfrak{p}^{\inf\{n_\mathfrak{p},m_\mathfrak{p}\}}, \quad \mathfrak{a} \cap \mathfrak{b} = \prod \mathfrak{p}^{\sup\{n_\mathfrak{p},m_\mathfrak{p}\}}.$$

Proposition 15.1.47. *Let A be a Dedekind domain, K its field of fractions and $\mathcal{P}$ the set of non-zero prime ideals of A. For $\mathfrak{p} \in \mathcal{P}$ let $v_\mathfrak{p}$ denote the corresponding essential valuation of A. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ be*

distinct elements of $\mathcal{P}$ and $n_1, \dots, n_r$ integers and $x_1, \dots, x_r$ elements of K. Then there exists $x \in K$ such that $v_{\mathfrak{p}_i}(x - x_i) \geq n_i$ for all i and $v_{\mathfrak{p}}(x) \geq 0$ for all $\mathfrak{p} \in \mathcal{P}$ distinct from the $\mathfrak{p}_i$.

Proof. Replacing if need be the n_i by greater integers, they may be assumed all to be positive. We examine first the case where the x_i are in A. It obviously amounts to finding an $x \in A$ satisfying the congruences

$$x \equiv x_i \mod \mathfrak{p}_i^{n_i}$$

and the existence of x then follows from Chinese remainder theorem.

We pass now to the general case. We may write $x_i = y_i/s$, where y_i, s are in A. Writing $x = y/s$, it amounts to finding a $y \in A$ such that, on the one hand, $v_{\mathfrak{p}_i}(y - y_i) \geq n_i + v_{\mathfrak{p}_i}(s)$ and, on the other, $v_{\mathfrak{p}}(y) \geq v_{\mathfrak{p}}(s)$ for all $p \in \mathcal{P}$ distinct from the $\mathfrak{p}_i$. As $v_{\mathfrak{p}}(s) = 0$ except for a finite number of indices $\mathfrak{p}$, it is thus reduced to the above case, whence the proposition. □

Proposition 15.1.48. *Let A be a Dedekind domain and $\mathfrak{a}$ a fractional ideal of A. Then $\mathfrak{a}$ is generated by at most two elements.*

Proof. By multiplying by an element of A, we can reduce to the case that $\mathfrak{a}$ is an ideal of A. Write $\mathfrak{a} = \prod \mathfrak{p}_i^{n_i}$ as a finite product and choose $a \in \mathfrak{a}$ with $aA = \prod \mathfrak{q}_j^{m_j} \prod \mathfrak{p}_i^{f_i}$ and the $\mathfrak{q}_j$ different from $\mathfrak{p}_i$. Then since $aA \subseteq \mathfrak{a}$ we have $f_i \geq n_i$ for each i. Choose $b \in A$ such that $v_{\mathfrak{p}_i}(b) = n_i$ and $v_{\mathfrak{q}_j}(b) = 0$, then we see

$$aA + bA = \prod \mathfrak{p}_i^{\inf\{f_i, f_i+1\}} \mathfrak{q}_j^{\inf\{0, m_j\}} = \prod \mathfrak{p}_i^{n_i} = \mathfrak{a}.$$

This proves the claim. □

15.1.10 The Krull-Akizuki theorem

Lemma 15.1.49. *Let A be a one-dimensional Noetherian domain and M a finitely generated torsion A-module. Then the length $\ell_A(M)$ of M is finite.*

Proof. As M is a torsion module, every prime ideal associated with M is nonzero and therefore maximal. The lemma then follows from Proposition 12.2.14. □

Lemma 15.1.50. *Let A be a ring, M an A-module and $(M_i)_{i \in I}$ a directed family of submoduler of M with union M. Then $\ell_A(M) = \sup_i \ell_A(M_i)$.*

Proof. We have $\ell_A(M_i) \leq \ell_A(M)$ for all i. The lemma is obvious if no integer exceeds the $\ell_A(M_i)$, both sides then being infinite. Otherwise, let i_0 be an index for which $\ell_A(M_{i_0})$ takes its greatest value. Then $M = M_{i_0}$ since the family (M_i) is directed, whence our assertion in this case. □

Lemma 15.1.51. *Let A be a one-dimensional Noetherian domain and M a torsion-free A-module of rank $r < \infty$. Then for every nonzero $a \in A$, we have*

$$\ell_A(M/aM) \leq r \cdot \ell_A(A/aA). \tag{1.10.1}$$

Proof. Lemma 15.1.49 shows that $\ell_A(A/Aa)$ is finite. We show (1.10.1) first in the case where M is finitely generated. As M is torsion-free and of rank r, there exists a submodule L of M which

is isomorphic to A^r and such that $Q = M/L$ is a finitely generated torsion A-module and hence of finite length (Lemma 15.1.49). For every integer $n \geq 1$, we have an exact sequence

$$0 \longrightarrow L/(a^n M \cap L) \longrightarrow M/a^n M \longrightarrow Q/a^n Q \longrightarrow 0$$

as $a^n L \subseteq a^n M \cap L$, this implies

$$\ell_A(M/a^n M) \leq \ell_A(L/a^n L) + \ell_A(Q/a^n Q) \leq \ell_A(L/a^n L) + \ell_A(Q). \tag{1.10.2}$$

Now, since M is torsion-free, multiplication by a defines an isomorphism of M/aM onto aM/a^2M and similarly for L; whence, by induction on n, the formulae:

$$\ell_A(M/a^n M) = n \cdot \ell_A(M/aM), \quad \ell_A(L/a^n L) = n \cdot \ell_A(L/aL) \tag{1.10.3}$$

Taking account of (1.10.2), we deduce that

$$\ell_A(M/aM) \leq \ell_A(L/aL) + n^{-1}\ell_A(Q) \tag{1.10.4}$$

for all $n > 0$. As L is isomorphic to A^r, we see $\ell_A(L/aL) = r\ell_A(A/aA)$, so we get (1.10.1) by letting n tend to infinity in (1.10.4).

We now pass to the general case. Let (M_i) be the family of finitely generated submodules of M. Then the module $T = M/aM$ is the union of the submodules $T_i = M_i/(M_i \cap aM)$. Now, T_i is isomorphic to a quotient of M_i/aM_i and hence

$$\ell_A(T_i) \leq r \cdot \ell_A(A/aA)$$

by what we have just proved. Whence $\ell_A(T) \leq r \cdot \ell_A(A/aA)$ by Lemma 15.1.50. □

Proposition 15.1.52 (Krull-Akizuki). *Let A be a one-dimensional Noetherian domain, K its field of fractions, L a finite extension of K and B a subring of L containing A. Then B is a one-dimensional Noetherian domain. Moreover, for every nonzero ideal $\mathfrak{b}$ of B, $B/\mathfrak{b}$ is an A-module of finite length.*

Proof. Let $\mathfrak{b}$ be a non-zero ideal of B. We shall show that $B/\mathfrak{b}$ is an A-module of finite length (hence, a fortiori, a B-module of finite length) and that $\mathfrak{b}$ is a finitely generated B-module. A non-zero element y of $\mathfrak{b}$ satisfies an equation of the form:

$$a_n y^n + a_{n-1} y^n + \cdots + a_1 y + a_0 = 0, \quad a_i \in A, a_0 \neq 0.$$

This equation shows that $a_0 \in By \subseteq \mathfrak{b}$. Applying Lemma 15.1.51 to $M = B$, it is seen that B/a_0B is an A-module of finite length, and so is $B/\mathfrak{b}$ which is a quotient module of it. Further the B-module $\mathfrak{b}$ contains, as a submodule, a_0B which is finitely generated. As $\mathfrak{b}/a_0B$ is of finite length (as a submodule of B/a_0B) and hence finitely generated, $\mathfrak{b}$ is certainly a finitely generated B-module.

The above shows first that B is Noetherian. On the other hand, if $\mathfrak{P}$ is a nonzero prime ideal of B, the ring $B/\mathfrak{P}$ is an integral domain and of finite length and hence is a field, so that $\mathfrak{P}$ is maximal. □

Corollary 15.1.53. *Let A be a one-dimensional Noetherian domain, K its field of fractions, L a finite extension of K and B a subring of L containing A. Then for every prime ideal $\mathfrak{p}$ of A, the set of prime ideals of B lying over $\mathfrak{p}$ is finite.*

Proof. Suppose first that $\mathfrak{p} = (0)$. Then the only prime ideal $\mathfrak{P}$ of B such that $\mathfrak{P} \cap A = (0)$ is (0): otherwise, writing $S = A - \{0\}$, then $S^{-1}\mathfrak{P}$ would be a non-zero prime ideal of $S^{-1}B$ and $S^{-1}B$ is just the field of fractions of B, for it is a subring of L containing K, whence an absurd conclusion. If $\mathfrak{p}$ is nonzero, it follows from Proposition 15.1.52 that $B/\mathfrak{p}B$ is a finite-dimensional vector space over the field $A/\mathfrak{p}$, hence an Artinian ring and therefore has only a finite number of prime ideals, which proves that there is only a finite number of prime ideals of B containing $\mathfrak{p}$. □

Corollary 15.1.54. *Let A be a one-dimensional Noetherian domain, K its field of fractions, L a finite extension of K and B a subring of L containing A. Then the integral closure of A in L is a Dedekind domain. In particular, the integral closure of a Dedekind domain in a finite extension of its field of fractions is a Dedekind domain.*

Proof. This integral closure is a one-dimensional integrally closed Noetherian domain, hence Dedekind. □

Proposition 15.1.55. *Let A be a Dedekind domain, K its field of fractions, L a finite extension of K and B the integral closure of A in L. Let $\mathfrak{p}$ be a non-zero prime ideal of A, $v_{\mathfrak{p}}$ the corresponding essential valuation of K and*

$$B\mathfrak{p} = \prod_i \mathfrak{P}_i^{e_i}$$

the decomposition of the ideal $B\mathfrak{p}$ as a product of prime ideals. Then:

(a) the prime ideals of B lying over $\mathfrak{p}$ are the $\mathfrak{P}_i$ such that $e_i > 0$.

(b) the valuations v_i on L corresponding to these ideals $\mathfrak{P}_i$ are, up to equivalence, the valuations on L extending $v_{\mathfrak{p}}$.

(c) $[B/\mathfrak{P}_i : A/\mathfrak{p}] = f(v_i/v)$ and $e_i = e(v_i/v)$.

Proof. To say that a prime ideal $\mathfrak{P}$ of B lies over $\mathfrak{p}$ amounts to saying that $\mathfrak{P} \supseteq \mathfrak{p}$, hence that $\mathfrak{P} \supseteq B\mathfrak{p}$ and that $\mathfrak{P}$ contains one of the $\mathfrak{P}_i$, such that $e_i > 0$. Now part (b) follows from Corollary 15.1.27. Finally, the residue field of v is identified with $A/\mathfrak{p}$ and that of v_i with $B/\mathfrak{P}_i$, hence the first claim of (c). Let t (resp. t_i) be a uniformizer for v (resp. v_i). Then

$$tB_{\mathfrak{P}_i} = tA_{\mathfrak{p}}B_{\mathfrak{P}_i} = \mathfrak{p}B_{\mathfrak{P}_i} = \Big(\prod_i \mathfrak{P}_j^{e_j}\Big)B_{\mathfrak{P}_i} = \prod_j (\mathfrak{p}_j B_{\mathfrak{P}_i})^{e_j} = (\mathfrak{p}_i B_{\mathfrak{P}_i})^{e_i} = t_i^{e_i} B_{\mathfrak{P}_i}$$

since $\mathfrak{p}_j B_{\mathfrak{P}_i} = B_{\mathfrak{P}_i}$ for $j \neq i$, whence the second claim of (c), since $e(v_i/v) = v_i(t)$. □

15.1.11 Unique factorization domains

A Krull domain all of whose divisorial ideals are principal is called a **factorial** or **unique factorization domain**. In other words, A is factorial if and only if $\mathfrak{C}(A)$ is reduced to 0.

Example 15.1.56.

(a) Every PID is factorial (and, recall, is a Dedekind domain). Conversely, every factorial Dedekind domain is a PID by Theorem 15.1.45.

(b) In particular, if K is a field, the rings $K[X]$ and $K[\![X]\!]$ are factorial domains.

(c) The local ring of a simple point of an algebraic variety is a factorial domain. The ring of germs of functions analytic at the origin of $\mathbb{C}^n$ is a factorial domain.

Theorem 15.1.57. *Let A be an integral domain. Thefollowing conditions are equivalent*

(i) A is factorial;

(ii) the ordered group of non-zero fractional principal ideal of A is a direct sum of groups isomorphic to $\mathbb{Z}$ (ordered by the product order).

(iii) Every non-empty family of integral principal ideals of A has a maximal element and the intersection of two principal ideals of A is a principal ideal;

(iv) Every non-empty family of integral principal ideals of A has a maximal element and every irreducible element of A is prime;

(v) A is a Krull domain and every prime ideal of height 1 is principal.

Proof. We shall denote by K the field of fractions of A and by $\mathscr{P}$ (or $\mathscr{P}(A)$) the ordered group of non-zero fractional principal ideals of A. We show that (i) implies (ii). If A is factorial, $\mathscr{P}$ is isomorphic to the group of divisors of A and hence to a direct sum of groups $\mathbb{Z}$.

Note now that the relation "the intersection of two integral principal ideals of A is a principal ideal" means that every ordered pair ofelements of A admits a lcm, that is, $\mathscr{P}$ is a lattice-ordered group. The fact that (ii) implies (iii) (and even is equivalent to it) therefore follows from **??**. The fact that (iii) implies (iv) follows from **??**. The fact that (iv) implies (ii) follows from **??** applied to the group $\mathscr{P}$.

We show that (ii) implies (v). If (ii) holds, there is an isomorphism of $\mathscr{P}$ onto $\mathbb{Z}^{\oplus I}$. Let $(v_i(x))_{i\in I}$ denote the element of $\mathbb{Z}^{\oplus I}$ corresponding to the ideal Ax. It is seen immediately that each v_i is a discrete valuation on K, that A is the intersection of the rings of the vI and that, for $x \neq 0$ in A, $v_i(x) \neq 0$ for a finite number of indices i. Hence A is a Krull domain. On the other hand, let $\mathfrak{p}$ be a prime ideal of A of height 1; it contains a non-zero element a which is necessarily not invertible and hence also (by definition of a prime ideal) one of the irreducible elements p of A. As p is prime and non zero, $\mathfrak{p} = p$, which proves that $\mathfrak{p}$ is principal.

Finally we show that (v) implies (i). Let $\mathfrak{a}$ be a divisorial ideal of A. There exist prime ideals $\mathfrak{p}_i$ of A of height 1 such that $\operatorname{div}(\mathfrak{a}) = \sum_i n_i \operatorname{div}(\mathfrak{p}_i)$ where $n_i \in \mathbb{Z}$. If (v) holds, $\mathfrak{p}_i$ is of the form Ap_i whence $\operatorname{div}(\mathfrak{a}) = \operatorname{div}(Ap_i^{n_i})$ and hence $\mathfrak{a} = \prod_i Ap_i^{n_i}$ since $\mathfrak{a}$ is divisorial. □

Proposition 15.1.58. *Let A be a Krull domain. If every divisorial ideal of A is invertible, then, for every maximal ideal $\mathfrak{m}$ of A, $A_\mathfrak{m}$ is factorial. The converse is true if it is also assumed that every divisorial ideal of A is finitely generated (in particular if A is Noetherian).*

Proof. Suppose that every divisorial ideal of A is invertible. As $A_\mathfrak{m}$ is a Krull domain, every divisorial ideal $\mathfrak{a}$ of $A_\mathfrak{m}$ is the intersection of two principal fractional ideals (Corollary 15.1.24), hence $\mathfrak{a} = \mathfrak{b}A_\mathfrak{m}$, where $\mathfrak{b}$ is a divisorial ideal of A (Corollary 10.2.33). As $\mathfrak{b}$ is invertible by

hypothesis, we deduce from Theorem 10.5.23 that $\mathfrak{a}$ is principal and hence $A_{\mathfrak{m}}$ is a factorial domain.

Conversely, if all the $A_{\mathfrak{m}}$ are factorial and $\mathfrak{a}$ is a finitely generated divisorial ideal of A, then $\mathfrak{a}A_{\mathfrak{m}}$ is a divisorial ideal of $A_{\mathfrak{m}}$, as follows from Corollary 15.1.24 and Corollary 10.2.31. By hypothesis $\mathfrak{a}A_{\mathfrak{m}}$ is principal and hence it follows from Theorem 10.5.23 that $\mathfrak{a}$ is invertible. □

Let A be an integral domain, K its field of fractions and $U(A)$ the multiplicative group of invertible elements of A. Recall that there is a canonical isomorphism of $K^{\times}/U$ onto the group $\mathscr{P}$ of non-zero fractional principal ideals of A. Condition (ii) of Theorem 15.1.57 may then be translated as follows:

Proposition 15.1.59. *Let A be an integral domain. For A to befactorial, it is necessary and sufficient that there exist a subset P of A such that every $a \in A$ may be written uniquely in the form $a = u\prod_{p\in P} p^{n_p}$, where $u \in U(A)$ and the n_p are positive integers which are zero exceptfor a finite number of them.*

If P satisfies this condition, clearly all its elements are irreducible and every irreducible element of A is associated with a unique element of P. Recall that P is then called a representative system of irreducible elements of A.

Suppose always that A is factorial. It has been seen that the group $\mathscr{P}$ is a lattice. In particular, every element of $K^{\times}$ may be written in an essentially unique way in the form of an irreducible fraction. Any two elements a, b of $K^{\times}$ have a gcd and a lcm. If $a = u\prod p^{n_p}$ and $b = v\prod p^{m_p}$ are decompositions of a and b as products of irreducible elements, then, then

$$\gcd(a,b) = w\prod p^{\inf\{n_p,m_p\}}, \quad \operatorname{lcm}(a,b) = w\prod p^{\sup\{n_p,m_p\}}.$$

For all $p \in P$, the mapping $a \mapsto n_p$ is a discrete valuation v_p on K whose ring is obviously A_{Ap}. It follows from Theorem 15.1.57 that the v_p are just the essential valuations of A and that the ideals Ap are just the prime ideals of A of height 1.

Proposition 15.1.60. *Let A be a Krull domain and S a multiplicative subset of A not containing* 0.

(a) If A is factorial, $S^{-1}A$ is factorial;

(b) If S is generated by a family of elements p_i such that the principal ideals Ap_i are prime and $S^{-1}A$ isfactorial, then A is factorial.

Proof. This follows from the definition of factorial domains and Proposition 15.1.42. □

Let A be a factorial domain, K its field of fractions and f a non-zero element of $K[X]$. The **content** of f is defined to be the gcd of the coefficients of f (up to a unit of A) and denote by $\operatorname{cont}(f)$. Let v be a valuation on K which is essential for A and $\bar{v}$ its canonical extension to $K[X]$, then

$$\bar{v}(f) = v(\operatorname{cont}(f)).$$

Moreover, it is easy to see $\operatorname{cont}(f)$ is uniquely determined by this property.

Lemma 15.1.61 (Guass's Lemma). *Let f, g be non-zero elements of $K[X]$, then*

$$\operatorname{cont}(fg) = \operatorname{cont}(f)\operatorname{cont}(g).$$

Proof. For every valuation v on K which is essential for A, let $\bar{v}$ denote its canonical extension to $K[X]$. Then

$$v(\mathrm{cont}(fg)) = \bar{v}(fg) = \bar{v}(f) + \bar{v}(g) = v(\mathrm{cont}(f)) + v(\mathrm{cont}(g)) = v(\mathrm{cont}(fg))$$

which proves the claim. □

Note that for every $f \in K[X]$, $f/\mathrm{cont}(f)$ is a polynomial with content 1 (such a polynomial is called **primitive**) and we can always write

$$f = \mathrm{cont}(f)\tilde{f}$$

where $\tilde{f}$ is a primitive polynomial.

Theorem 15.1.62. *Let A be a factorial domain, K its field of fractions, (p_i) a representative system of irreducible elements of A and (P_α) a representative system of primitive irreducible polynomials of $K[X]$. Then:*

(a) $A[X]$ is a factorial domain;

(b) the set p_i and P_i is a representative system of irreducible elements of $A[X]$.

Proof. Let f be a non-zero element of $A[X]$. In the ring $K[X]$, f can be decomposed uniquely in the form:

$$f = a \prod_\alpha P_\alpha^{n_\alpha}$$

where $a \in K^\times$ and $n_\alpha \geq 0$. Lemma 15.1.61 proves that a is the content of f. Hence $a \in A$. As A is factorial, a can be decomposed uniquely in the form:

$$a = u \prod_i p_i^{m_i}$$

whence the existence and uniqueness of the decomposition

$$f = u \prod_i p_i^{m_i} \prod_\alpha P_\alpha^{n_\alpha}.$$

Note that this theorem proves that every element of A admits the same decomposition into irreducible elements in A and $A[X]$. The gcd of a family of elements of A is therefore the same in A and in $A[X]$. □

Corollary 15.1.63. *If A is a factorial domain, the domain $A[X_1, \ldots, X_n]$ is factorial. Also the domain $A[X_n]_{n\in\mathbb{N}}$ is factorial.*

Proposition 15.1.64. *Let A be a Zariski ring and $\widehat{A}$ its completion. If $\widehat{A}$ is a factorial domain, A is a factorial domain.*

Proof. This follows from definition of factorial domain and Proposition 15.1.41. □

Proposition 15.1.65. *Let C be a ring which is either a field or a DVR. Then the domain of formal power series $C[\![X_1, \ldots, X_n]\!]$ is factorial.*

Proof. Let $\mathfrak{m}$ be the maximal ideal of C and π a generator of $\mathfrak{m}$ (if C is a field, then $\pi = 0$). Let C be given the $\mathfrak{m}$-adic topology, which is Hausdorff. As C is a Noetherian local ring, $B = C[\![X_1, \dots, X_n]\!]$ is a Noetherian local ring and its completion is $\widehat{C}[\![X_1, \dots, X_n]\!]$. By the Corollary to **??**, it suffices to prove that $\widehat{C}[\![X_1, \dots, X_n]\!]$ is factorial. Now, if C is a field, then $\widehat{C} = C$; if C is a DVR, the same is true of $\widehat{C}$ (Theorem 14.5.1). We shall therefore assume in the remainder of the proof that C is complete.

Arguing by induction starting with the trivial case n = 0, we shall assume that it has been proved that $A = C[\![X_1, \dots, X_{n-1}]\!]$ is factorial. We shall identify B with $A[\![X_n]\!]$ and denote by $\mathfrak{M}$ the maximal ideal of A (generated by $\pi, X_1, \dots, X_{n-1}$). We shall prove that every non-zero element g of B is, in an essentially unique way, a product of irreducible elements.

Let K be the field $C/C\pi$. As $B/B\pi$ is identified with $K[\![X_1, \dots, X_n]\!]$, the ideal $B\pi$ is prime and π is irreducible. If $\pi \neq 0$, $B_{B\pi}$ is therefore the ring of a normed discrete valuation w; every nonzero element g of B may therefore be written as $g = \pi^{w(g)} f$, where $f \in B$ and f is not a multiple of π. It will therefore suffice to show that f is an essentially unique product of extremal elements. Now the canonical image of f in $K[\![X_1, \dots, X_n]\!]$ is not zero; **??** therefore shows that there exists an automorphism of B which maps f to an element $\tilde{f}$ such that the coefficients of $\tilde{f}(0, \dots, 0, X_n)$ are not all in $C\pi$; this means that the coefficients of the series $\tilde{f}$, considered as a formal power series in X_n, are not all in $\mathfrak{M}$. It will suffice to prove our assertion for $\tilde{f}$.

In what follows, all the elements of B will be considered as formal power series in X_n with coefficients in A. By **??** (applicable since C and therefore A are separable and complete and the reduced series of $\tilde{f}$ is nonzero), $\tilde{f}$ is associated, in B, with a unique distinguished polynomial F. By **??**, every series which divides $\tilde{f}$ (or, what amounts to the same, which divides F) is associated with a distinguished polynomial which divides F and every decomposition of $\tilde{f}$ is, to within invertible factors, of the form $\tilde{f} = uF_1 \cdots F_r$, where u is invertible and the F_i are irreducible distinguished polynomials (in B) such that $F = F_1 \dots F_r$. By **??**, the F_i are also irreducible in $A[X_n]$. Now, as A is factorial by the induction hypothesis, so is $A[X_n]$; hence, since they are monic, the F_i are uniquely determined by F (up to a permutation). This shows the uniqueness of the decomposition $\tilde{f} = uF_1 \cdots F_r$; its existence follows from the fact that B is Noetherian, which completes the proof. □

15.2 Modules over integrally closed Noetherian domains

Throughout this paragraph, A will be a integral domain with field of fractions K. Then $P(A)$, $\mathfrak{D}(A)$ and $\mathfrak{C}(A)$ will respectively denote the set of prime ideals of A of height 1, the divisor group of A and the divisor class group of A, these latter being written additively.

The general method of studying finitely generated modules over an integrally closed Noetherian domain A consists of "localizing" the modules with respect to all the prime ideals $\mathfrak{p} \in P(A)$ of height 1 in A. As $A_\mathfrak{p}$ is then a DVR, the structure of finitely generated $A_\mathfrak{p}$-modules is well known and therefore gives information about the structure of finitely generated A-modules. In the particular case where A is a Dedekind domain, we can arrive at as complete a theory as when A is a principal ideal domain.

15.2.1 Lattices

Let V be a finite-dimensional vector space over the field K. A **lattice of V with respect to A** (or simply a lattice of V) is defined to be any sub-A-module M of V such that there exist two free sub-A-modules L_1, L_2 of V such that $L_1 \subseteq M \subseteq L_2$ and $\operatorname{rank}_A(L_1) = \dim_K V$.

Example 15.2.1.

(a) If we take $V = K$, the lattices of K are just the nonzero fractional ideals of K.

(b) If $\dim_K V = n$, every free sub-A-module L of V has a basis containing at most n elements, every subset of V which is free over A being free over K. For L to be a lattice of V, it is necessary and sufficient that L have a basis of n elements (in other words, that $\operatorname{rank}_A(L) = n$).

(c) If A is a PID, every lattice M of V is a finitely generated A-module (since A is Noetherian) which is torsion-free and hence a free A-module.

Proposition 15.2.2. *For a sub-A-module M of V to be a lattice of V, it is necessary and sufficient that $KM = V$ and that M be contained in a finitely generated sub-A-module of V.*

Proof. The conditions are obviously necessary, for a free sub-A-module of V with the same rank as V generates V. Conversely, if $KM = V$, M contains a basis $a_1, \dots, a_n$ of V over K and hence it contains the free sub-A-modulc L_1 generated by the a_i. On the other hand, if $M \subseteq M_1$, where M_1 is a sub-A-module of V generated by a finite number of elements b_i and $e_1, \dots, e_n$ is a basis of V over K, there exists a nonzero element s of A such that each of the b_i is a linear combination of the $s^{-1}e_i$ with coefficients in A. If L_2 is the free sub-A-modules of V generated by the $s^{-1}e_i$, then $M \subseteq L_2$. □

Corollary 15.2.3. *Suppose that A is Noetherian. For a sub-A-module M of V to be a lattice of V, it is necessary and safiicient that $KM = V$ and M be finitely generated.*

Proposition 15.2.4. *Let M be a lattice of V and M_1 a sub-A-modale of V. If there exist two elements $x, y \in K^\times$ such that $xM \subseteq M_1 \subseteq yM$, then M_1 is a lattice of V. Conversely, if M_1 is a lattice of V, there exist two non-zero elements a, b of A such that $aM \subseteq M_1 \subseteq b^{-1}M$.*

Proof. If L_1, L_2 are two free lattices of V such that $L_1 \subseteq M \subseteq L_2$, the relations $xM \subseteq M_1 \subseteq yM$ imply $xL_1 \subseteq M_1 \subseteq yL_2$ and xL_1 and yL_2 are free lattices. Conversely, if M_1 is a lattice and $e_1, \dots, e_n$ is a basis of L_2 over A, the relation $KM_1 = V$ implies the existence of $x = a/s \in K^\times$ (where a and s are non-zero elements of A) such that $xe_i \in M_1$ for all i, whence $xM \subseteq xL_2 \subseteq M_1$ and a fortiori $aM \subseteq M_1$. Exchanging the roles of M and M_1 it can be similarly shown that there exists $b \neq 0$ in A such that $bM_1 \subseteq M$. □

Proposition 15.2.5 (Properties of Lattices).

(a) If M_1 and M_2 are lattices of V, so are $M_1 \cap M_2$ and $M_1 + M_2$.

(b) If W is a vector subspace of V and M is a lattice of V, then $M \cap W$ is a lattice of W.

(c) Let V, $V_1, \dots, V_k$ be vector spaces of finite dimension over K and let $f : V_1 \times \cdots \times V_k \to V$ be a multilinear mapping whose image generates V. If M_i is a lattice of V_i for each i, then the sub-A-module of V generated by $f(M_1 \times \cdots \times M_k)$ is a lattice of V.

(d) *Let V and W be two vector spaces of finite dimension over K, M a lattice of V and N a lattice of W. Then the sub-A-module $(N : M)$ of $\mathrm{Hom}_K(V, W)$, consisting of the K-linear mappings f such that $f(M) \subseteq N$, is a lattice of $\mathrm{Hom}_K(V, W)$.*

Proof. For (a), by virtue of Proposition 15.2.4, there exist non-zero a and b in A such that $aM_1 \subseteq M_2 \subseteq b^{-1}M_1$. We conclude that $M_1 \cap M_2$ and $M_1 + M_2$ lie betwcen aM_1 and $b^{-1}M_1$ and are therefore lattices by virtue of Proposition 15.2.4.

As for (b), let S be a complement of W in V, L_W a free lattice of W and L_S a free lattice of S, so that $L = L_S + L_W$ is a free lattice of V. Then there exist x, y in $K^\times$ such that $xL \subseteq M \subseteq yL$. We deduce that $xL_W \subseteq M \cap W \subseteq yL_W$, which shows that $M \cap W$ is a lattice of W.

Now we prove (c). As $KM_i = V_i$ clearly by linearity $f(M_1 \times \cdots \times M_k)$ generates the vector K-space V. On the other hand, for all i, there exists a finitely generated sub-A-module N_i of V_i such that $M_i \subseteq N_i$. The sub-A-module N of V generated by $f(N_1 \times \cdots \times N_k)$ is finitely generated and contains M and hence M is a lattice of V (Proposition 15.2.2).

Finally, consider (d). Let P (resp. Q) be a free lattice of V (resp. W) containing M (resp. contained in N). Obviously $(N : M) \subseteq (Q : P)$. Now it is immediate that $(Q : P)$ is isomorphic to $\mathrm{Hom}_A(P, Q)$, hence is a free A-module of rank $(\mathrm{rank}_A P)(\mathrm{rank} Q)$ and therefore a lattice of $\mathrm{Hom}_K(V, W)$. Similarly, if P' (resp. Q') is a free lattice of V (resp. W) contained in M, (resp. containing N), then $(Q' : P') \subseteq (N : M)$ and $(Q' : P')$ is a lattice of $\mathrm{Hom}_K(V, W)$, whence the conclusion. □

In the notation of Proposition 15.2.5(d), the canonical mapping $(N : M) \to \mathrm{Hom}_A(M, N)$ which maps every K-linear mapping $f \in (N : M)$ to the A-linear mapping from M to N which has the same graph as $f|_M$, is bijective: for every A-linear mapping $g : M \to N$ can be imbedded in a K-linear mapping

$$g \otimes 1 : M \otimes_A K \to N \otimes_A K$$

and by Proposition 15.2.2 $M \otimes_A K$ and $N \otimes_A K$ are respectively identified with V and W.

In particular, if we take $W = K$, $N = A$, $\mathrm{Hom}_K(V, W)$ is just the dual vector K-space V^* of V and $(A : M)$ is identified with the dual A-module M^* of M. We shall henceforth make this identification and we shall say that M^* is the dual lattice of M: it is therefore the set of $x^* \in V^*$ such that $\langle x^*, x\rangle \in A$ for all $x \in M$.

Corollary 15.2.6. *Let U, V, W be three vector spaces of finite dimension over K and $f : U \times V \to W$ a left non-degenerate K-bilinear mapping. If M is a lattice of V and N a lattice of W, then the set $(N :_f M)$ of $x \in U$ such that $f(x, y) \in N$ for all $y \in M$ is a lattice of U.*

Proof. Let $\phi_f : U \to \mathrm{Hom}_K(V, W)$ be the K-linear mapping left associated with f such that $\phi_f(x)$ is the linear mappingy $y \mapsto f(x, y)$.Recall that to say that f is left non-degenerate means that ϕ_f is injective. By Proposition 15.2.5(d) $(N : M)$ is a lattice of $\mathrm{Hom}_K(V, W)$, as $(N :_f M) = \phi_f^{-1}(N : M)$ and ϕ_f is injective, the corollary follows from Proposition 15.2.5(b). □

Example 15.2.7. Let S be a (not necessarily associative) K-algebra of finite dimension with a unit element. Then the bilinear mapping $(x, y) \mapsto xy$ of $S \times S$ to S is (left and right) non-degenerate. If M and N are lattices of S with respect to A, so are $M \cdot N$ and the set of $x \in S$ such that $xM \subseteq N$. Note that there exists a sub-A-algebra of S containing the unit element of

S which is a lattice of S: for consider a basis $e_1, \dots, e_n$ of S such that e_1 is the unit element of S and let $e_i e_j = \sum_k c_{ij}^k e_k$ be the multiplication table of S, so that $c_{1j}^k = \delta_j^k$ and $c_{i1}^k = \delta_i^k$. Let $s \in A$ be a non-zero element such that $\tilde{c}_{ij}^k := s \cdot c_{ij}^k \in A$ for all triplets of indices (i, j, k). If we write $w_i = s^{-1} e_i$ for $i \geq 2$, then

$$w_i w_j = s\tilde{c}_{ij}^1 e_1 + \sum_{k \geq 2} \tilde{c}_{ij}^k w_k$$

for $i, j \geq 2$. The lattice of S with basis e_1 and the $w_2, \dots, w_n$ is a sub-A-algebra of S with unit element e_1.

Example 15.2.8. Let V be a finite-dimensional vector space over K and f a non-degenerate bilinear form on V. If M is a lattice of V, it follows from the Corollary 15.2.6 that the set M_f^* of $x \in V$ such that $f(x, y) \in A$ for all $y \in M$ is also a lattice of V. If $\phi_f : V \to V^*$ is the linear mapping left associated with f (which is bijective), $\phi_f(M_f^*)$ is just the dual lattice M^* of M.

Proposition 15.2.9. *Let B be an integral domain, A a subring of B and K and L the respective field of fractions of A and B. Let V be a finite-dimensional vector space over K.*

(a) For every lattice M of V with respect to A, the image BM of $M_{(B)} = M \otimes_A B$ in $V_{(L)} = V \otimes_K L$ is a lattice of $V_{(L)}$ with respect to B.

(b) Suppose further that B is a flat A-module. Then the canonical mapping $M_{(B)} \to BM$ is bijective. If further B is faithfully flat, the mapping which maps every lattice M of V with respect to A to the lattice BM of $V_{(L)}$ with respect to B is injective.

Proof. As $KM = V$, clearly $L(BM) = V_{(L)}$. On the other hand M is contained in a finitely generated sub-A-module M_1 of V and hence BM is contained in BM_1 which is a finitely generated B-module; whence assertion (a).

We see $\mathrm{Ind}_K^L V = V \otimes_K L = V \otimes_A L$ and, as L is a flat B-module, it is also a flat A-module. If B is a flat A-module, then the canonical mapping $M \otimes_A B \to V \otimes_A B$ is injective. On the other hand, since V is a free K-module and K a flat A-module, V is a flat A-module and hence the canonical mapping $V \otimes_A B \to V \otimes_A L$ is injective, which establishes the first assertion. To see also that the relation $BM_1 = BM_2$ implies $M_1 = M_2$ for two lattices M_1, M_2 of V with respect to A when B is a faithfully flat A-module, note first that $BM_1 \cap BM_2 = B(M_1 \cap M_2)$. We may therefore confine our attention to the case where $M_1 \subseteq M_2$ and our assertion then follows from Proposition 7.3.1 applied to the canonical injection $M_1 \to M_2$. □

Corollary 15.2.10. *Suppose that A is a DVR. Let $\widehat{A}$ be its completion and let $\widehat{K}$ be the field of fractions of $\widehat{A}$. The mapping η which maps every lattice M of V to the lattice $\widehat{A}M$ of $\widehat{V} = V \otimes_K \widehat{K}$ with respect to A is bijective and its inverse maps every lattice $\widehat{M}$ of $\widehat{V}$ with respect to $\widehat{A}$ to its intersection $\widehat{M} \cap V$ (V being canonically identified with a vector sub-K-space of $\widehat{V}$).*

Proof. If L is a free lattice of V, the lattices aL (for $a \in A$ nonzero) form a fundamental system of neighbourhoods of 0 for a topology $\mathcal{T}$ on V (compatible with its A-module structure), which (when a basis of L over A is taken) is identified with the product topology on K^n. By virtue of Proposition 15.2.4, a fundamental system of neighbourhoods of 0 for $\mathcal{T}$ also consists of all the lattices of V with respect to A. Clearly $\widehat{V}$ is the completion of V with respect to $\mathcal{T}$. Moreover, if $\mathfrak{m}$ is the maximal ideal of A, the topology $\mathcal{T}$ induces on every lattice M of V with respect to A the $\mathfrak{m}$-adic topology since M is a finitely generated A-module (Theorem 11.4.12) and $\widehat{A}M$ is

the completion of M with respect to this topology (Proposition 11.4.3). Moreover, as M is open (and therefore closed) in V, $\widehat{A}M \cap V = M$, which proves again the fact that η is injective (which follows directly from Proposition 15.2.9(b), since $\widehat{A}$ is a faithfully flat A-module).

Finally, if $\widehat{M}$ is a lattice of $\widehat{V}$ with respect to A and $M = \widehat{M} \cap V$, then since $\widehat{A}L$ is a free lattice of $\widehat{V}$ with respect to $\widehat{A}$ and every element of $\widehat{A}$ is the product of an element of A and an invertible element of $\widehat{A}$, there exists $a, b \in \widehat{A}$ such that $a\widehat{A}L \subseteq \widehat{M} \subseteq b^{-1}\widehat{A}L$, whence $aL \subseteq \widehat{M} \cap V \subseteq b^{-1}L$, so $\widehat{M} \cap V$ is a lattice of V with respect to A. Moreovcr $\widehat{M}$ is open in V and, as V is dense in $\widehat{V}$, $\widehat{M}$ is the completion of $\widehat{M} \cap V = M$. This proves that η is surjective, whence the corollary □

Let S be a multiplicative subset of A not containing 0. Then we can apply Proposition 15.2.9 to $B = S^{-1}A$ with $L = K$, $BM = S^{-1}M$. Hence $S^{-1}M$ is a lattice of V with respect to $S^{-1}A$. Moreover:

Proposition 15.2.11. *Let V, W be vector spaces of finite dimension over K, M a lattice of V and N a lattice of W. If M is finitely generated, then*

$$S^{-1}(N : M) = (S^{-1}N : S^{-1}M)$$

in $\mathrm{Hom}_K(V, W)$.

Proof. Clearly the left hand side is contained in the right hand side. Conversely, let $f \in (S^{-1}N : S^{-1}M)$ and let $x_1, \dots, x_n$ be a system of generators of M. There exists $s \in S$ such that $f(x_i) \in s^{-}1N$ for all i and hence $sf \in (N : M)$, which proves the proposition. □

15.2.2 Duality and reflexive modules

From now on the domain A is assumed to be Noetherian and integrally closed and that $P(A)$ denotes the set of prime ideals of A of height 1. Every lattice with respect to A is a finitely generated A-module by Corollary 15.2.3.

Let V be a vector space of finite dimension over K, V^* its dual and V^{**} its bidual. We shall identify V and V^{**} by means of the canonical map J_M. Let M be a lattice of V, recall that the dual A-module M^* of M is canonically identified with the dual lattice of M, which is the set of $x^* \in V^*$ such that $\langle x^*, x\rangle \in A$ for all $x \in M$. The bidual A-module M^{**} of M is therefore a lattice of V which contains M. Moreover $M^{***} = M^*$, for the relation $M \subseteq M^{**}$ implies $(M^{**})^* \subseteq M^*$ and on the other hand $M^* \subseteq (M^*)^{**}$ by the above.

If $\mathfrak{p}$ is a prime ideal, Proposition 15.2.11 applied with $N = A$ gives the relation $(M^*)_\mathfrak{p} = (M_\mathfrak{p})^*$, which justifies the notation $M^*_\mathfrak{p}$ for both terms.

Theorem 15.2.12. *If M is a lattice of V, then $M^* = \bigcap_{\mathfrak{p}\in P(A)} M^*_\mathfrak{p}$.*

Proof. Clearly M^* is contained in each of the $M^*_\mathfrak{p}$. Conversely, suppose that $x^* \in \bigcap_{\mathfrak{p}\in P(A)} M^*_\mathfrak{p}$. If $x \in M$, then $\langle x^*, x\rangle \in \bigcap_{\mathfrak{p}\in P(A)} A_\mathfrak{p} = A$, and thus $x^* \in M^*$. □

Corollary 15.2.13. *If M is a lattice of V, then $M^{**} = \bigcap_{\mathfrak{p}\in P(A)} M_\mathfrak{p}$.*

Proof. Theorcm 15.2.12 applied to M^* shows that $M^{**} = \bigcap_{\mathfrak{p}\in P(A)} M^{**}_\mathfrak{p}$. But as $A_\mathfrak{p}$ is a principal ideal domain, $M^*_\mathfrak{p}$ is a finitely generated free $A_\mathfrak{p}$-module and hence $M^{**}_\mathfrak{p}$ is canonically identified with $M_\mathfrak{p}$, whence the corollary. □

For any lattice M with respect to A, the canonical mapping $J_M : M \to M^{**}$ identifies an element $x \in M$ with itself, for x is the unique element y of $V = V^{**}$ such that $\langle x^*, x\rangle = \langle x^*, y\rangle$ for all $x^* \in M^*$, since M^* generates V^*. We shall say that M is **reflexive** if $M^{**} = M$. As we have above $M^* = (M^*)^{**}$, it is seen that the dual of any lattice M is always reflxive.

Theorem 15.2.14. *If M is a lattice of V, the following conditions are equivalent:*

(i) *M is reflexive;*

(ii) $M = \bigcap_{\mathfrak{p}\in P(A)} M_{\mathfrak{p}}$;

(iii) $\mathrm{Ass}(V/M) \subseteq P(A)$.

Proof. The equivalence of (i) and (ii) follows from the Corollary 15.2.13. If (ii) holds, then $\bigcap_{\mathfrak{p}\in P(A)}(V/M_{\mathfrak{p}}) = \{0\}$ in V/M, hence by Corollary 12.1.9 we have

$$\mathrm{Ass}(V/M) \subseteq \bigcup_{p\in P(A)} \mathrm{Ass}(V/M_{\mathfrak{p}}).$$

As $V/M_{\mathfrak{p}}$ is an $A_{\mathfrak{p}}$-module, an element of $A - \mathfrak{p}$ cannot annihilate a nonzero element of $V/M_{\mathfrak{p}}$, since the elements of $A - \mathfrak{p}$ are invertible in $A_{\mathfrak{p}}$. The elements of $\mathrm{Ass}(V/M_{\mathfrak{p}})$ are therefore contained in $\mathfrak{p}$ and are nonempty, since $V/M_{\mathfrak{p}}$ is a torsion $A_{\mathfrak{p}}$-module. As $\mathfrak{p}$ is of height 1, necessarily $\mathrm{Ass}(V/M_{\mathfrak{p}}) = \{p\}$ if $V/M_{\mathfrak{p}} \neq \{0\}$ and $\mathrm{Ass}(V/M_{\mathfrak{p}}) = \varnothing$ if $V/M_{\mathfrak{p}} = \{0\}$; hence $\mathrm{Ass}(V/M) \subseteq P(A)$.

Finally, if condition (iii) holds, then

$$\mathrm{Ass}(M^{**}/M) \subseteq \mathrm{Ass}(V/M) \subseteq P(A)$$

On the other hand, if $\mathfrak{p} \in P(A)$, then it has been seen in the proof of the Corollary 15.2.13 that ${}^{**}_{\mathfrak{p}} = M_{\mathfrak{p}}$, whence $\mathfrak{p} \notin \mathrm{Ass}(M^{**}/M)$ by Proposition 12.1.14. We conclude that $\mathrm{Ass}(M^{**}/M) = \varnothing$, whence $M^{**} = M$. □

Corollary 15.2.15. *Let M, N be two lattices of V with respect to A such that N is reflexive. In order that $M \subseteq N$, it is necessary and sufficient that, for all $\mathfrak{p} \in P(A)$, $M_{\mathfrak{p}} \subseteq N_{\mathfrak{p}}$.*

Proof. The condition is obviously necessary and, if it is fulfilled, then

$$\bigcap_{\mathfrak{p}\in P(A)} M_{\mathfrak{p}} \subseteq \bigcap_{\mathfrak{p}\in P(A)} N_{\mathfrak{p}} = N$$

As $M \subseteq M^{**} = \bigcap_{\mathfrak{p}\in P(A)} M_{\mathfrak{p}}$, certainly $M \subseteq N$. □

Example 15.2.16 (Example of reflexive submodules).

(a) Every free lattice is reflexive.

(b) Take $V = K$. For a fractional ideal $\mathfrak{a}$ of K to be a reflexive lattice, it is necessary and sufficient that it be a divisorial ideal by the observation $\mathfrak{a}^* = (A : \mathfrak{a})$ and Proposition 15.1.3.

(c) Let M be a lattice with respect to A. If S is a multiplicative subset of A not containing 0, Proposition 15.2.11 shows that $S^{-1}(M^*) = (S^{-1}M)^*$. If M is reflexive, $S^{-1}M$ is therefore a reflexive lattice with respect to $S^{-1}A$.

(d) If M is a finitely generated A-module and T its torsion submodule, the dual M^* of M is the same as the dual of M/T, since, for every linear form f on M, the image $f(T)$ is a torsion submodule of A and hence zero. As M/T is isomorphic to a lattice of a vector space over K, it is seen that the dual of every finitely generated A-module is reflexive.

Proposition 15.2.17. *Let V be a vector space of finite dimension over K.*

(a) If M_1 and M_2 are reflexive lattices of V, so is $M_1 \cap M_2$.

(b) If W is a vector subspace of V and M is a reflexive lattice of V, then $M \cap W$ is a reflexive lattice of W.

(c) Let V, W be two vector spaces of finite dimension over K and M (resp. N) a lattice of V (resp. W). If N is reflexive, the lattice $(N : M)$ is reflexive.

Proof. For (a), note that $(M_1 \cap M_2)_\mathfrak{p} = (M_1)_\mathfrak{p} \cap (M_2)_\mathfrak{p}$ for all $\mathfrak{p} \in P(A)$. If $M_1 = \bigcap_{\mathfrak{p}\in P(A)}(M_1)_\mathfrak{p}$ and $M_2 = \bigcap_{\mathfrak{p}\in P(A)}(M_2)_\mathfrak{p}$, then

$$M_1 \cap M_2 = \bigcap_{\mathfrak{p}\in P(A)} (M_1 \cap M_2)_\mathfrak{p}$$

whence the conclusion by virtue of Theorem 15.2.14. Simialrly $(M \cap W)_\mathfrak{p} = M_\mathfrak{p} \cap W$, whence (b). Now for (c), as M is finitely generated, it follows from Proposition 15.2.11 that $(N : M)_\mathfrak{p} = (N_\mathfrak{p} : M_\mathfrak{p})$. Moreover, the relation $N = \bigcap_{\mathfrak{p}\in P(A)} N_\mathfrak{p}$ implies

$$(N : M) = \bigcap_{\mathfrak{p}\in P(A)} (N_\mathfrak{p} : M_\mathfrak{p})$$

For if $f \in \bigcap_{\mathfrak{p}\in P(A)}(N_\mathfrak{p} : M_\mathfrak{p})$ and $x \in M$, then $f(x) \in N_\mathfrak{p}$ for all $\mathfrak{p} \in P(A)$, whence $f \in (N : M)$. This shows $(N : M)$ is reflexive. □

Proposition 15.2.18. *Let $0 \to M \to N \to Q \to 0$ be an exact sequence of A-modules. Suppose that N is finitely generated and torsion-free.*

(a) If M is reflexive, then $\mathrm{Ass}(Q) \subseteq P(A) \cup \{(0)\}$ (in other words, every ideal associated with Q is either (0) or of height 1).

(b) Conversely, if N is reflexive and $\mathrm{Ass}(Q) \subseteq P(A) \cup \{(0)\}$, then M is reflexive.

Proof. As A is Noetherian, M is finitely generated. If we write $V = \mathrm{Ind}_A^K M$ and $W = \mathrm{Ind}_A^K N$, then M (resp. N) is canonically identified with a lattice of V (resp. W) (Proposition 15.2.2). Consider the two exact sequences:

$$0 \to V/M \to W/M \to W/V \to 0, \quad 0 \to Q \to W/M \to W/N \to 0.$$

from which we deduce that

$$\mathrm{Ass}(Q) \subseteq \mathrm{Ass}(W/M) \subseteq \mathrm{Ass}(V/M) \cup \mathrm{Ass}(W/V)$$

If M is reflexive, then $\mathrm{Ass}(V/M) \subseteq P(A)$. On the other hand, clearly $\mathrm{Ass}(W/V)$ is, either empty, or reduced to $\{0\}$, whence (a). Similarly,

$$\mathrm{Ass}(V/M) \subseteq \mathrm{Ass}(W/M) \subseteq \mathrm{Ass}(Q) \cup \mathrm{Ass}(W/N)$$

The hypotheses N is reflexive then imply that $\mathrm{Ass}(V/M) \subseteq P(A) \cup \{(0)\}$. But V/M is a torsion A-module and hence $(0) \notin \mathrm{Ass}(V/M)$; Theorem 15.2.14 then shows that M is reflexive. □

Proposition 15.2.19. *Let A and B be two rings, $\rho : A \to B$ a ring homomorphism and M a finitely generated A-module. Suppose that A is Noetherian and that B is a flat A-module. Then, if M is reflexive, so is the B-module $\mathrm{Ind}_A^B = M \otimes_A B$.*

Proof. We know that there exists a canonical isomorphism $\omega_M : \mathrm{Ind}_A^B(M^*) \to (\mathrm{Ind}_A^B M)^*$, such that

$$\langle \omega_M(x^* \otimes 1), x \otimes 1\rangle = f(\langle x^*, x\rangle)$$

for $x \in M$, $x^* \in M^*$. As M is a quotient of a finitely generated free A-module L, M^* is isomorphic to a sub-A-module of the dual L^* and L^* is free and finitely generated; since A is Noetherian, M^* is therefore also a finitely generated A-module, whence an isomorphism $\omega_{M^*} : \mathrm{Ind}_A^B(M^{**}) \to (\mathrm{Ind}_A^B(M^*))^*$ such that

$$\langle \omega_{M^*}(x^{**} \otimes 1), x^* \otimes 1\rangle = f(\langle x^{**}, x^*)$$

for $x^* \in M$ and $x^{**} \in M^{**}$. On the other hand, there is an isomorphism $\omega_M^t : (\mathrm{Ind}_A^B M)^{**} \to (\mathrm{Ind}_A^B(M^*))^*$, whence by composition a canonical isomorphism

$$\phi = (\omega_M^t)^{-1} \circ \omega_{M^*} : \mathrm{Ind}_A^B(M^{**}) \to (\mathrm{Ind}_A^B M)^{**}$$

such that, in the above notation:

$$\langle \phi(x^{**} \otimes 1), \omega_M(x^* \otimes 1)\rangle = f(\langle x^{**}, x^*\rangle). \tag{2.2.1}$$

We consider now the canonical homomorphism $J_M : M \to M^{**}$ and show that the composite homomorphism:

$$\psi = (J_M \otimes 1) \circ \phi : \mathrm{Ind}_A^B M \to \mathrm{Ind}_A^B(M^{**}) \to (\mathrm{Ind}_A^B M)^{**}$$

is just the canonical homomorphism $J_{\mathrm{Ind}_A^B M}$. This follows immediately from (2.2.1) which gives the relations:

$$\langle \psi(x \otimes 1), \omega_M(x^* \otimes 1)\rangle = f(\langle J_M(x), x^*\rangle) = f(\langle x^*, x\rangle) = \langle \omega_M(x^* \otimes 1), x \otimes 1\rangle.$$

and from the fact that the elements $\omega_M(x^* \otimes 1)$ generate $(\mathrm{Ind}_A^B M)^*$. This being so, the hypothesis that M is reflexive means that J_M is bijective, hence so is $J_M \otimes 1$ and therefore $\psi = J_{\mathrm{Ind}_A^B M}$ is bijective, which shows the proposition. □

15.2.3 Local construction of reflexive modules

We keep the notation and hypotheses of the last part. We shall say that a property holds "for almost all $\mathfrak{p} \in P(A)$" if the set of $\mathfrak{p} \in P(A)$ for which it is not true is finite.

Lemma 15.2.20. *Let $\mathfrak{p}$ and $\mathfrak{q}$ be two prime ideals of A such that (0) is the only prime ideal of A contained in $\mathfrak{p} \cap \mathfrak{q}$. Then, for every sub-$A$-module E of V, $(E_{\mathfrak{p}})_{\mathfrak{q}} = KE$.*

Proof. Let S be the multiplicative subset $(A - \mathfrak{p})(A - \mathfrak{q})$ of A; by Corollary 10.2.21, $(E_{\mathfrak{p}})_{\mathfrak{q}} = S^{-1}E$. The prime ideals of $S^{-1}A$ correspond to the prime ideals $\mathfrak{q}$ of A such that $\mathfrak{p}' \cap S = \varnothing$ and by hypothesis (0) is the only prime ideal of A not meeting S; hence $S^{-1}A = K$ and $S^{-1}E = KE$. □

Theorem 15.2.21. *Let V be a vector space of finite dimension over K and M a lattice of V with respect to A.*

(a) Let N be a lattice of V with respect to A. Then for every prime ideal $\mathfrak{p}$ of A, $N_{\mathfrak{p}}$ is a lattice of V with respect to $A_{\mathfrak{p}}$ and, for almost all $\mathfrak{p} \in P(A)$, $N_{\mathfrak{p}} = M_{\mathfrak{p}}$.

(b) Conversely, suppose given for all $\mathfrak{p} \in P$ a lattice $N(\mathfrak{p})$ of V with respect to $A_{\mathfrak{p}}$ such that $N(\mathfrak{p}) = M_{\mathfrak{p}}$ for almost all $\mathfrak{p} \in P(A)$. Then $N = \bigcap_{\mathfrak{p}\in P(A)} N(\mathfrak{p})$ is a reflexive lattice of V with respect to A and it is the only reflexive lattice of V with respect to A whose localization at $\mathfrak{p}$ is $N(\mathfrak{p})$ for all $\mathfrak{p} \in P(A)$.

Proof. The first assertion follows from Proposition 15.2.9. Moreover, there exist x, y in $K^\times$ such that $xN \subseteq M \subseteq yN$. We know that, for almost all $\mathfrak{p} \in P(A)$, $v_{\mathfrak{p}}(x) = v_{\mathfrak{p}}(y) = 0$, which shows that x and y are invertible in A and hence $M_{\mathfrak{p}} = N_{\mathfrak{p}}$.

Now we prove (b). We may replace M by $x^{-1}M$ where $x \neq 0$ in A and assume that $N(\mathfrak{p}) \subseteq M_{\mathfrak{p}}$ for all $\mathfrak{p} \in P(A)$. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ be the elements of $P(A)$ such that $N(\mathfrak{p}) =$ for $\mathfrak{p}$ distinct from the $\mathfrak{p}_i$, we write:

$$Q = M \cap N(\mathfrak{p}_1) \cap \cdots \cap N(\mathfrak{p}_n).$$

As each of the $N(\mathfrak{p}_i)$ contain a free lattice with respect to $A_{\mathfrak{p}_i}$, it contains a fortiori a lattice of V with respect to A, hence Q contains a lattice of V with respect to A (Proposition 15.2.5) and, as Q is contained in M, Q is a lattice with respect to A. If $\mathfrak{p} \in P$ is distinct from the $\mathfrak{p}_i$, Lemma 15.2.20 applied to $N(\mathfrak{p}_i)$ gives

$$(N(\mathfrak{p}_i))_{\mathfrak{p}} = ((N(\mathfrak{p}_i))_{\mathfrak{p}_i})_{\mathfrak{p}} = KN(\mathfrak{p}_i) = V$$

since the $\mathfrak{p}_i$ and $\mathfrak{p}$ are of height 1. Then

$$Q_{\mathfrak{p}} = M_{\mathfrak{p}} \cap (N(\mathfrak{p}_i))_{\mathfrak{p}} \cap \cdots \cap (N(\mathfrak{p}_n))_{\mathfrak{p}} = M_{\mathfrak{p}} = N(\mathfrak{p}).$$

On the other hand, if $\mathfrak{p}$ is equal to $\mathfrak{p}_i$, then $(N(\mathfrak{p}_i))_{\mathfrak{p}_j} = V$ for $i \neq j$ by the argument as above and $(N(\mathfrak{p}_i))_{\mathfrak{p}_i} = N(\mathfrak{p}_i)$, whence

$$Q_{\mathfrak{p}_i} = M_{\mathfrak{p}_i} \cap N(\mathfrak{p}_i) = N(\mathfrak{p}_i).$$

We have therefore proved that $Q_{\mathfrak{p}} = N(\mathfrak{p})$ for all $\mathfrak{p} \in P(A)$. Then $N = Q^{**} = \bigcap_{\mathfrak{p}\in P(A)} Q_{\mathfrak{p}}$ is reflexive and satisfies the relations $N_{\mathfrak{p}} = Q_{\mathfrak{p}} = N(\mathfrak{p})$ for all $\mathfrak{p} \in P(A)$. The uniqueness property follows immediately from Theorem 15.2.14. □

Proposition 15.2.22. *Let M be a finitely generated A-module. The following conditions are equivalent:*

(i) $M_{\mathfrak{p}} = 0$ for every prime ideal $\mathfrak{p}$ of height ≤ 1.

(ii) The annihilator $\mathfrak{a}$ of M is nonzero and $(A : \mathfrak{a}) = A$.

*An A-module M is called **pseudo-zero** if it is finitely generated and it satisfies the equivalent conditions above.*

Proof. We know (by Corollary 10.2.16) that the condition $M_\mathfrak{p} = 0$ is equivalent to $\mathfrak{a} \not\subseteq \mathfrak{p}$ and hence to $\mathfrak{a}A_\mathfrak{p} = A_\mathfrak{p}$. On the other hand, for every integral ideal $\mathfrak{b} \neq 0$ of A, the relation "$\mathfrak{b}A_\mathfrak{p} = A_\mathfrak{p}$ for all $\mathfrak{p} \in P(A)$" is equivalent to $\operatorname{div}(\mathfrak{b}) = \operatorname{div}(A) = 0$ in $\mathfrak{D}(A)$ (Proposition 15.1.16), or also to $\operatorname{div}(A : \mathfrak{b}) = 0$ and, as $(A : \mathfrak{b})$ is divisorial, this relation is also equivalent to $(A : \mathfrak{b}) = A$. The proposition then follows by noting that to say that $\mathfrak{a} \not\subseteq (0)$ means that $\mathfrak{a} \neq (0)$. □

Example 15.2.23 (Example of pseudo-zero modules).

(a) If A is a Dedekind domain, every prime ideal of A is of height 1, so to say that M is pseudo-zero means then that $\operatorname{supp}(M) = \varnothing$ and hence that $M = 0$.

(b) Let k be a field and $A = k[X, Y]$ the polynomial ring over k in two indeterminates. If $\mathfrak{m}$ is the maximal ideal $AX + AY$ of A, the A-module $A/\mathfrak{m}$ is pseudo-zero, for its annihilator $\mathfrak{m}$ is not of height ≤ 1 since it contains the principal prime ideals AX and AY and is distinct from them; therefore $(A : \mathfrak{m}) = A$.

Let $\phi : M \to N$ a homomorphism of A-modules. Then ϕ is called **pseudo-injective** (resp. **pseudo-surjective**, **pseudo-zero**) if $\ker \phi$ (resp. $\operatorname{coker} \phi$, $\operatorname{im} \phi$) is pseudo-zero. Also ϕ is called **pseudo-bifective** if it is both pseudo-injective and pseudo-surjective. A pseudo-bijective homomorphism is also called a **pseudo-isomorphism**.

Suppose that M and N are finitely generated. Then, for $\phi : M \to N$ to be pseudo-injective (resp. pseudo-surjective, pseudo-zero), it is necessary and sufficient that, for all $\mathfrak{p} \in P(A) \cup \{(0)\}$, $\phi_\mathfrak{p} : M_\mathfrak{p} \to N_\mathfrak{p}$ be injective (resp. surjective, zero) (this follows from the exactness of the A-module $A_\mathfrak{p}$).

Example 15.2.24. Let M be a torsion-free finitely generated A-module. Then M is identified with a lattice of $V = M \otimes_A K$. We have seen that $(M_\mathfrak{p})_\mathfrak{q} = V$ for $\mathfrak{p} \neq \mathfrak{q}$ in $P(A)$, therefore $M_\mathfrak{p} = M_\mathfrak{p}^{**}$ for all $\mathfrak{p} \in P(A)$. Also, for $\mathfrak{p} = 0$, $M_\mathfrak{p}$ and $M_\mathfrak{p}^{**}$ are both equal to V. Therefore the canonical mapping $J_M : M \to M^{**}$ of M to its bidual is a pseudo-isomorphism.

Example 15.2.25. For all $\mathfrak{p} \in P(A)$, the canonical mapping $\phi : A/\mathfrak{p}^n \to A/\mathfrak{p}^{(n)} = A/(A \cap \mathfrak{p}^n A_\mathfrak{p})$ is a pseudo-isomorphism, as, for all $\mathfrak{q} \in P(A)$ distinct from $\mathfrak{p}$, $A_\mathfrak{q}/\mathfrak{p}^n A_\mathfrak{q} = A_\mathfrak{q}/\mathfrak{p}^{(n)} A_\mathfrak{q} = 0$ and $A_\mathfrak{p}/\mathfrak{p}^n A_\mathfrak{p} = A_\mathfrak{p}/\mathfrak{p}^{(n)} A_\mathfrak{p}$.

Theorem 15.2.26. *Let E be a finitely generated A-module, T the torsion submodule of E and $M = E/T$. There exists a pseudo-isomorphism $\phi : E \to T \times M$.*

For this theorem, we shall first prove two lemmas.

Lemma 15.2.27. *Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ be a family of prime ideals of A of height 1 and let $S = \bigcap_{i=1}^k (A - \mathfrak{p}_i)$. Then the ring $S^{-1}A$ is a principal ideal domain.*

Proof. The ring $S^{-1}A$ is a semi-local ring whose maximal ideals are the $\mathfrak{m}_i = S^{-1}\mathfrak{p}_i$ for $1 \leq i \leq k$, the local ring $(S^{-1}A)_{\mathfrak{m}_i}$ being isomorphic to $A_{\mathfrak{p}_i}$ and hence a discrete valuation ring. The ring $S^{-1}A$ is therefore a Dedekind domain and, as it is semi-local it is a principal ideal domain. □

Lemma 15.2.28. *There exists a homomorphism $\eta : E \to T$ whose restriction to T is both a homothety and a pseudo-isomorphism.*

Proof. Let $\mathfrak{a}$ be the annihilator of T. As T is a finitely generated torsion A-module, $\mathfrak{a} \neq 0$. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ be the prime ideals of height 1 containing $\mathfrak{a}$ (which are finite in number). If this number is 0, T is pseudo-zero (Proposition 15.2.22) and we may take $\eta = 0$. Otherwise, let $S = \bigcap_{i=1}^{k}(A - \mathfrak{p}_i)$; by Lemma 15.2.27, $S^{-1}A$ is a PID and hence $S^{-1}M$, which is a torsion-free finitely generated $S^{-1}A$-module, is free and, as $S^{-1}M = (S^{-1}E)/(S^{-1}T)$, $S^{-1}T$ is a direct factor of $S^{-1}E$. Now,

$$\mathrm{Hom}_{S^{-1}A}(S^{-1}E, S^{-1}T) = S^{-1}\mathrm{Hom}_A(E, T)$$

hence there exist $s_0 \in S$ and $\eta_0 \in \mathrm{Hom}_A(E, T)$ such that $s_0^{-1}\eta_0$ is a projector of $S^{-1}E$ onto $S^{-1}T$. If $\psi_0 \in \mathrm{Hom}_A(T, T)$ denotes the restriction of η_0 to T, there therefore exists $s_1 \in S$ such that $s_1\psi_0(x) = s_1 s_0 x$ for all $x \in T$. Writing $s = s_1 s_0$, $\eta = s_1\eta_0$, $\psi = s_1\psi_0$, then ψ is the homothety of ratio s on T and is the restriction of η to T. It remains to verify that ψ is a pseudo-isomorphism.

Now, if $\mathfrak{p} = 0$ or if $\mathfrak{p} \in P(A)$ is distinct from the $\mathfrak{p}_i$, then $T_\mathfrak{p} = 0$ and $\psi_\mathfrak{p} : T_\mathfrak{p} \to T_\mathfrak{p}$ is an isomorphism. If on the contrary $\mathfrak{p}$ is equal to one of the $\mathfrak{p}_i$, then s is invertible in $A_{\mathfrak{p}_i}$ and $h_{\mathfrak{p}_i}$ is the homothety of ratio s on $T_{\mathfrak{p}_i}$ is also an isomorphism, which completes the proof of Lemma 15.2.28. □

Proof of Theorem 15.2.26. Let $\eta : E \to T$ be a homomorphism satisfying the properties of Lemma 15.2.28. Let ψ be the restriction of η to T and let π be the canonical projection of E onto M. We show that the homomorphism $\phi = (\eta, \pi) : E \to T \times M$ solves the problem. There is the commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & T \arrow[r] \arrow[d, "\psi"] & E \arrow[r] \arrow[d, "\phi"] & M \arrow[r] \arrow[d, "1_M"] & 0 \\
0 \arrow[r] & T \arrow[r] & T \times M \arrow[r] & M \arrow[r] & 0
\end{tikzcd}$$

where the rows are exact. The snake diagram gives the exact sequence:

$$0 \longrightarrow \ker\psi \longrightarrow \ker\phi \longrightarrow 0 \longrightarrow \mathrm{coker}\,\psi \longrightarrow \mathrm{coker}\,\phi \longrightarrow 0$$

and hence $\ker\phi$ is isomorphic to $\ker\psi$ and $\mathrm{coker}\,\phi$ to $\mathrm{coker}\,\psi$. As ψ is a pseudo-isomorphism, so is ϕ. □

We can say that "to within a pseudo-isomorphism" Theorem 15.2.26 reduces the study of finitely generated A-modules to that of torsion-free modules on the one hand and to that of torsion modules on the other. Moreover, we have seen above that a torsion-free module is pseudo-isomorphic to its bidual and hence to a reflexive module. As for torsion modules, there is the following result, which determines them to within a pseudo-isomorphism:

Theorem 15.2.29. *Let T be a finitely generated torsion A-module. There exist two finite families $(n_i)_{i\in I}$ and $(\mathfrak{p}_i)_{i\in I}$ where the n_i are positive integers and the $\mathfrak{p}_i$ are prime ideals of A of height 1 such that there exists a pseudo-isomorphism of T to $\bigoplus_{i\in I} A/\mathfrak{p}_i^{n_i}$. Moreover, the families $(n_i)_{i\in I}$ and $(\mathfrak{p}_i)_{i\in I}$ with this property are unique to within a bijection of the indexing set and the $\mathfrak{p}_i$ containing the annihilator of T.*

Proof. Let $T' = \bigoplus_{i\in I} A/\mathfrak{p}_i^{n_i}$. If $\phi : T \to T'$ is a pseudo-isomorphism and $\mathfrak{p} \in P(A)$, then $\phi_\mathfrak{p} : T_\mathfrak{p} \to T_\mathfrak{p}$ is an isomorphism. Now, $T'_\mathfrak{p}$ is the direct sum of the $A_\mathfrak{p}/\mathfrak{p}^{n_i}A_\mathfrak{p}$ the sum being over the indices i such that $\mathfrak{p}_i = \mathfrak{p}$. The $\mathfrak{p}^{n_i}A_\mathfrak{p}$ are therefore the elementary divisors of the torsion $A_\mathfrak{p}$-module $T_\mathfrak{p}$ and are therefore unique.

We may confine our attention to the case where $T \neq 0$. Let $\mathfrak{a}$ be the annihilator (non-zero and distinct from A) of T and $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ the prime ideals of A of height 1 containing $\mathfrak{a}$ (which are finite in number and $S = \bigcap_{i=1}^k (A - \mathfrak{p}_i)$. The semi-local ring $B = S^{-1}A$ is a principal ideal domain and has maximal ideals the $\mathfrak{m}_i = S^{-1}\mathfrak{p}_i$; as $S^{-1}T$ is a finitely generated torsion B-module, it is isomorphic to a finite direct sum $\bigoplus_{i=1}^k B/\mathfrak{m}_i^{n_i}$. As $B/\mathfrak{m}_i^{n_i}$ is isomorphic to $S^{-1}(A/\mathfrak{p}_i^{n_i})$, we have obtained a torsion A-module T' of the desired type and an isomorphism ϕ_0 of $S^{-1}T$ onto $S^{-1}T'$. As $\mathrm{Hom}_{S^{-1}A}(S^{-1}T, S^{-1}T')$ is equal to $S^{-1}\mathrm{Hom}_A(T, T')$, there exist $s \in S$ and a homomorphism $\phi : T \to T'$ such that $\phi_0 = s^{-1}f$. It remains to show that f is a pseudo-isomorphism. Now if $\mathfrak{p} = 0$ or $\mathfrak{p} \in P(A)$ is distinct from the $\mathfrak{p}_i$, then $T_\mathfrak{p} = T'_\mathfrak{p} = 0$. If on the contrary $\mathfrak{p}$ is one of the $\mathfrak{p}_i$, s is invertible in $A_{\mathfrak{p}_i}$ and, as $\phi_{\mathfrak{p}_i} = s(\phi_0)$ and $(\phi_0)_{\mathfrak{p}_i}$ is an isomorphism of $T_{\mathfrak{p}_i} = (S^{-1}T)_{\mathfrak{m}_i}$ onto $T'_{\mathfrak{p}_i} = (S^{-1}T')_{\mathfrak{m}_i}$, so is $\phi_{\mathfrak{p}_i}$. □

Given an exact sequence of A-modules $0 \to E \to F \to G \to 0$, if E and G are pseudo-zero, so is F, as follows from definition and the exactness of localization. In the language of categories, we may then say that, in the category C of A-modules, the sub-category C' of pseudo-zero modules is full and we may then define the quotient category C/C'. The objects in this category are also A-modules but the set of morphisms from E to F (for E, F in C) is the direct limit of the set of commutative groups $\mathrm{Hom}_A(E', F')$, where E' (resp. F') runs through the set of submodules of E (resp. the set of quotient modules F/F'' of F) such that E/E' (resp. F'') is pseudo-zero. Of course, for every ordered pair of A-modules E, F, there is a canonical homomorphism $\mathrm{Hom}_C(E, F) \to \mathrm{Hom}_{C/C'}(E, F)$. To say that a homomorphism $\phi \in \mathrm{Hom}_A(E, F)$ is pseudo-zero (resp. pseudo-injective, pseudo-surjective, pseudo-bijective) means that its canonical image in $\mathrm{Hom}_{C/C'}(E, F)$ is zero (resp. a monomorphism, an epimorphism, an isomorphism).

15.2.4 Divisors attached to finite generated torsion modules

We keep to assume that A is Noetherian and integrally closed. Recall that $\mathfrak{D}(A)$ denotes the divisor group of A, written additively. We know that $\mathfrak{D}(A)$ is the free $\mathbb{Z}$-module generated by the elements of $P(A)$.

Let T be a finitely generated torsion A-module. For all $\mathfrak{p} \in P(A)$, $T_\mathfrak{p}$ is a finitely generated torsion $A_\mathfrak{p}$-module and hence a module of finite length (Corollary 12.2.16). We shall denote this length by $\ell_\mathfrak{p}(T)$. Now $T_\mathfrak{p} = 0$ for all $\mathfrak{p}$ not containing the annihilator of T and hence for almost all $\mathfrak{p}$, which justifies the following definition:

Definition 15.2.30. *If T is a finitely generated torsion A-module, the divisor:*

$$\chi(T) = \sum_{\mathfrak{p} \in P(A)} \ell_\mathfrak{p}(T) \cdot \mathfrak{p}$$

*is called the **content** of T.*

Proposition 15.2.31. *Let χ be the content function defined above.*

(a) The function χ is additive.

(b) If T_1 and T_2 are pseudo-isomorphic, then $\chi(T_1) = \chi(T_2)$.

(c) In order that $\chi(T) = 0$, it is necessary and sufficient that T be pseudo-zero.

Proof. In view of the definition, it suffices to consider for each $\mathfrak{p} \in P(A)$ the values of $\ell_{\mathfrak{p}}$, for the torsion modules considered. The claimed properties then follows from that of length function. □

Corollary 15.2.32. *If there is a long exact sequence*

$$0 \longrightarrow T_n \longrightarrow T_{n-1} \longrightarrow \cdots \longrightarrow T_0 \longrightarrow 0$$

of finitely generated torsion A-modules, then $\sum_{i=0}^{n}(-1)^i \chi(T_i) = 0$.

Recall that we may speak of the set $F(A)$ of classes of finitely generated A-madules with respect to the relation of isomorphism; for every finitely generated A-module M, let $\mathrm{cl}(M)$ denote the corresponding element of $F(A)$. We shall denote by $T(A)$ the subset of $F(A)$ consisting of the classes of finitely generated torsion A-modules. Clearly χ defines a mapping of $T(A)$ to $\mathfrak{D}(A)$, also denoted by χ, such that $\chi(\mathrm{cl}(T)) = \chi(T)$.

Proposition 15.2.33. *Let G be a commutative group and $\delta : T(A) \to G$ a function. For every finitely generated torsion A-module T, we also write, by an abuse of language, $\delta(T) = \delta(\mathrm{cl}(T))$. Suppose that the following conditions are satisfied:*

(a) The function δ is additive.

(b) If T is pseudo-zero, then $\delta(T) = 0$.

Then there exists a unique homomorphism $\theta : \mathfrak{D}(A) \to G$ such that $\delta = \theta \circ \chi$.

Proof. As $\chi(A/\mathfrak{p}) = \mathfrak{p}$ for all $\mathfrak{p}$, necessarily $\theta(\mathfrak{p}) = \delta(A/\mathfrak{p})$ for all $\mathfrak{p} \in P(A)$, which proves the uniqueness of θ, since the elements of $P(A)$ form a basis of $\mathfrak{D}(A)$. Conversely, let θ be the homomorphism from $\mathfrak{D}(A)$ to G such that $\theta(p) = \delta(A/\mathfrak{p})$ for all $\mathfrak{p} \in P(A)$ and let us show that it solves the problem. For this, we write

$$\psi(T) = \delta(T) - \theta(\chi(T))$$

for every finitely generated torsion A-module T. Clearly conditions (a) and (b) are also satisfied if δ is replaced by ψ. On the other hand, $\psi(A/\mathfrak{p}) = 0$ if $\mathfrak{p} \in P(A)$. If $\mathfrak{p}$ is a nonzero prime ideal and not in P, the annihilator of $A/\mathfrak{p}$ is contained in no ideal of $P(A)$, hence $A/\mathfrak{p}$ is pseudo-zero and therefore $\psi(A/\mathfrak{p}) = 0$. This being so, every finitely generated torsion A-module T admits a chain og submodules whose factors are isomorphic to A-modules of the form $A/\mathfrak{p}$, where $\mathfrak{p} \in \mathrm{supp}(T)$ (Theorem 12.1.18), and hence $\mathfrak{p} \neq 0$ since T is a torsion module. By induction on the length of this decomposition series, we deduce (in view of property (a) for ψ) that $\psi(T) = 0$. □

Remark 15.2.1. We may consider the quotient category $\mathcal{A}/\mathcal{A}'$ of the category $\mathcal{A}$ of finitely generated torsion A-modules by the full sub-category $\mathcal{A}'$ of pseudo-zero finitely generated torsion A-modules. In the language of Abelian categories, Proposition 15.2.33 then expresses the fact that the Grothendieck group of the Abelian category $\mathcal{A}/\mathcal{A}'$ is canonically isomorphic to $\mathfrak{D}(A)$.

Proposition 15.2.34. *If $\mathfrak{a}$ is a nonzero ideal of A, then*

$$\chi(A/\mathfrak{a}) = \chi((A : \mathfrak{a})/A) = \mathrm{div}(\mathfrak{a}).$$

Proof. Let $\mathfrak{p} \in P(A)$. Then since $A_\mathfrak{p}$ is a DVR we have $\mathfrak{a}A_\mathfrak{p} = \mathfrak{p}^{n_p}A_\mathfrak{p}$ where some $n_\mathfrak{p} \neq 0$. As $(A/\mathfrak{a})_\mathfrak{p} = A_\mathfrak{p}/\mathfrak{a}A_\mathfrak{p} = (A/a)$, we then see $\ell_\mathfrak{p}(A/\mathfrak{a}) = n_\mathfrak{p}$, whence $\chi(A/\mathfrak{a}) = \sum_{\mathfrak{p}\in P(A)} n_\mathfrak{p}\mathfrak{p} = \operatorname{div}(\mathfrak{a})$ by Proposition 15.1.20. On the other hand, $(A : a)_\mathfrak{p} = (A_\mathfrak{p} : \mathfrak{a}A_\mathfrak{p}) = \mathfrak{p}^{-n_\mathfrak{p}}A_\mathfrak{p}$, hence $\ell_\mathfrak{p}((A : \mathfrak{a})/A) = n_\mathfrak{p}$ and we conclude in the same way. □

Corollary 15.2.35. *Let M be a finitely generated tosion A-module. If $\bigoplus_{i\in I} A/\mathfrak{p}_i^{n_i}$ is the canonical A-module to which M is pseudo-isomorphic to, then*

$$\chi(M) = \sum_{i\in I} n_i\mathfrak{p}_i.$$

Proof. By Proposition 15.2.34, we see $\chi(A/\mathfrak{p}_i^{n_i}) = \operatorname{div}(\mathfrak{p}_i^{n_i}) = n_i\mathfrak{p}_i$, whence the claim. □

Now let V be a vector space of dimension n over K and M a lattice of V with respect to A. Let W be the exterior power $\bigwedge^n V$, which is a one-dimensional vector space over K and let M_W denote the lattice of W generated by the image of M under the canonical map $V^n \to \bigwedge^n V$ (Proposition 15.2.5). If e is a basis of W over K, we may write $M_W = \mathfrak{a}e$, where $\mathfrak{a}$ is a nonzero fractional ideal of A.

Let M' be another lattice of V and let us write $M'_W = \mathfrak{a}'e$, where $\mathfrak{a}'$ is a nonzero fractional ideal of A. The divisor $\operatorname{div}(\mathfrak{a}) - \operatorname{div}(\mathfrak{a}')$ does not depend on the choice of basis e of W, $\mathfrak{a}$ and $\mathfrak{a}'$ being multiplied by the same element of $K^\times$ when the basis is changed. We shall write $\chi(M, M') = \operatorname{div}(\mathfrak{a}) - \operatorname{div}(\mathfrak{a}')$ and say that this divisor is the **relative invariant** of M' with respect to M. Clearly, if M, M', M'' are three lattices of V, then:

$$\chi(M, M') + \chi(M', M'') + \chi(M, M'') = 0, \quad \chi(M, M') + \chi(M', M) = 0.$$

For all $\mathfrak{p} \in P(A)$, it follows immediately from the definitions that $(M_W)_\mathfrak{p} = (M_\mathfrak{p})_W$. Moreover, since $M_\mathfrak{p}$ is then a free A-module since A is a principal ideal domain, a basis of M over A is a basis of V over K, hence $(M_\mathfrak{p})_W = \bigwedge^n(M_\mathfrak{p})$ and the fractional ideal $\mathfrak{a}_\mathfrak{p}$ equals $\mathfrak{a}A_\mathfrak{p}$. If we set $\mathfrak{a}_\mathfrak{p} = \mathfrak{p}^{n_\mathfrak{p}}A_\mathfrak{p}$ and $\mathfrak{a}'_\mathfrak{p} = \mathfrak{p}^{n'_\mathfrak{p}}A_\mathfrak{p}$, then

$$\chi(M, M') = \sum_{\mathfrak{p}\in P(A)} (n_\mathfrak{p} - n'_\mathfrak{p})\mathfrak{p},$$

which may also be written as:

$$\chi(M, M') = \sum_{\mathfrak{p}\in P(A)} \chi(M_\mathfrak{p}, M'_\mathfrak{p}).$$

identifying $\mathfrak{D}(A_\mathfrak{p})$ with the sub-$\mathbb{Z}$-module of $\mathfrak{D}(A)$ generated by $\mathfrak{p}$.

Proposition 15.2.36. *Let M be a lattice of V and ϕ a K-automorphism of V. Then:*

$$\chi(M, \phi(M)) = -\operatorname{div}(\det(\phi)).$$

Proof. For all $\mathfrak{p} \in P(A)$, we have $\bigwedge^n \phi(M_\mathfrak{p}) = \bigwedge^n \phi(M)_\mathfrak{p}$. If $e_1, \dots, e_n$ is a basis of $M_\mathfrak{p}$, then

$$\bigwedge^n(M_\mathfrak{p}) = A_\mathfrak{p} \cdot e_1 \wedge \cdots \wedge e_n, \quad \bigwedge^n \phi(M_\mathfrak{p}) = A_\mathfrak{p}(\det(\phi)) \cdot e_1 \wedge \cdots \wedge e_n$$

whence the claim. □

Proposition 15.2.37. *If M, M' are two lattices of V such that $M' \subseteq M$, then M/M' is a finitely generated torsion A-module and $\chi(M, M') = -\chi(M/M')$.*

Proof. Clearly $M/M' \subseteq V/M'$ is a finitely generated torsion module. On the other hand, for all $\mathfrak{p} \in P(A)$, since $A_\mathfrak{p}$ is a PID, we know that there exist bases $e_1, \dots, e_n$ of $M_\mathfrak{p}$ and $e'_1, \dots, e'_n$ of $M'_\mathfrak{p}$ such that $e'_i = \pi^{\nu_i} e_i$ for all i and integers v, π being a uniformizer of $A_\mathfrak{p}$. Therefore (in the notation introduced above) $n_i - n'_i = \sum_{i=1}^n \nu_i$. Also, $(M/M')_\mathfrak{p} = M_\mathfrak{p}/M'_\mathfrak{p}$ is isomorphic to the torsion $A_\mathfrak{p}$-module $\bigoplus_{i=1}^n A_\mathfrak{p}/\mathfrak{p}_i^{\nu_i} A_\mathfrak{p}$, and hencc its length is $\sum_{i=1}^n \nu_i$, which proves the proposition. □

Corollary 15.2.38. *Let L_1, L_2 be two free A-modules of the same rank n and let $\phi : L_1 \to L_2$ be a homomorphism. For* coker ϕ *to be a torsion A-module, it is necessary and sufficient that* $\det(\phi) \neq 0$ *and in this case,*

$$\chi(\operatorname{coker} \phi) = \operatorname{div}(\det(\phi)).$$

Proof. The modules L_1 and L_2 can be considered as lattices in $V_1 = L_1 \otimes_A K$ and $V_2 = L_2 \otimes_A K$ respectively, ϕ extending to a K-homomorphism $\operatorname{Ind}_A^K \phi$ from V_1 to V_2. Then $\operatorname{Ind}_A^K(\operatorname{coker} \phi) = \operatorname{coker} \operatorname{Ind}_A^K \phi$, and to say that $\operatorname{coker} \phi$ is a torsion A-module means that $\operatorname{coker} \operatorname{Ind}_A^K \phi = 0$. Now, it amounts to the same to say that $\operatorname{Ind}_A^K \phi$ is surjective or that $\det(\operatorname{Ind}_A^K \phi) = \det(\phi) \neq 0$, whence the first assertion. On the other hand, we may write $\phi(L_1) = \psi(L_2)$, where ϕ is an endomorphism of L_2 of determinant $\det(\phi)$. As $\operatorname{coker} \phi = L_2/\psi(L_2)$, the formula follows from Proposition 15.2.36. □

Example 15.2.39. If $A = \mathbb{Z}$, the divisor group of A is identified with the multiplicative group $\mathbb{Q}_+^\times$ of rational numbers > 0. For every finite commutative group T, $\chi(T)$ is the order of T; the above corollary shows that the order of the group $\operatorname{coker} \phi$ is equal to the absolute value of $\det(\phi)$.

15.2.5 Divisor classes attached to a finite generated module

Recall that $\mathfrak{C}(A)$ denotes the divisor class group of A, the quotient of $\mathfrak{D}(A)$ by the subgroup of principal divisors. For every divisor $D \in \mathfrak{D}(A)$, we shall denote by $c(D)$ its class in $\mathfrak{C}(A)$.

Proposition 15.2.40. *Let M be a finitely generated A-module. There exists a free submodule L of M such that M/L is a torsion module and the element $c(\chi(M/L))$ of $\mathfrak{C}$ does not depend on the free submodule L. The element $c(M) := -c(\chi(M/L))$ will be called the* ***divisor class attached to M****.*

Proof. We write $S = A - \{0\}$ and let $V = S^{-1}M = M \otimes_A K$. If n is the dimension of V over K, there exist n elements $e_1, \dots, e_n$ of M whose canonical images in V form a basis of V. These elements are obviously linearly independent in M and hence generate a free submodule L of M such that $S^{-1}(M/L) = S^{-1}M/S^{-1}L = 0$, so that M/L is a torsion module.

Now let L_1 be another free submodule of M of rank n. Since $S^{-1}L = S^{-1}L_1$, there exists $s \in S$ such that $sL_1 \subseteq L$. We may therefore limit ourselves to proving that, if $L_1 \subseteq L_2$ are two free submodules of M of rank n, then

$$c(\chi(M/L_1)) = c(\chi(M/L_2)).$$

Now, $\chi(M/L_1) = \chi(M/L_2) + \chi(L_2/L_1)$ and it follows from Corollary 15.2.38 that $\chi(L_2/L_1)$ is a principal divisor and therefore the claim follows. □

Proposition 15.2.41 (Properties of the divisor class of modules).

(a) The function c is additive.

(b) If M_1 and M_2 are pseudo-isomorphic, then $c(M_1) = c(M_2)$.

(c) If T is a torsion A-module, then $c(T) = -c(\chi(T))$.

(d) If $\mathfrak{a}$ is a nonzero fractional ideal of A, then $c(\mathfrak{a}) = -c(\mathrm{div}(\mathfrak{a}))$.

(e) If L is a free A-module then $c(L) = 0$.

Proof. To prove (a), consider a exact sequence

$$0 \longrightarrow M_1 \xrightarrow{\phi} M_2 \xrightarrow{\psi} M_3 \longrightarrow 0$$

Then there are free sub-module L_1 (resp. L_3) of M_1 (resp. M_3) such that M_1/L_1 (resp. M_3/L_3) is a torsion module. Since L_3 is free and ψ is surjective, there exists in $\psi^{-1}(L_3)$ a free complement L_{23} of $\ker\psi$ which is isomorphic to L_3. But $\ker\psi = \mathrm{im}\,\phi$ contains $\phi(L_1) = L_{12}$ which is free since ϕ is injective. The sum $L_2 = L_{12} + L_{23}$ is direct and L_2 is therefore a free submodule of M_2. There is moreover the commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & L_1 \arrow[r] \arrow[d] & L_2 \arrow[r] \arrow[d] & L_3 \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & M_1 \arrow[r, "\phi"] & M_2 \arrow[r, "\psi"] & M_3 \arrow[r] & 0
\end{tikzcd}$$

where the rows are exact and the vertical arrows are injections. We therefore obtain from the snake diagram the exact sequence:

$$0 \longrightarrow M_1/L_1 \longrightarrow M_2/L_2 \longrightarrow M_3/L_3$$

As M_1/L_1 and M_3/L_3 are torsion modules, this exact sequence shows first that so is M_2/L_2 and then

$$\chi(M_2/L_2) = \chi(M_1/L_1) + \chi(M_3/L_3)$$

which proves (a).

Assertions (c) and (e) are obvious from the definition. We prove (b). Therefore let $\phi : M_1 \to M_2$ be a pseudo-isomorphism and let L_1 be a free submodule of M_1 such that M_1/L_1 is a torsion module. We set $L_2 = \phi(L_1)$; as $\ker\phi$ is pseudo-zero, it is a torsion module, hence $\ker\phi \cap L_1 = 0$ and therefore L_2 is free. Let $\bar{\phi} : M_1/L_1 \to M_2/L_2$ be the homomorphism derived from ϕ by taking quotients; $\ker\phi$ is isomorphic to $\ker\bar{\phi}$ and $\mathrm{coker}\,\phi$ to $\mathrm{coker}\,\bar{\phi}$ and hence $\bar{\phi}$ is a pseudo-isomorphism. Moreover $\mathrm{coker}\,\bar{\phi} = M_2/\bar{\phi}(M_1)$ is a torsion module and so is $\phi(M_1)/L_2 = \phi(M_1/L_1)$, hence M_2/L_2 is a torsion module and it follows that $\chi(M_1/L_1) = \chi(M_2/L_2)$.

Finally it remains to prove (d). Let $x \in K^\times$ be such that $\mathfrak{a} \subseteq xA$. By considering the exact sequence $0 \to \mathfrak{a} \to xA \to xA/\mathfrak{a} \to 0$, we obtain

$$c(\mathfrak{a}) = c(xA) - c(xA/\mathfrak{a}) = -c(xA/\mathfrak{a})$$

by (a) and (e). But $xA/\mathfrak{a}$ is isomorphic to $A/x^{-1}\mathfrak{a}$, whence, by virtue of (c),

$$c(xA/\mathfrak{a}) = -c(\chi(A/x^{-1}\mathfrak{a})) = -c(\operatorname{div}(x^{-1}\mathfrak{a})) = -c(\operatorname{div}(\mathfrak{a}))$$

This completes the proof. □

Corollary 15.2.42. *If there is a long exact sequence*

$$0 \longrightarrow M_n \longrightarrow M_{n-1} \longrightarrow \cdots \longrightarrow M_0 \longrightarrow 0$$

of finitely generated A-modules, then $\sum_{i=0}^{n}(-1)^i c(M_i) = 0$.

Proof. We argue by induction on n, the case $n = 2$ being Proposition 15.2.41(a). If $N_{n-1} = \operatorname{coker}(M_n \to M_{n-1})$, there are the two exact sequences:

$$0 \longrightarrow M_n \longrightarrow M_{n-1} \longrightarrow N_{n-1} \longrightarrow 0$$

$$0 \longrightarrow N_{n-1} \longrightarrow M_{n-2} \longrightarrow \cdots \longrightarrow M_0 \longrightarrow 0$$

The first shows that M_{n-1} is finitely generated and the induction hypothesis gives

$$(-1)^{n-1}c(N_{n-1}) + \sum_{i=0}^{n-2} c(M_i) = 0$$

and

$$c(N_{n-1}) = c(M_{n-1}) - c(M_n),$$

whence the corollary. □

Corollary 15.2.43. *If a nonzero divisorial fractional ideal $\mathfrak{a}$ of A admits a finite free resolution, it is principal.*

Proof. In fact we apply Corollary 15.2.42 to a finite free resolution of $\mathfrak{a}$:

$$0 \longrightarrow L_n \longrightarrow L_{n-1} \longrightarrow \cdots \longrightarrow L_0 \longrightarrow \mathfrak{a} \longrightarrow 0$$

By Proposition 15.2.41(e), we see $c(\mathfrak{a}) = 0$, so $\operatorname{div}(\mathfrak{a})$ is principal (Proposition 15.2.41(d)). As $\mathfrak{a}$ is assumed to be divisorial, it is principal. □

Corollary 15.2.44. *If every nonzero divisorial ideal of A admits a finite free resolution, A is factorial.*

If M is a finitely generated A-module, we shall denote its rank by $\operatorname{rank}(M)$ (recall that it is the dimension over K of $M \otimes_A K$). We know that $\operatorname{rank}(M)$ is a additive function. We write

$$\gamma(M) = (\operatorname{rank}(M), c(M)) \in \mathbb{Z} \times \mathfrak{C}(A).$$

Then γ is also additive and, if M is pseudo-zero, $\gamma(M) = 0$ (since M is a torsion module). There exists a unique mapping from $F(A)$ to $\mathbb{Z} \times \mathfrak{C}(A)$, also denoted by γ, such that $\gamma(M) = \gamma(\operatorname{cl}(M))$ for every finitely generated A-module M. We shall see that the above properties essentially characterize γ:

Proposition 15.2.45. *Let G be a commutative group and δ a map from the set $F(A)$ of classes of finitely generated A-modules to G. For every finitely generated A-module M we also write, by an abuse of language, $\delta(M) = \delta(\mathrm{cl}(M))$. Suppose the following conditions are satisfied:*

(a) δ is additive.

(b) If T is pseudo-zero, then $\delta(T) = 0$.

Then there exists a unique homomorphism $\delta : \mathbb{Z} \times \mathfrak{C}(A) \to G$ such that $\delta = \theta \circ \gamma$.

Proof. By Proposition 15.2.41, every element of $\mathbb{Z} \times \mathfrak{C}(A)$ is of the form $(\mathrm{rank}(M), c(M))$ for some suitable finitely generated A-module M; whence the uniqueness of θ. We apply Proposition 15.2.33 to the restriction of $-\delta$ to $T(A)$: then there exists a homomorphism $\theta_0 : \mathfrak{D}(A) \to G$ such that

$$-\delta(T) = \theta_0(\chi(T)).$$

for every finitely generated torsion A-module T. Let x be a non-zero element of A; applying property (a) to the exact sequence:

$$0 \longrightarrow A \xrightarrow{h_x} A \longrightarrow A/xA \longrightarrow 0$$

where h_x is multiplication by x, we obtain $\delta(A/xA) = 0$, whence $\theta_0(\mathrm{div}(x)) = 0$. Taking quotients, θ_0 therefore defines a homomorphism $\theta_1 : \mathfrak{C}(A) \to G$ and $\delta(T) = \theta_1(c(T))$ for every torsion A-module T. We show now that the homomorphism θ defined by $\theta(n, z) = n\delta(A) + \theta_0(z)$ solves the problem. For this, we write $\delta'(M) = \delta(M) - \theta(\gamma(M))$ for every finitely generated A-module M. Clearly condition (a) is still satisfied if δ is replaced by δ'. Moreover, $\delta'(M) = 0$ when M is a torsion module or a free module. But as for every finitely generated A-module M, there exists a free sub-module L of M such that M/L is a torsion module, property (a) shows that $\delta'(M) = 0$ for every finitely generated A-module M. □

Remark 15.2.2. In the language of Abelian categories, Proposition 15.2.45 shows that $\mathbb{Z} \times \mathfrak{C}(A)$ is canonically isomorphic to the Grothendieck group of the quotient category $\mathcal{F}/\mathcal{F}'$, where $\mathcal{F}$ is the category of finitely generated A-modules and $\mathcal{F}'$ the full sub-category of $\mathcal{F}$ consisting of the pseudo-zero modules.

15.2.6 Properties relative to finite field extensions

In this part A and B denote two integrally closed Naetherian domains such that $A \subseteq B$ and B is a finitely generated A-module. Let K and L the fields of fractions of A and B respectively. We shall write instead of div_A, χ_A, c_A, χ_A respectively where A-modules are concerned and use analogous notation for B-modules.

We know that B is integral over A by Proposition 13.1.1, so for a prime ideal $\mathfrak{P}$ of B to be of height 1, it is necessary and sufficient that $\mathfrak{p} = \mathfrak{P} \cap A$ be of height 1. Moreover by Corollary 15.1.53, for $\mathfrak{p} \in P(A)$, there is only a finite number of prime ideals $\mathfrak{P} \in P(B)$ lying over $\mathfrak{p}$. To abbreviate, we shall denote by $\mathfrak{P}|\mathfrak{p}$ the relation "$\mathfrak{P}$ lies over $\mathfrak{p}$". We shall then denote by $e_{\mathfrak{P}/\mathfrak{p}}$ or $e(\mathfrak{P}/\mathfrak{p})$ the ramification index of the valuation $v_{\mathfrak{P}}$ over the valuation $v_{\mathfrak{p}}$ and by $f_{\mathfrak{P}/\mathfrak{p}}$ or $f(\mathfrak{P}/\mathfrak{p})$ the residue degree $f(v_{\mathfrak{P}}/v_{\mathfrak{p}})$. Recall that the discrete valuations $v_{\mathfrak{p}}$ and $v_{\mathfrak{P}}$ are normed and that $f_{\mathfrak{P}/\mathfrak{p}}$ is the degree of the field of fractions of $B/\mathfrak{P}$ over the field of fractions of $A/\mathfrak{p}$. We

set $n = \mathrm{rank}_A(B)$, where B is considered as an A-module; hence by definition $n = [L : K]$ and, for all $\mathfrak{p} \in P(A)$, n is also the rank of the free $A_\mathfrak{p}$-module $B_\mathfrak{P}$ for all $\mathfrak{P}|\mathfrak{p}$. Then it follows from Theorem 14.6.35 that for all $\mathfrak{p} \in P(A)$:

$$\sum_{\mathfrak{P}|\mathfrak{p}} e_{\mathfrak{P}/\mathfrak{p}} f_{\mathfrak{P}/\mathfrak{p}} = n. \tag{2.6.1}$$

This being so, as $\mathfrak{D}(A)$ and $\mathfrak{D}(B)$ are free $\mathbb{Z}$-modules, we define an increasing homomorphism of ordered groups $N : \mathfrak{D}(B) \to \mathfrak{D}(A)$ (also denoted by $N_{B/A}$) by the condition:

$$N(\mathfrak{P}) = f_{\mathfrak{P}/\mathfrak{p}}\mathfrak{p} \quad \text{for } \mathfrak{P} \in P(B) \text{ and } \mathfrak{P}|\mathfrak{p}.$$

On the other hand we have defined an increasing homomorphism of ordered groups $i : \mathfrak{D}(A) \to \mathfrak{D}(B)$ (also denoted by $i_{B/A}$) by the condition:

$$i(\mathfrak{p}) = \sum_{\mathfrak{P}|\mathfrak{p}} e_{\mathfrak{P}/\mathfrak{p}}\mathfrak{P}$$

for $\mathfrak{p} \in P(A)$. Clearly for every family (D_i) (resp. (E_i)) of divisors of A (resp. B):

$$i(\sup_i D_i) = \sup_i i(D_i), \qquad i(\inf_i D_i) = \inf_i i(D_i), \tag{2.6.2}$$

$$N(\sup_i E_i) = \sup_i N(E_i), \qquad N(\inf_i E_i) = \inf_i N(E_i). \tag{2.6.3}$$

Also, the formula (2.6.1) implies $N \circ i = n \cdot 1_{\mathfrak{D}(A)}$.

Recall that in Proposition 15.1.37 we have proved that $i(\mathrm{div}_A(a)) = \mathrm{div}_B(a)$ for any $a \in A$. Now let $b \in B$ and consider $N(\mathrm{div}_B(b))$. We recall that the norm $N_{L/K}(b)$ of b is in A and, as $v_\mathfrak{P}$ and $v_\mathfrak{p}$ are normed, we have

$$(v_\mathfrak{P})|_K = e_{\mathfrak{P}/\mathfrak{p}} \cdot v_\mathfrak{p} \quad \text{for } \mathfrak{P}|\mathfrak{p}.$$

The formula in (6.4.2) then becomes

$$v_\mathfrak{p}(N_{L/K}(b)) = \sum_{\mathfrak{P}|\mathfrak{p}} f_{\mathfrak{P}/\mathfrak{p}}(b)$$

which implies $N(\mathrm{div}_B(b)) = \mathrm{div}_A(N_{L/K}(b))$. Therefore, by taking quotients, the homomorphisms N and i define homomorphisms which will also be denoted, by an abuse of language, by:

$$i : \mathfrak{C}(A) \to \mathfrak{C}(B), \quad N : \mathfrak{C}(B) \to \mathfrak{C}(A).$$

Proposition 15.2.46. *Let $A \subseteq B$ be Noetherian integrally closed domains and B a finitely generated A-module.*

(a) For E to be a pseudo-zero B-module, it is necessary and sufficient that the A-module $\mathrm{Rees}_A^B E$ be pseudo-zero.

(b) For E to be finitely generated torsion B-module, it is necessary and sufieient that $\mathrm{Rees}_A^B E$ be a finitely generated torsion A-module and in this case we have

$$\chi_A(\mathrm{Rees}_A^B E) = N(\chi_B(E)).$$

(c) *For E to be finitely generated B-module, it is necessary and suflicient that* $\mathrm{Rees}_A^B E$ *be a finitely generated A-module and in this case we have*

$$c_A(\mathrm{Rees}_A^B E) = N(c_B(E)) + \mathrm{rank}_B(E)c_A(B), \quad \mathrm{rank}_A(\mathrm{Rees}_A^B E) = n \cdot \mathrm{rank}_B(E).$$

Proof. As B is a finitely generated A-module, for E to be a finitely generated B-module, it is necessary and sufficient that $\mathrm{Rees}_A^B E$ be a finitely generated A-module. Moreover, if $\mathfrak{b}$ is the annihilator of E, $\mathfrak{b} \cap A = \mathfrak{a}$ is the annihilator of $\mathrm{Rees}_A^B E$. As B is integral over A, there is no ideal other than 0 lying over the ideal 0 of A and hence it amounts to the same to say that $\mathfrak{a} \neq 0$ or that $\mathfrak{b} \neq 0$.

By virtue of this last remark, we may confine our attention to the case where E is a torsion B-module. If $\mathfrak{b}$ is contained in a prime ideal $\mathfrak{P} \in P(B)$, $\mathfrak{a}$ is contained in $\mathfrak{P} \cap A = \mathfrak{p}$, which is of height 1. Conversely, if $\mathfrak{a}$ is contained in a prime ideal $\mathfrak{p} \in P(A)$, there exists a prime ideal $\mathfrak{P}$ of B which contains $\mathfrak{b}$ and lies over $\mathfrak{p}$. Assertion (a) follows from these remarks and Proposition 15.2.22.

For every finitely generated torsion B-module E, we write

$$\delta(E) = \chi_A(\mathrm{Rees}_A^B E).$$

clearly δ satisfies that conditions Proposition 15.2.33 (taking account of part (a)). There therefore exists a homomorphism $\theta : \mathfrak{D}(B) \to \mathfrak{D}(A)$ such that $\delta(E) = \theta(\chi_B(E))$ for every finitely generated torsion B-module E. The homomorphism θ is determined by its value for every B-module of the form $B/\mathfrak{P}$ where $\mathfrak{P} \in P(B)$, since $\chi_B(B/\mathfrak{P}) = \mathfrak{P}$. Now, for every prime ideal $\mathfrak{q} \neq \mathfrak{p} = \mathfrak{P} \cap A$ in $P(A)$, $\mathfrak{p} \not\subseteq \mathfrak{q}$ and hence $(B/\mathfrak{P})_\mathfrak{q} = 0$. On the other hand, $\mathfrak{P}B_\mathfrak{P}$ is a maximal ideal of $B_\mathfrak{P}$ and $(B/\mathfrak{P})_\mathfrak{p} = B_\mathfrak{P}/\mathfrak{P}B_\mathfrak{P}$ is isomorphic to the field of fractions of $B/\mathfrak{P}$, that is to the residue field of $v_\mathfrak{P}$. Its length as an $A_\mathfrak{p}$-module is therefore $f_{\mathfrak{P}/\mathfrak{p}}$, which proves that $\theta = N$, by the definition of χ_A.

If T is the torsion submodule of E, then $\mathrm{Rees}_A^B T$ is the torsion submodule of $\mathrm{Rees}_A^B E$ and $\mathrm{Rees}_A^B(E/T) = \mathrm{Rees}_A^B T/\mathrm{Rees}_A^B T$. To prove (c) we may therefore confine our attention to the case where E is torsion-free. Then E is identified with a sub-B-module of $\mathrm{Ind}_B^L E$ and contains a basis $e_1, \dots, e_m$ over L. If $b_1, \dots, b_s$ is a basis of L over K consisting ofelements of B, the $b_j e_i$ form a basis of $\mathrm{Ind}_B^L E$ over K consisting of elements of E, whence the second equality (c). On the other hand, let F be a free sub-B-module of E such that E/F is a torsion B-module; as $\mathrm{Rees}_A^B F$ is a direct sum of $\mathrm{rank}_B(E)$ A-modules isomorphic to B, by Proposition 15.2.41,

$$c_A(\mathrm{Rees}_A^B F) = \mathrm{rank}_B(E) \cdot c_A(B).$$

Moreover, by definiton of N and part (b), we have

$$c_A(\mathrm{Rees}_A^B(E/F)) = -c_A(N(\chi_B(E/F))) = -N(c_B(\chi_B(E/F))) = N(c_B(E))$$

Then it suffices to apply Proposition 15.2.41 to finish the proof. □

Proposition 15.2.47. *Let E be a finitely generated B-module. For E to be reflexive, it is necessary and suficient that* $\mathrm{Rees}_A^B E$ *be a reflexive A-module.*

Proof. We have remarked in the proof of Proposition 15.2.46 that for E to be a torsion-free

B-module, it is necessary and sufficient that $\mathrm{Rees}_A^B E$ be a torsion-free A-module. We may therefore assume that E is a lattice of $W = E \otimes_B L$ with respect to B. We shall use the following lemma:

Lemma 15.2.48. *Let W be a vector space of finite dimension over L and let E be a lattice of W with respect to B. Then, for all $\mathfrak{p} \in P(A)$, we have $(\mathrm{Rees}_A^B E)_{\mathfrak{p}} = \bigcap_{\mathfrak{P}|\mathfrak{p}} E_{\mathfrak{P}}$.*

If $S = A - \mathfrak{p}$, the prime ideals of the ring $S^{-1}B$ are generated by the prime ideals of B not meeting S, in other words the ideals $\mathfrak{P}_i$ lying over $\mathfrak{p}$ and the ideal (0). This shows that $S^{-1}B$ is a semi-local ring whose maximal ideals are the $\mathfrak{m}_i = S^{-1}\mathfrak{P}_i$ for $1 \leq i \leq m$. Moreover the local ring $(S^{-1}B)_{\mathfrak{m}_i}$ in is isomorphic to $B_{\mathfrak{P}_i}$ and hence is a discrete valuation ring. The ring $S^{-1}B$ is therefore a Dedekind domain and, as it is semi-local, it is a principal ideal domain. This being so, $(\mathrm{Rees}_A^B E)_{\mathfrak{p}}$ is equal to $S^{-1}E$ considered as an $A_{\mathfrak{p}}$-module; by the above, $S^{-1}E$ is a free lattice of W with respect to $S^{-1}B$ (hence reflexive) and Theorem 15.2.14 may therefore be applied to it, giving $S^{-1}E = \bigcap_i (S^{-1}E)_{\mathfrak{m}_i}$. But $(S^{-1}E)_{\mathfrak{m}_i} = E_{\mathfrak{P}_i}$, which proves the lemma.

Returning to the proof, by the above lemma we have

$$\bigcap_{\mathfrak{P} \in P(B)} E_{\mathfrak{P}} = \bigcap_{\mathfrak{p} \in P(A)} (\mathrm{Rees}_A^B E)_{\mathfrak{p}}.$$

and the conclusion follows from Theorem 15.2.14. □

Corollary 15.2.49. *The ring B is a reflexive A-module.*

Proposition 15.2.50. *Let $A \subseteq B$ be Noetherian integrally closed domains and B a finitely generated A-module.*

(a) For a finitely generated A-module M to be pseudo-Zero, it is necessary and sufficient that $M \otimes_A B$ be a pseudo-zero B-module.

(b) If M is a finitely generated torsion A-module, then $M \otimes_A B$ is a finitely generated B-module and

$$\chi_B(M \otimes_A B) = i(\chi_A(M)).$$

(c) If M is a finitely generated A-module, $M \otimes_A B$ is a finitely generated B-module

$$c_B(M \otimes_A B) = i(c_A(M)), \quad \mathrm{rank}_B(M \otimes_A B) = \mathrm{rank}_A(M).$$

Proof. Let $\mathfrak{P}$ be a prime ideal of B and $\mathfrak{p} = \mathfrak{P} \cap A$, then $(M \otimes_A B)_{\mathfrak{P}} = M \otimes_A B_{\mathfrak{P}}$, and on the other hand

$$M \otimes_A B_{\mathfrak{P}} = (M \otimes_A A_{\mathfrak{p}}) \otimes_{A_{\mathfrak{p}}} B_{\mathfrak{P}} = M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} B_{\mathfrak{P}}.$$

the relation $M_{\mathfrak{p}} = 0$ is therefore equivalent to $(M \otimes_A B)_{\mathfrak{P}} = 0$. It suffices to apply this remark to the ideal $\mathfrak{P} = (0)$ and the ideals $\mathfrak{P} \in P(B)$ to prove (a), taking account of the definition. To prove (b), we shall use the following lemma:

Lemma 15.2.51. *Let M_1, M_2 be two finitely generated A-modules, and $\phi : M_1 \to M_2$ an injective homomorphism. Then the kernel of $\phi \otimes 1 : M_1 \otimes_A B \to M_2 \otimes_A B$ is pseudo-zero.*

Let $\mathfrak{p}$ be a prime ideal of A of height ≤ 1. Then $(M_i \otimes_A B)_\mathfrak{p} = (M_i)_\mathfrak{p} \otimes_{A_\mathfrak{p}} B_\mathfrak{p}$ and $(\phi \otimes 1_B)_\mathfrak{p} = \phi_\mathfrak{p} \otimes 1_{B_\mathfrak{p}}$ the hypothesisthat ϕ is injective implies that so is $\phi_\mathfrak{p}$. On the other hand, in view of the choice of $\mathfrak{p}$, $A_\mathfrak{p}$ is a principal ideal domain and $B_\mathfrak{p}$ a finitely generated torsion-free $A_\mathfrak{p}$ -module and hence free; we conclude that $\phi_\mathfrak{p} \otimes 1_{B_\mathfrak{p}}$ is itself injective. If $I = \ker(\phi \otimes 1)$, then $I_\mathfrak{p} = \ker((\phi \otimes 1)_\mathfrak{p})$, therefore $I_\mathfrak{p} = 0$, whence a fortiori $I_\mathfrak{P} = (I_\mathfrak{p})_\mathfrak{P} = 0$ for $\mathfrak{P}|\mathfrak{p}$, which proves the lemma.

We return now to the proof of (b). For every finitely generated torsion Amodule M, write $\delta(M) = \chi_B(M \otimes_A B)$. It follows from (a) that, if M is pseudo-zero, then $\delta(M) = 0$. On the other hand, consider an exact sequence of finitely generated torsion A-modules:

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

It follows from the above lemma that there is an exact sequence of B-modules:

$$0 \longrightarrow I \longrightarrow M_1 \otimes_A B \longrightarrow M_2 \otimes_A B \longrightarrow M_3 \otimes_A B \longrightarrow 0$$

where I is pseudo-zero. Using the additivity of χ we therefore see δ is additive. We therefore conclude from Proposition 15.2.33 that there exists a homomorphism $\delta : \mathfrak{D}(A) \to \mathfrak{D}(B)$ such that $\delta(M) = \theta(\chi_A(M))$ for every finitely generated torsion A-module M. To prove that $\theta = i$, it suffices to show that $\delta(A/\mathfrak{p}) = i(\mathfrak{p})$ for all $\mathfrak{p} \in P(A)$. Now $(A/\mathfrak{p}) \otimes_A B = B/\mathfrak{p}B$ and, for all $\mathfrak{P} \in P(B)$, $(B/\mathfrak{p}B)_\mathfrak{P} = B_\mathfrak{P}/\mathfrak{p}B_\mathfrak{P}$. The last module is 0 if $\mathfrak{P}$ does not lie over $\mathfrak{p}$. If on the contrary $\mathfrak{P}|\mathfrak{p}$, then $B_\mathfrak{P}/\mathfrak{p}B_\mathfrak{P}$ is a $B_\mathfrak{P}$-module of length $e(\mathfrak{P}/\mathfrak{p})$ by definition of the ramification index. Therefore $\chi_B(B/\mathfrak{p}B) = \sum_{\mathfrak{P}|\mathfrak{p}} e_{\mathfrak{P}/\mathfrak{p}}\mathfrak{P} = i(\mathfrak{p})$, which proves (b).

The second formula in (c) is immediate, for

$$(M \otimes_A B) \otimes_B L = M \otimes_A L = M \otimes_A K \otimes_K L$$

and the rank of $(M \otimes_A K) \otimes_K L$ over L is equal to the rank of $M \otimes_A K$ over K. To show the first, consider a free submodule H of M such that $Q = M/H$ is a torsion A-module. Applying the lemma as above, we obtain an exact sequence of B-modules:

$$0 \longrightarrow I \longrightarrow H \otimes_A B \longrightarrow M \otimes_A B \longrightarrow Q \otimes_A B \longrightarrow 0$$

where I is pseudo-zero. It therefore follows from Proposition 15.2.41(a), (b) and (e) that

$$c_B(M \otimes_A B) = c_B(Q \otimes_A B) - c_B(\chi_B(Q \otimes_A B)) = -c_B(i(\chi_A(Q))) = -i(c_A(\chi_A(Q))) = i(c_A(M))$$

by virtue of (b), which completes the proof. □

15.2.7 Modules over Dedekind domains

We now assume that A is a Dedekind domain. Then we know that the ideals $\mathfrak{p} \in P(A)$ are maximal and that they are the only nonzero prime ideals of A. The group $\mathfrak{D}(A)$ is identified with the group $\mathfrak{F}(A)$ of fractional nonzero ideals of A.

Proposition 15.2.52. *Let A be a Dedekind domain. Every pseudo-zero A-module is zero. Every pseudo-infective (resp. pseudo-surjeetive, pseudo-bijective, pseudo-zero) A-module homomorphism is injective (resp. smjeetive, bijective, zero).*

Proof. The first assertion has already been shown; the others follow from it immediately. □

Proposition 15.2.53. *Let A be a Dedekind domain and M a finitely generated A-module. The following properties are equivalent:*

(a) M is torsion-free;

(b) M is reflexive;

(c) M is projective.

Proof. We already know (with no hypothesis on the integral domain A) that (ii) implies (i) and that (iii) implies (ii). If M is torsion-free, it is identified with a lattice of $V = M \otimes_A K$ with respect to A. $M_{\mathfrak{p}}$ is therefore a free $A_{\mathfrak{p}}$-module for every maximal ideal $\mathfrak{p} \in P(A)$, since $A_{\mathfrak{p}}$ is a principal ideal domain. The conclusion then follows from Theorem 10.5.4. □

Corollary 15.2.54. *Let M be a finitely generated A-module and let T be its torsion submodule. Then T is a direct factor of M.*

Proof. As M/T is torsion-free and finitely generated, it is projective by Proposition 15.2.53 and the corollary therefore follows. □

Proposition 15.2.55. *Let A be a Dedekind domain and T a finitely generated torsion A-module. There exist two finite families $(n_i)_{i\in I}$ and $(\mathfrak{p}_i)_{i\in I}$ where the n_i are positive integers and the $\mathfrak{p}_i$ are elements of $P(A)$, such that T is isomorphic to the direct sum $\bigoplus_{i\in I}(A/\mathfrak{p}_i^{n_i})$. Further, the families $(n_i)_{i\in I}$ and $(\mathfrak{p}_i)_{i\in I}$ are unique to within a bijection of the indexing set.*

Proof. This follows from Theorem 15.2.29 since a pseudo-isomorphism is here an isomorphism. □

Proposition 15.2.56. *Let A be a Dedekind domain and M a finitely generated torsion-free A-module of rank $n \geq 1$. Then there exists a nonzero ideal $\mathfrak{a}$ of A such that M is isomorphic to the direct sum of the modules A^{n-1} and $\mathfrak{a}$. Moreover, the class of the ideal $\mathfrak{a}$ is determined uniquely by this condition.*

Proof. **??** shows that there exists a free submodule L of M such that M/L is isomorphic to an ideal $\mathfrak{b}$ of A. If $\mathfrak{b} = 0$, we take $\mathfrak{a} = A$. Otherwise, $\mathfrak{b}$ is of rank 1, hence $L = A^{n-1}$ and $\mathfrak{b}$ is a projective module by Proposition 15.2.53. M is therefore isomorphic to the direct sum of L and $\mathfrak{b}$, which proves the first part of the proposition. Moreover, it follows from Proposition 15.2.41 that $c(M) = c(\mathfrak{a})$ whence the uniqueness of the class of $\mathfrak{a}$. □

Chapter 16

Dimension

16.1 Dimension of rings and modules

16.1.1 Dimension of a ring

Definition 16.1.1. *Let A be a ring. Then* ***dimension*** *of A, denoted by* $\dim(A)$*, is defined to be the Krull dimension of the topological space* $\operatorname{Spec}(A)$*. For a prime ideal $\mathfrak{p}$ of A, the dimension of A at $\mathfrak{p}$, denoted by* $\dim_{\mathfrak{p}}(A)$*, is defined to be* $\dim_{\mathfrak{p}}(\operatorname{Spec}(A))$*.*

Recall that the map $\mathfrak{p} \mapsto V(\mathfrak{p})$ is a bijection from prime ideals of A to irreducible closed subsets of $\operatorname{Spec}(A)$. The dimension of A is then the supremum of the length of chains of prime ideals of A. Since we do not consider the zero ring, $\dim(A)$ will always be a positive integer.

Let $\mathfrak{p} \in \operatorname{Spec}(A)$, the sets $D(f)$, where f runs through A, form a basis of the topology of $\operatorname{Spec}(A)$, and $\mathfrak{p}$ belongs to the open set $D(f)$ if and only if f does not belong to $\mathfrak{p}$. Therefore, $\dim_{\mathfrak{p}}(A)$ is the infimum of the numbers $\dim(A_f)$, where f runs through $A - \mathfrak{p}$ (Corollary 10.4.23).

Example 16.1.2 (Examples of dimension of rings).

(a) For $\dim(A) = 0$, it is necessary and sufficient that every prime ideal of A is maixmal. Thus a zero-dimensional integral domain is a field, and a zero-dimensional Noetherian ring is Artinian.

(b) A Dedekind domain is a Noetherian integrally closed domain of dimension one. More generally, a ring is a finite product of Dedekind's rings if and only if it is Noetherian, reduced, integrally closed in its total ring of fractions, and of dimension one.

(c) Let k be a field and A an k-algebra that is integral over k. Then since $\dim(k) = 0$ we have $\dim(A) = 0$.

(d) For a ring A we have
$$\dim(A[X]) \geq \dim(A) + 1.$$
In fact, if $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_n$ is a chain of prime ideals of A, then we have a chain $\mathfrak{P}_0 \subset \cdots \subset \mathfrak{P}_n \subset \mathfrak{P}_{n+1}$ of prime ideals of $A[X]$, where $\mathfrak{P}_i = \mathfrak{p}_i A[X]$ for $1 \leq i \leq n$ and $\mathfrak{P}_{n+1} = \mathfrak{p}_n A[X] + XA[X]$. By the same reasoning, we prove the inequality $\dim(A[\![X]\!]) \geq \dim(A) +$

1. We deduces by induction the inequalities

$$\dim(A[X_1, \dots, X_n]) \geq \dim(A) + n, \quad \dim(A[\![X_1, \dots, X_n]\!]) \geq \dim(A) + n.$$

Later we will see, the equality hold if A is Noetherian.

Proposition 16.1.3. *Let A be a ring.*

(a) For any ideal $\mathfrak{a}$ of A, we have $\dim(A/\mathfrak{a}) \leq \dim(A)$.

(b) Let S be a multiplicative subset of A, then $\dim(S^{-1}A) \leq \dim(A)$.

(c) We have $\dim(A) = \sup_{\mathfrak{p}} \dim(A/\mathfrak{p}) = \sup_{\mathfrak{m}} \dim(A_{\mathfrak{m}})$, where $\mathfrak{p}$ runs through minimal prime ideals of A and $\mathfrak{m}$ runs through maximal ideals of A.

(d) Assume that A has finitely many minimal prime ideals. Then for any prime ideal $\mathfrak{p}$ of A,

$$\dim_{\mathfrak{p}}(A) = \sup_{\mathfrak{q}} \dim_{\mathfrak{p}/\mathfrak{q}}(A/\mathfrak{q})$$

where $\mathfrak{q}$ runs through minimal prime ideals of A contained in $\mathfrak{p}$.

(e) Let $\mathfrak{a}$ be an ideal of A which is not contained in any minimal prime ideal of A. Then we have $\dim(A) \geq \dim(A/\mathfrak{a}) + 1$. In particular, if A is an integral domain, then $\dim(A) \geq \dim(A/\mathfrak{a}) + 1$ for any nonzero ideal $\mathfrak{a}$ of A.

Proof. By Proposition 10.4.20, $\operatorname{Spec}(A/\mathfrak{a})$ is homeomorphic to the subspace $V(\mathfrak{a})$ of $\operatorname{Spec}(A)$, and we get $\dim(A/\mathfrak{a}) \leq \dim(A)$ therefore. Similarly, part (b) follows from Corollary 10.4.23. Also, by Proposition 10.4.12, the irreducible components of $\operatorname{Spec}(A)$ are homeomorphic to $\operatorname{Spec}(A/\mathfrak{p})$, where $\mathfrak{p}$ are minimal prime ideals of A. This proves (c), and (d) follows from Corollary 4.2.5.

Finally, let $\mathfrak{a}$ be an ideal of A which is not contained in any minimal prime ideal of A. We prove that, for any chain $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_n$ of prime ideals of A such that $\mathfrak{a} \subseteq \mathfrak{p}_0$ we have $\dim(A) \geq n + 1$. By the hypothesis on $\mathfrak{a}$ we see $\mathfrak{p}_0$ is not minimal, so there exists a prime ideal $\mathfrak{p}_{-1}$ of A contained in $\mathfrak{p}_0$, distinct from $\mathfrak{p}_0$, and $\mathfrak{p}_{-1} \subset \mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_0$ is a chain of prime ideals of A, whence $\dim(A) \geq n + 1$. □

Corollary 16.1.4. *Let $\rho : A \to B$ be a ring homomorphism. Then $\dim(B)$ is the supremum of the numbers $\dim(B/\mathfrak{p}^e)$, where $\mathfrak{p}$ covers the set of minimal prime ideals of A.*

Proof. In fact, for each minimal prime ideal $\mathfrak{P}$ of B, there exists a minimal prime ideal $\mathfrak{p}$ of A contained in $\mathfrak{P}^c$, and therefore

$$\dim(B/\mathfrak{P}) \leq \dim(B/\mathfrak{p}^e) \leq \dim(B)$$

whence the claim by Proposition 16.1.3. □

For an ideal $\mathfrak{a}$ of A, we define the **height** (resp. **coheight**) $\operatorname{ht}(\mathfrak{a})$ (resp. $\operatorname{coht}(\mathfrak{a})$) of $\mathfrak{a}$ to be the codimension (resp. dimension) of $V(\mathfrak{a})$ in $\operatorname{Spec}(A)$. Also, the ring is called **catenary** if $\operatorname{Spec}(A)$ is catenary.

Proposition 16.1.5. *Let A be a ring.*

(a) *The height of a prime ideal* $\mathfrak{p}$ *is the supremum of the length of chains* $\mathfrak{p}_0 \subseteq \cdots \subseteq \mathfrak{p}_n$ *of prime ideals of* A *such that* $\mathfrak{p}_n = \mathfrak{p}$.

(b) *Let* $\mathfrak{p}$ *be a prime ideal of* A *and* $\mathfrak{a}$ *an ideal of* A. *Then* $\dim(A_\mathfrak{p}/\mathfrak{a}A_\mathfrak{p}) = -\infty$ *if* $\mathfrak{a}$ *is not contained in* $\mathfrak{p}$, *and* $\dim(A_\mathfrak{p}/\mathfrak{a}A_\mathfrak{p}) = \operatorname{codim}(V(\mathfrak{p}), V(\mathfrak{a}))$ *if* $\mathfrak{a}$ *is contained in* $\mathfrak{p}$. *In particular, for a prime ideal* $\mathfrak{p}$ *of* A, *we have* $\dim(A_\mathfrak{p}) = \operatorname{ht}(\mathfrak{p})$.

(c) *For any ideal* $\mathfrak{a}$ *of* A, *we have* $\operatorname{ht}(\mathfrak{a}) = \inf_{\mathfrak{p}\supseteq\mathfrak{a}} \operatorname{ht}(\mathfrak{p}) = \inf_{\mathfrak{p}\supseteq\mathfrak{a}} \dim(A_\mathfrak{p})$.

Proof. Part (a) follows from definition, and part follows from the fact that the map $\mathfrak{q} \mapsto \mathfrak{q}(A_\mathfrak{p}/\mathfrak{a}A_\mathfrak{p})$ is an increasing isomorphism of the set of prime ideals $\mathfrak{q}$ of A such that $\mathfrak{a} \subseteq \mathfrak{q} \subseteq \mathfrak{p}$ on the set of prime ideals of the local ring $A_\mathfrak{p}/\mathfrak{a}A_\mathfrak{p}$. Now let $\mathfrak{a}$ be an ideal of A. Then the irreducible closed subset of $V(\mathfrak{a})$ are the sets $V(\mathfrak{p})$, where $\mathfrak{p}$ is a prime ideal of A containing $\mathfrak{a}$. Part (c) then follows from the definition of codimension. □

Corollary 16.1.6. *Let* $\mathfrak{p}$ *be a prime ideal of* A *and* S *a multiplicative subset of* A *not meeting* $\mathfrak{p}$. *Then* $\operatorname{ht}(\mathfrak{p}) = \operatorname{ht}(S^{-1}\mathfrak{p})$.

Proof. This follows from Proposition 10.2.36. □

Proposition 16.1.7. *Let* A *be a ring. Let* $\mathfrak{a}, \mathfrak{b}$ *be proper ideals of* A *such that* $\mathfrak{a} \subseteq \mathfrak{b}$. *Then*

$$\operatorname{codim}(V(\mathfrak{b})), V(\mathfrak{a})) \leq \dim(A/\mathfrak{a}) - \dim(A/\mathfrak{b})$$

In particular, for any ideal $\mathfrak{a}$ *of* A, *we have* $\operatorname{ht}(\mathfrak{a}) + \dim(A/\mathfrak{a}) \leq \dim(A)$.

Proof. This from Proposition 4.2.9 and of the relations $\dim(A/\mathfrak{a}) = \dim(V(\mathfrak{a}))$, $\dim(A/\mathfrak{b}) = \dim(V(\mathfrak{b}))$. □

Proposition 16.1.8. *Let* A *be a ring.*

(a) *For* A *to be catenary, it is necessary and sufficient that, for every triple* $(\mathfrak{p}, \mathfrak{q}, \mathfrak{r})$ *of prime ideals of* A *such that* $\mathfrak{r} \subseteq \mathfrak{q} \subseteq \mathfrak{p}$, *we have*

$$\dim(A_\mathfrak{p}/\mathfrak{q}A_\mathfrak{p}) + \dim(A_\mathfrak{q}/\mathfrak{r}A_\mathfrak{q}) = \dim(A_\mathfrak{p}/\mathfrak{r}A_\mathfrak{p}).$$

(b) *If* A *is an integral domain with finite dimension, then for* A *to be catenary, it is necessary and sufficient that, for every pair* $(\mathfrak{p}, \mathfrak{q})$ *of prime ideals of* A *such that* $\subseteq \mathfrak{q} \subseteq \mathfrak{p}$, *we have*

$$\operatorname{ht}(\mathfrak{q}) + \dim(A_\mathfrak{p}/\mathfrak{q}A_\mathfrak{p}) = \operatorname{ht}(\mathfrak{p}).$$

Proof. This follows directly from Proposition 4.2.11 and Corollary 4.2.12. □

Proposition 16.1.9. *Let* A *be a ring of finite dimension such that all maximal chains of prime ideals have the same length. Then* A *is catenary, and for any prime ideal* $\mathfrak{p}$ *of* A *we have*

$$\operatorname{ht}(\mathfrak{p}) = \dim(A) - \operatorname{coht}(\mathfrak{p}).$$

Moreover, for any pair $(\mathfrak{p}, \mathfrak{q})$ *of prime ideals such that* $\mathfrak{q} \subseteq \mathfrak{p}$, *we have*

$$\dim(A_\mathfrak{p}/\mathfrak{q}A_\mathfrak{p}) = \operatorname{coht}(\mathfrak{q}) - \operatorname{coht}(\mathfrak{p}).$$

Proof. This is a reformulation of Proposition 4.2.13. □

16.1.2 Dimension of a finitely generated module

Let A be a finitely generated A-module. The **dimension** (resp. **codimension**) of M, denoted by $\dim_A(M)$ (resp. $\operatorname{codim}(M)$), is defined to be the dimension (resp. codimension) of the support of M.

The support of the A-module A is $\operatorname{Spec}(A)$, so the dimension of the A-module A equals the dimension of the ring A. Also, since M is finitely generated,

$$\operatorname{supp}(M) = V(\mathfrak{a}) = \operatorname{supp}(A/\mathfrak{a})$$

where $\mathfrak{a}$ is the annihilator of M. Consequently, the dimension of the A-mqdule M, the dimension of the A-module $A/\mathfrak{a}$, the dimension of the ring $A/\mathfrak{a}$ and the dimension of the $(A/\mathfrak{a})$-module M are all the supremum of the set of lengths of the chains $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_n$ of prime ideals of A such that $\mathfrak{a} \subseteq \mathfrak{p}_0$. By Proposition 16.1.3(c), the dimension of M is also the supremum of the dimensions of the rings (or of the A-modules) $A/\mathfrak{p}$, where $\mathfrak{p}$ runs through the set of prime ideals of A, minimal among those which contain $\mathfrak{a}$.

Example 16.1.10. If A is Noetherian, then by Proposition 12.2.14, we see $\dim_A(M) = 0$ if and only $\operatorname{supp}(M)$ consists of maximal ideals, or equivalently M is of finite length.

Example 16.1.11. If M is a finitely generated module over a Noetherian ring A, $\dim_A(M)$ is then the supremum of the numbers $\dim(A/\mathfrak{p})$, where $\mathfrak{p}$ runs through the set $\operatorname{Ass}_A(M)$ of prime ideals of A associated with M (Proposition 12.1.14).

Proposition 16.1.12. *Let A be a ring and M a finitely generated A-module.*

(a) For each $\mathfrak{p} \in \operatorname{supp}(M)$, we have $\dim_{A_\mathfrak{p}}(M_\mathfrak{p}) = \operatorname{codim}(V(\mathfrak{p}), \operatorname{supp}(M))$.

(b) We have $\dim_A(M) = \sup_\mathfrak{p} \dim_{A_\mathfrak{p}}(M_\mathfrak{p})$, where $\mathfrak{p}$ runs through prime ideals in $\operatorname{supp}(M)$ (resp. maximal ideal in $\operatorname{supp}(M)$).

(c) Let $0 \to M' \to M \to M'' \to 0$ be an exact sequence of finitely generated A-modules. Then $\dim_A(M) = \sup\{\dim_A(M'), \dim_A(M'')\}$.

Proof. Let $\mathfrak{a}$ be the annihilator of M, then the annihilator of $M_\mathfrak{p}$ is $\mathfrak{a}A_\mathfrak{p}$, whence $\dim_{A_\mathfrak{p}}(M_\mathfrak{p}) = \dim(A_\mathfrak{p}/\mathfrak{a}A_\mathfrak{p})$, and the claim follows from Proposition 16.1.5 and $\operatorname{supp}(M) = V(\mathfrak{a})$. Also, part (b) follows from (a), and (c) follows from Proposition 10.4.31. □

16.1.3 Cycle associated with a module

In this part, let A be a Noetherian ring. Let $Z(A)$ be the free $\mathbb{Z}$-module generated by the set of closed irreducible subsets of $\operatorname{Spec}(A)$. For any irreducible closed subset Y of $\operatorname{Spec}(A)$, we denote by $[Y]$ the element correspondent of $Z(A)$. The elements of $Z(A)$ are sometimes called **cycles**. Let M be a finitely generated A-module. For any prime ideal $\mathfrak{p}$ of A which is a minimal element of $\operatorname{supp}(M)$, we have $0 < \ell_{A_\mathfrak{p}}(M_\mathfrak{p}) < +\infty$ by Corollary 12.2.16. We set

$$z(M) = \sum_\mathfrak{p} \ell_{A_\mathfrak{p}}(M_\mathfrak{p}) \cdot [V(\mathfrak{p})]$$

where $\mathfrak{p}$ runs through the finite set of minimal element of $\mathrm{supp}(M)$.

Example 16.1.13. For any $\mathfrak{p} \in \mathrm{Spec}(A)$, we have $z(A/\mathfrak{p}) = [V(\mathfrak{p})]$. More generally, let M be a finitely generated A-module, and let $(M_i)_{1\leq i\leq n}$ be a chain of M such that for each i, the modulus M_i/M_{i+1} is isomorphic to $A/\mathfrak{p}_i$, where $\mathfrak{p}_i$ is a prime ideal of A. Then we have $z(M) = \sum_{i\in J} \ell_i[V(\mathfrak{p}_i)]$, where J is the subset of I consists of i such that $\mathfrak{p}_i$ be a minimal element of $\{\mathfrak{p}_0, \dots, \mathfrak{p}_{n-1}\}$, and ℓ_i is the number of indices j such that $\mathfrak{p}_j = \mathfrak{p}_i$.

For any integer d, let $Z_{\leq d}$ (resp. Z_d, resp. $Z^{\geq d}$, resp. Z^d) be the $\mathbb{Z}$-submodule of $Z(A)$ generated by the elements $[V(\mathfrak{p})]$ where $\mathfrak{p}$ is a prime ideal of A such that $\mathrm{coht}(\mathfrak{p}) \leq d$ (resp. $\mathrm{coht}(\mathfrak{p}) = d$, resp. $\mathrm{ht}(\mathfrak{p}) \geq d$, resp. $\mathrm{ht}(\mathfrak{p}) = d$). An element of Z_d (resp. Z^d) is called a **cycle** of dimension d (resp. codimension d). We have

$$Z_{\leq d} = Z_{\leq d-1} \oplus Z_d, \quad Z^{\geq d} = Z^{\geq d-1} \oplus Z^d.$$

Let C be the set of classes of finitely generated A-modules, and for each integer d, let $C_{\leq d}$ (resp. $C^{\geq d}$) be the subgroup generated by finitely generated A-modules of dimension $\leq d$ (resp. of codimension $\geq d$).

Lemma 16.1.14. *Let M be a finitely generated A-module.*

(a) For M be in $C_{\leq d}$, it is necessary and sufficient that $z(M) \in Z_{\leq d}$. In this case, the projection $z_d(M)$ of $z(M)$ on Z_d parallel to $Z_{\leq d-1}$ is given by

$$z_d(M) = \sum_{\mathrm{coht}(\mathfrak{p})=d} \ell_{A_\mathfrak{p}}(M_\mathfrak{p}) \cdot [V(\mathfrak{p})].$$

(b) For M be in $C^{\geq d}$, it is necessary and sufficient that $z(M) \in Z^{\geq d}$. In this case, the projection $z^d(M)$ of $z(M)$ on Z^d parallel to $Z^{\geq d-1}$ is given by

$$z^d(M) = \sum_{\mathrm{ht}(\mathfrak{p})=d} \ell_{A_\mathfrak{p}}(M_\mathfrak{p}) \cdot [V(\mathfrak{p})].$$

Proof. For M to be dimension $\leq d$, it is necessary and sufficient that for any minimal prime $\mathfrak{p}$ of $\mathrm{supp}(M)$, we have $\mathrm{coht}(\mathfrak{p}) \leq d$, which means $z(M) \in Z_{\leq d}$. Suppose now $\dim(M) \leq d$, and let $\mathfrak{p} \in \mathrm{Spec}(A)$ be such that $\mathrm{coht}(\mathfrak{p}) = d$. Then, either $\mathfrak{p} \notin \mathrm{supp}(M)$ and $M_\mathfrak{p} = 0$, or $\mathfrak{p} \in \mathrm{supp}(M)$ and $\mathfrak{p}$ is a minimal element of $\mathrm{supp}(M)$. The coefficient of $[V(\mathfrak{p})]$ in $z(M)$ is in both cases $\ell_{A_\mathfrak{p}}(M_\mathfrak{p})$, whence (a). Part (b) is proved analogously, noting that a finitely generated module M is in $C^{\geq d}$ if and only if we have $M_\mathfrak{p} = 0$ for any prime ideal $\mathfrak{p}$ of height $< d$. □

By Proposition 10.4.31, the sets $C_{\leq d}$ and $C^{\geq d}$ are hereditary, and we can consider the corresponding Grothendieck groups $K(C_{\leq d})$ and $K(C^{\geq d})$, which are subgroups of $K(C)$, the Grothendieck group of finitely generated A-modules. By Lemma 16.1.14, the functions z_d and z^d are additive, whence extends to homomorphisms

$$\zeta_d : K(C_{\leq d}) \to Z_d, \quad \zeta^d : K(C^{\geq d}) \to Z^d$$

Moreover, since $C_{\leq d-1} \subseteq C_{\leq d}$ and $C^{\geq d+1} \subseteq C^{\geq d}$, we have canonical homomorphisms

$$i_d : K(C_{\leq d-1}) \to K(C_{\leq d}), \quad i^d : K(C^{\geq d+1}) \to K(C^{\geq d}).$$

Proposition 16.1.15. *The following sequence of $\mathbb{Z}$-modules*

$$K(C_{\leq d-1}) \xrightarrow{i_d} K(C_{\leq d}) \xrightarrow{\zeta_d} Z_d \longrightarrow 0$$

$$K(C^{\geq d+1}) \xrightarrow{i^d} K(C^{\geq d}) \xrightarrow{\zeta^d} Z^d \longrightarrow 0$$

are exact.

Proof. We have $\zeta_d \circ i_d = 0$ by Lemma 16.1.14. For every $\mathfrak{p} \in \operatorname{Spec}(A)$ such that $\operatorname{coht}(\mathfrak{p}) = d$, we see $\zeta_d([A/\mathfrak{p}]) = z_d(Z/\mathfrak{p}) = [V(\mathfrak{p})]$, so the homomorphism ζ_d is surjective. Now by Proposition 12.1.17, $K(C_{\leq d})$ is generated by the elements $[A/\mathfrak{p}]$, where $p \in \operatorname{Spec}(A)$ and $\operatorname{coht}(\mathfrak{p}) \leq d$. Therefore, every element ξ can be written into $\xi = i_d(\eta) + \sum_{i=1}^k n_i[A/\mathfrak{p}_i]$, where $\eta \in K(C_{\leq d-1})$, $n_i \in \mathbb{Z}$ and $\operatorname{coht}(\mathfrak{p}_i) = d$ for each i. From this, we see $\zeta_d(\xi) = \sum_{i=1}^k n_i[V(\mathfrak{p}_i)]$, and $\zeta_d(\xi) = 0$ if and only if $\xi \in \operatorname{im} i_d$, which proves the claim. The proof for i^d and ζ^d can be done similarly. □

Example 16.1.16. Let A be a Noetherian integral domain. Then $Z^0 = \mathbb{Z}\operatorname{Spec}(A)$ and $z^0(M) = \operatorname{rank}(M) \cdot \operatorname{Spec}(A)$. Therefore the modules in $C^{\geq 1}$ are the torsion modules.

Example 16.1.17. Assume that A is Noetherian and integrally closed. Then Z^1 is identified with the group $\mathfrak{D}(A)$ of divisors of A. The modules in $C^{\geq 2}$ are therefore pseudo-zero modules (Proposition 15.2.22). If M is a finitely generated torsion module, then $z^1(M) \in Z^1\mathfrak{D}(A)$ is the content $\chi(M)$ of M. Proposition 15.2.31 and Proposition 15.2.33 is then equivalent to the exactness of the sequence $K(C^{\geq 2}) \longrightarrow K(C^{\geq 1}) \longrightarrow Z^1 \longrightarrow 0$.

Example 16.1.18. The elements in C_0 are finitely generated A-modules of dimension 0, that is, of finite length. Let $\epsilon : Z_0 \to \mathbb{Z}$ be the evaluation map, then $\ell_A(M) = \epsilon(z_0(M))$, in view of Corollary 12.2.18.

Example 16.1.19. Let A be a integral domain of finite dimension. Let $d = \dim(A)$, then $C_{\leq d} = C$ and $Z_d = \mathbb{Z}\operatorname{Spec}(A)$. Also, we have $z_d(M) = \operatorname{rank}(M)\operatorname{Spec}(A) = z^0(M)$, whence the modules in $C_{\leq d-1}$ are precisely the torsion A-modules.

16.1.4 Exercise

Exercise 16.1.1. In this exercise, we develop a way to measure the complexity of a partially ordered set.

(a) Prove that, for any partially ordered set E we can associate an element of $\mathbb{N} \cup \{\pm\infty\}$, denoted by $\operatorname{dev}(E)$, and called the **deviation** of E, which satisfies the following conditions:

  (α) A trivial poset (one in which no two elements are comparable) has deviation $-\infty$.

  (β) A poset E is said to have deviation at most n (for a positive integer n) if for every descending chain of elements $(a_k)_{k\in\mathbb{N}}$, all but a finite number of the posets (a_k, a_{k+1}) have deviation less than n. The deviation of E (if it exists) is the minimum value of α for which this is true.

(b) Show that for $\operatorname{dev}(E) \leq 0$, it is necessary and sufficient that any decreasing sequence of E is stationary. We have $\operatorname{dev}(\mathbb{N}) = 0$, $\operatorname{dev}(\mathbb{Z}) = 1$, $\operatorname{dev}(\mathbb{Q}) = +\infty$.

(c) Let E and F be partially ordered sets. Show that if there exists an increasing map from E to F, then $\operatorname{dev}(E) \leq \operatorname{dev}(F)$. Show that $\operatorname{dev}(E \times F) = \sup\{\operatorname{dev}(E), \operatorname{dev}(F)\}$.

Exercise 16.1.2. Let A be a ring (not necessarily commutative), M a left A-module, we denote by $\operatorname{dev}(M)$ the deviation of the set of submodules of M, orederd by inclusion. We put $\operatorname{dev}(A)$ to be the deviation of the left A-module A.

(a) If N is a sub-A-module of M, then

$$\operatorname{dev}(M) = \sup\{\operatorname{dev}(N), \operatorname{dev}(M/N)\}.$$

(b) Suppose that A is commutative. If $\mathfrak{p}$ and $\mathfrak{q}$ are distinct prime ideals of A and $\mathfrak{p} \subseteq \mathfrak{q}$, then $\operatorname{dev}(A/\mathfrak{p}) > \operatorname{dev}(A/\mathfrak{q})$. In particular, $\dim(A) \leq \operatorname{dev}(A)$.

(c) Suppose that A is commutative and Noetherian. Let $\mathscr{P}_A$ be the set of prime ideals of A such that $\dim(A/\mathfrak{p}) = \dim(A)$ and S be complement of the union of prime ideals in $\mathscr{P}_A$. Let M be a finitely generated A-module. If $S^{-1}M = 0$ then

$$\operatorname{dev}(M) \leq \sup_{\mathfrak{p} \notin \mathscr{P}_A} \operatorname{dev}(A/\mathfrak{p}).$$

(d) Suppose that A is commutative and Noetherian. Prove that $\dim(A) = \operatorname{dev}(A)$ and $\dim(M) = \operatorname{dev}(M)$ for any finitely generated A-module M.

Proof. For a module E, we let $\mathcal{L}(E)$ denote the lattice of submodules of E. Then if N is a submodule of M, there are ordered homomorphisms $\mathcal{L}(N) \to \mathcal{L}(M)$ and $\mathcal{L}(M/N) \to \mathcal{L}(M)$, whence

$$\operatorname{dev}(M) \geq \sup\{\operatorname{dev}(N), \operatorname{dev}(M/N)\}.$$

On the other hand, we have an ordered homomorphism

$$\mathcal{L}(M) \to \mathcal{L}(N) \times \mathcal{L}(M/N), \quad M' \mapsto (M' \cap N, M' + N/N).$$

This proves the equality in (a).

Suppose that A is commutative and let $\mathfrak{p} \subseteq \mathfrak{q}$ be distinct prime ideals. By replacing A with $A/\mathfrak{p}$, we may assume that $\mathfrak{p} = 0$. For any nonzero element $x \in \mathfrak{q}$, consider the sequence $(x^n A)$ in A. We have

$$\operatorname{dev}(A) > \operatorname{dev}(x^n A/x^{n+1}A) = \operatorname{dev}(A/xA) \geq \operatorname{dev}(A/\mathfrak{q})$$

so the claim in (b) follows. Now let $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_n$ be a saturated chain in A. Then $\operatorname{dev}(A/\mathfrak{p}_0) > \cdots > \operatorname{dev}(A/\mathfrak{p}_n)$, which shows $\operatorname{dev}(A) \geq n = \dim(A)$.

Suppose that A is Noetherian and let M be a finitely generated A-module. Then there is a composition series $(M_i)_{0 \leq i \leq n}$ of M such that M/M_{i+1} is isomomorphic to $A/\mathfrak{p}_i$. If $S^{-1}M = 0$, we have $\mathfrak{p}_i \notin \mathscr{P}_A$ for all i. Since $\operatorname{dev}(M) = \sup_i \operatorname{dev}(M_i/M_{i+1})$, we conclude that

$$\operatorname{dev}(M) \leq \sup_{\mathfrak{p} \notin \mathscr{P}_A} \operatorname{dev}(A/\mathfrak{p}).$$

Finally, we show that $\operatorname{dev}(A) = \dim(A)$ by induction on $\dim(A)$. So assume that $\operatorname{dev}(B) = \dim(B)$ for every Noetherian commutative B such that $\dim(B) < \dim(A)$. Then in the notation

of (c), since $\dim(A/\mathfrak{p}) < \dim(A)$, we have $\operatorname{dev}(A/\mathfrak{p}) = \dim(A/\mathfrak{p})$ for $\mathfrak{p} \notin \mathscr{P}_A$, whence

$$\operatorname{dev}(M) \leq \sup_{\mathfrak{p} \in \mathscr{P}_A} \dim(A/\mathfrak{p}) < \dim(A) \tag{1.4.1}$$

if M is finitely generated and $S^{-1}M = 0$. Now let $(\mathfrak{a}_k)$ be a sequence of decreasing ideals in A. Since $S^{-1}A$ is Artinian (it has dimension zero), there exists an integer N such that

$$S^{-1}\mathfrak{a}_n = S^{-1}\mathfrak{a}_{n+1} = \cdots$$

for $n \geq N$. In other words, $S^{-1}(\mathfrak{a}_n/\mathfrak{a}_{n+1}) = 0$ for $n \geq N$, so by (16.1.2) we have $\operatorname{dev}(\mathfrak{a}_n/\mathfrak{a}_{n+1}) < \dim(A)$ for $n \geq N$. From the definition of $\operatorname{dev}(A)$, this shows $\operatorname{dev}(A) \leq \dim(A)$, which gives $\operatorname{dev}(A) = \dim(A)$.

Now let M be a finitely generated A-module and let $(M_i)_{0 \leq i \leq n}$ be the composition series of M such that $M_i/M_{i+1} \cong A/\mathfrak{p}_i$, where $\mathfrak{p}_i$ is a prime ideal of M. Then

$$\operatorname{dev}(M) = \sup_i\{\operatorname{dev}(M_i/M_{i+1})\} = \sup_i\{\operatorname{dev}(A/\mathfrak{p}_i)\} = \sup_i\{\dim(A/\mathfrak{p}_i)\}.$$

We also note that, since the minimal elements in $\{\mathfrak{p}_0, \ldots, \mathfrak{p}_{n-1}\}$ are the embedded primes for M, which correspond to irreducible components of $\mathfrak{a} = \operatorname{Ann}(M)$. Since $\dim(M) = \dim(V(\mathfrak{a}))$ is the supremum of the dimension of these components, we conclude that $\operatorname{dev}(M) = \dim(M)$. □

Exercise 16.1.3. Let A be a Noetherian commutative ring, $\mathfrak{a}$ an ideal of A contained in the Jacobson radical of A, and $\operatorname{gr}(A)$ the graded ring associated with the $\mathfrak{a}$-adic filtration. Associate to each ideal of A an ideal of $\operatorname{gr}(A)$, and deduce that $\operatorname{dev}(A) \leq \operatorname{dev}(\operatorname{gr}(A))$. Concequently, deduce that $\dim(A) \leq \dim(\operatorname{gr}(A))$.

Exercise 16.1.4. Let A be a ring such that

(a) For every maximal ideal $\mathfrak{m}$ of A, $A_\mathfrak{m}$ is Noetherian.

(b) Every nonzero element $x \in A$ is contained in a finite number of maximal ideals of A.

Show that A is Noetherian.

Proof. Let $(\mathfrak{a}_n)$ be an increasing sequence of ideals in A, and assume that $\mathfrak{a}_1 \neq 0$. Then by condition (b), the ideal $\mathfrak{a}_1$ is contained in finitely many maximal ideals, say $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$. Since each ring $A_{\mathfrak{m}_i}$ is Noetherian, there exists an integer N such that

$$\mathfrak{a}_n A_{\mathfrak{m}_i} = \mathfrak{a}_{n+1} A_{\mathfrak{m}_i} = \cdots$$

for $n \geq N$ and $i = 1, \ldots, r$. But if $\mathfrak{m}$ is a maximal ideal other than $\mathfrak{m}_i$, then $\mathfrak{a}_n \not\subseteq \mathfrak{m}$ for all n, so

$$\mathfrak{a}_n A_\mathfrak{m} = \mathfrak{a}_{n+1} A_\mathfrak{m} = \cdots = A_\mathfrak{m}$$

trivially holds. By Corollary 10.3.21, we conclude that $\mathfrak{a}_n = \mathfrak{a}_{n+1} = \cdots$ for $n \geq N$, so A is Noetherian. □

Exercise 16.1.5. Let K be a field, $(n_i)_{i \geq 1}$ a strict increasing sequence of positive integers; for each $i \geq 0$, put $\mathfrak{p}_i$ to be the ideal of the ring $R = K[(X_j)_{j \in \mathbb{N}}]$ generated by the elements X_j where

$n_1 + \cdots + n_i \leq j < n_1 + \cdots + n_{i+1}$. Let S be the complement of the union of the $\mathfrak{p}_i$'s, and consider the ring $A = S^{-1}R$. Prove that $S^{-1}R$ is Noetherian but has infinite dimension.

Proof. We first note that an nonzero element in $S^{-1}R$ can only be contained in finitely many $S^{-1}\mathfrak{p}_i$ (since this is true in R for $\mathfrak{p}_i$). Since the ideals of $S^{-1}A$ correspond to ideals of R contained in $\bigcup_i \mathfrak{p}_i$, and any such ideal can only be contained in finitely many $\mathfrak{p}_i$, by prime avoidence we conclude that the $S^{-1}\mathfrak{p}_i$ are the only maximal ideals in $S^{-1}R$. Moreover, for each $S^{-1}\mathfrak{p}_i$, $(S^{-1}R)_{S^{-1}\mathfrak{p}_i}$ is isomomorphic to $R_{\mathfrak{p}_i}$, which is Noetherian since it is just $K(x_J)[x_I]_{(x_I)}$ where I is indices appears in the generators of $\mathfrak{p}_i$ and J its complement. By Exercise 16.1.4, we conclude that $S^{-1}R$ is Noetherian. Now it is easy to see each maximal ideal $S^{-1}\mathfrak{p}_i$ has height $\geq n_i$ in $S^{-1}R$, so $S^{-1}R$ has infinite dimension. □

Exercise 16.1.6. Let A be the ring of germs at 0 of smooth functions on $\mathbb{R}$. We propose to show that the ring A is of infinite dimension. We denote by C the algebra of smooth functions on $\mathbb{R}$, F the ideal of functions zero on a neighborhood of 0, so that $A = C/F$.

(a) Let $(x_n)_{n\in\mathbb{N}}$ be a strict decreasing sequence of positive numbers tending to 0, and let $\mathcal{U}$ be an ultrafilter on $\mathbb{N}$ finer than the filter of complements of finite subsets. Show that the set J_1 of $f \in C$ such that the set of $n \in \mathbb{N}$ such that $f(x_n) = 0$ belongs to $\mathcal{U}$, is a prime ideal of C.

(b) We denote by $\tau_n(f)$ the function $x \mapsto f(x + x_n)$. Show that if J is a prime ideal of C, the set $\varphi(J)$ of $f \in C$ such that the set of $n \in \mathbb{N}$ where $\tau_n(f) \in J$ belongs to $\mathcal{U}$ is a prime ideal of C.

(c) We define a sequence I_n of ideals of C by $I_0 = J_1$ and $I_{n+1} = \varphi(I_n)$. Show that $(I_n)_{n\in\mathbb{N}}$ is a strict decreasing sequence of prime ideals of C containing F.

Proof. Let (x_n) and $\mathcal{U}$ be as in (a), and define J_1 by

$$J_1 = \{f \in C : \{n \in \mathbb{N} : f(x_n) = 0\} \in \mathcal{U}\}.$$

Now let $f, g \in C$ and assume that $fg \in J_1$; put

$$E_f = \{n \in \mathbb{N} : f(x_n) = 0\}, \quad E_g = \{n \in \mathbb{N} : g(x_n) = 0\}.$$

Then by definition, the set $E_{fg} = \{n \in \mathbb{N} : f(x_n)g(x_n) = 0\}$ belongs to $\mathcal{U}$. Assume that $E_f, E_g \notin \mathcal{U}$, then since $\mathcal{U}$ is a ultrafilter, we have $E_f^c, E_g^c \in \mathcal{U}$. But then

$$E_f^c \cap E_g^c = \{n \in \mathbb{N} : f(x_n) \neq 0, g(x_n) \neq 0\} = \{n \in \mathbb{N} : f(x_n)g(x_n) \neq 0\} = E_{fg}^c \in \mathcal{U}$$

which is a contradiction since $E_{fg} \in \mathcal{U}$. This proves that either of E_f and E_g is in $\mathcal{U}$, so J_1 is a prime ideal.

Now for a prime ideal J of C, define $\varphi(J)$ by

$$\varphi(J) = \{f \in C : \{n \in \mathbb{N} : \tau_n(f) \in J\} \in \mathcal{U}\}.$$

Again, for an element $f \in C$ we put $E_f(J) = \{n \in \mathbb{N} : \tau_n(f) \in J\}$. By noting that, since J is a

prime ideal,

$$E_f(J)^c \cap E_g(J)^c = \{n \in \mathbb{N} : \tau_n(f) \notin J, \tau_n(g) \notin J\} = \{n \in \mathbb{N} : \tau_n(f)\tau_n(g) \notin J\} = E_{fg}(J)^c,$$

it is easy to show that $\varphi(J)$ is a prime ideal, just as in (a).

Define the sequence (I_n) by $I_0 = J_1$ and $I_{n+1} = \varphi(I_n)$. To prove the first assertion in (c), we first note that, since $\mathcal{U}$ is finer than the finite complement filter on $\mathbb{N}$, every element in $\mathcal{U}$ is infinite (otherwise its complement belongs to $\mathcal{U}$). Let $f \in F$, then there exists a neighborhood U of 0 such that $f|_U = 0$. Then since $x_n \to 0$, there exists an integer N such that $x_n \in U$ when $n \geq N$, whence $f(x_n) = 0$ for $n \geq N$. Since $\mathcal{U}$ is finer than the finite complement filter on $\mathbb{N}$, this means $E_f = \{n \in \mathbb{N} : f(x_n) = 0\} \in \mathcal{U}$, so $f \in J_1$. This shows $F \subseteq J_1 = I_0$. Now let J be a prime ideal of C containing F, and consider $\varphi(J)$. Let $f \in F$, and let U be a neighborhood of 0 such that $f|_U \equiv 0$. Then since x_n is strict decreasing and tend to 0, there exists $N > 0$ such that $(x_n + U) \cap U$ contains a neighborhood of 0 for $n \geq N$, whence $\tau_n(f) \in F \subseteq J$ for $n \geq N$. This shows $f \in \varphi(J)$, so $F \subseteq \varphi(J)$. Thus we have shown that I_n contains F for each n.

It remains to prove that (I_n) is strict decreasing. We prove a more general fact: let J be a prime ideal of C such that, if f_n, f are elements in C and $f_n \to f$ pointwisely and $f_n \in J$ for all n, then $f \in J$ (we say J is *pointwise closed* if this is true). Then $\varphi(J) \subseteq J$ and $\varphi(J)$ is pointwise closed. For this, let $f \in \varphi(J)$, then $E_f(J)$ is infinite, hence contains a sequence (y_n) tends to 0; we have $\tau_{y_n}(f) \in J$ for each n, and letting n tends to infinite shows that $f \in J$, since $y_n \to 0$ by hypothesis and J is pointwise closed; this shows $\varphi(J) \subseteq J$. □

Exercise 16.1.7. Let R be a DVR and π a uniformizer for R. In the ring $R[T]$, the ideal $\mathfrak{m}_1 = (\pi T - 1)$ is maximal with height 1, the ideal $\mathfrak{m}_2 = (\pi) + (T)$ is maximal with height 2. The field $R[T]/\mathfrak{m}_1$ and $R[T]/\mathfrak{m}_2$ are isomomorphic to the field of fractions of R and to the residual field of R respectively. We have

$$\dim(R[T]) = 2, \quad \dim(R[T]/\mathfrak{m}_1) + \dim(R[T]_{\mathfrak{m}_1}) = 1, \quad \dim(\mathrm{gr}_{\mathfrak{m}_1}(R[T])) = 1. \tag{1.4.2}$$

Proof. Let K be the fraction field of R. Then it is easy to see $R[T]/\mathfrak{m}_1 \cong R[\pi^{-1}] = K$, so $\mathfrak{m}_1$ is maximal. Moreover, since $\mathfrak{m}_1$ is principal, it has height 1 by Corollary 16.3.17. Also, the quotient $R[T]/\mathfrak{m}_2$ is clearly isomomorphic to κ_R, so $\mathfrak{m}_2$ is maximal, and has height 2 by Corollary 16.3.17.

Clearly $\dim(R[T]) = \dim(R) + 1 = 2$ since R is Noetherian. The ring $R[T]_{\mathfrak{m}_1}$ has dimension equal to $\mathrm{ht}(\mathfrak{m}_1)$, which is 1. These prove the first two equalities in (1.4.2). To see $\dim(\mathrm{gr}_{\mathfrak{m}_1}(R[T])) = 1$, note that $\mathrm{gr}_{\mathfrak{m}_1}(R[T])$ is isomomorphic to a polynomial ring over K. □

Exercise 16.1.8. With the notations of the previous exercise, suppose that the residue field of R and fraction field of R are isomomorphic (this is the case for example when $R = k[\![X]\!]$, the field k being the field of fractions of a ring of formal series with an infinite number of indeterminates with coefficients in a field). Let σ be an isomorphism of $R[T]/\mathfrak{m}_1$ to $R[T]/\mathfrak{m}_2$. Let C be the subring of $R[T] = E$ formed of the elements of E whose classes modulo $\mathfrak{m}_1$ and $\mathfrak{m}_2$ are associated by σ: in other words, if $\pi_i : R[T] \to R[T]/\mathfrak{m}_i$ is the natural map, then

$$C = \{x \in R[T] : \sigma(\pi_1(x)) = \pi_2(x)\}.$$

Show that C is noetherian and that $\mathfrak{m}_1\mathfrak{m}_2 = \mathfrak{m}_1 \cap \mathfrak{m}_2$ is a maximal ideal of C. Show that E is the

integral closure of C (note that we have $E = C + (\pi T - 1)C$ and that $(\pi T - 1)^2 + (\pi T - 1)$ belongs to C).

Let A be the local ring $C_{\mathfrak{m}_1\mathfrak{m}_2}$. Then A is integral with dimension 2, hence catenary; the integral closure $B = E \otimes_C A$ of A is a semi-local Noetherian ring with exactly two maximal ideals $\mathfrak{n}_1$ and $\mathfrak{n}_2$, and we have $\dim(B_{\mathfrak{n}_1}) = 1$, $\dim(B_{\mathfrak{n}_2}) = 2$.

Proof. □

Exercise 16.1.9. Retain the notations of the previous exercise, and identify B with a quotient ring of the polynomial ring $A[U]$ by the prime ideal generated by $U^2 + U - \pi T(\pi T - 1)$. Let $\mathfrak{q}_i$ be the ideal of $A[U]$ such that $\mathfrak{n}_i = \mathfrak{q}_i/\mathfrak{p}$. Then $\mathrm{ht}(\mathfrak{q}_1) = 3$, $\mathrm{ht}(\mathfrak{p}) = 1$ and the chain $\mathfrak{p} \subseteq \mathfrak{q}_1$ is saturated. In particular, $A[U]$ and $A[U]_{\mathfrak{q}_1}$ are not catenary.

Exercise 16.1.10. Let A be a ring.

(a) Assume that A is an integral domain and let $f \in A[T]$, $f \neq 0$. Prove that there exists a maximal ideal $\mathfrak{m}$ of $A[T]$ such that $f \notin \mathfrak{m}$.

(b) Prove that $\dim(\mathrm{Max}(A[T])) \geq \dim(A) + 1$, so $\dim(\mathrm{Max}(A[T])) = \dim(A[T]) = \dim(A) + 1$ when A is Noetherian.

(c) Let k be a field, S the subset $1 + (X)$ of $k[X, Y]$, and $A = S^{-1}k[X, Y]$. Show that we have $\dim(\mathrm{Max}(A)) = 1$ and $\dim(\mathrm{Spec}(A)) = 2$. Generalize this to several indeterminates.

(d) Show that for any couple of integers $0 \leq n < m$, there exists a Noetherian ring A such that $\dim(\mathrm{Max}(A)) = n$ and $\dim(\mathrm{Max}(A[T])) = m$.

(e) Let A be the Noetherian ring defined in Exercise 16.1.5. Show that $\dim(\mathrm{Max}(A)) = 1$ and $\dim(\mathrm{Max}(A[T])) = \infty$.

Proof. Since the Jacobson radical of $A[T]$ is zero if A is integral, we have (a). Now let $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_n$ be a chain of prime ideals in A. Consider the chain

$$\mathfrak{p}_0[T] \subset \cdots \subset \mathfrak{p}_1[T] \subset \cdots \subset \mathfrak{p}_n[T] \subset (\mathfrak{p}_n, T)$$

of prime ideals of $A[T]$ and put

$$\begin{cases} U_i = V(\mathfrak{p}_i[T]) \cap \mathrm{Max}(A[T]), & 0 \leq i \leq n \\ U_{n+1} = V(\mathfrak{p}_n, T) \cap \mathrm{Max}(A[T]). \end{cases}$$

It is easy to see the chain $(U_i)_{0 \leq i \leq n+1}$ is decreasing and each U_i is closed; the fact it is strict follows immediately from (a). It remains to show that each U_i is irreducible. This shows the equality $\dim(\mathrm{Max}(A[T])) \geq \dim(A) + 1$. Recall that $\dim(\mathrm{Max}(A)) \leq \dim(A)$ for any ring and $\dim(A[T]) = \dim(A) + 1$ if A is Noetherian. So if A is Noetherian, we have

$$\dim(A) + 1 \leq \dim(\mathrm{Max}(A[T])) \leq \dim(A[T]) = \dim(A) + 1.$$

Let A be the ring in (c). Then the ring $A = S^{-1}k[X, Y]$ is just the ring $S^{-1}k[Y][X]$, and it is easy to see the chain $0 \subseteq (X) \subseteq (X, Y)$ corresponds to a chain of length 2 in A, whence $\dim(A) = 2$. For the space $\mathrm{Max}(A)$, note that a maximal ideal $(X - a, Y - b)$ is disjoint from S if and only

if $a = 0$, which indicates $\dim(\mathrm{Max}(A)) = 1$ at least when k is algebraically closed. In general, let $0 \le n \le m$ and consider the ring $k[X_1, \dots, X_m]$. Let S be the subset $1 + (X_1, \dots, X_{m-n})$, and $A = S^{-1}k[X_1, \dots, X_m]$. Then $\dim(A) = m$ and $\dim(\mathrm{Max}(A)) = n$. Note that in this case, since A is Noetherian, we have $\dim(\mathrm{Max}(A[T])) = \dim(A) + 1 = m + 1$, so (d) is proved.

Finally, consider the example of Exercise 16.1.5. Since A is Noetherian, we have

$$\dim(\mathrm{Max}(A[T])) = \dim(A[T]) = \infty.$$

But the maximal ideals of A are the $S^{-1}\mathfrak{p}_i$'s, and if $S^{-1}\mathfrak{p}$ is a prime ideal of A, it is contained in finitely many $S^{-1}\mathfrak{p}_i$'s. However, note that each singleton in $\mathrm{Max}(A)$ is closed, so the set $V(S^{-1}\mathfrak{p}) \cap \mathrm{Max}(A)$ is not irreducible unless it is a singleton or the whole space $\mathrm{Max}(A)$. This shows $\dim(\mathrm{Max}(A)) = 1$ (in fact, the topology on $\mathrm{Max}(A)$ is the cofinite topology, hence has Krull dimension 1). □

16.2 Dimension of algebras

16.2.1 Dimension and the going-down property

Let $\rho : A \to B$ be a ring homomorphism. Recall that we say ρ has the going-down property if it satisfies the going down theorem.

Proposition 16.2.1. *Let $\rho : A \to B$ be a ring homomorphism with the going-down property. Let F be a closed subset of* $\mathrm{Spec}(A)$. *If Y is an irreducible component of the inverse image of F under $\rho^* : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$, then the closure of $\rho^*(Y)$ is an irreducible component of F.*

Proof. Let $\mathfrak{a}$ be an ideal of A such that $F = V(\mathfrak{a})$. By Proposition 10.4.18, the inverse image by ρ^* of F is the subset $V(\mathfrak{a}^e)$ of $\mathrm{Spec}(B)$. Let $Y = V(\mathfrak{P})$ be an irreducible component of $V(\mathfrak{a}^e)$, then the closure of $\rho^*(Y)$ is the irreducible closed subset $V(\mathfrak{P}^c)$. So we have to prove that, if $\mathfrak{P}$ is a prime ideal minimal among the prime ideals of B containing $\mathfrak{a}^e$, then $\mathfrak{P}^c$ is minimal among the prime ideals of A containing $\mathfrak{a}$.

Suppose the contrary, then there would exist a prime ideal $\mathfrak{q}$ of A with $\mathfrak{a} \subseteq \mathfrak{q} \subset \mathfrak{P}^c$. According to the going-down property, there exist a prime ideal $\mathfrak{Q}$ of B lying over $\mathfrak{q}$ such that $\mathfrak{Q} \subset \mathfrak{P}$, whence $\mathfrak{a}^e \subseteq \mathfrak{Q} \subset \mathfrak{P}$, contrary to the hypothesis made on $\mathfrak{P}$. □

Proposition 16.2.2. *Let $\rho : A \to B$ be a ring homomorphism with the going-down property. Then we have the inequality*

$$\dim(B) \ge \dim(A) + \inf_{\mathfrak{m} \in \mathrm{Max}(A)} \dim(B/\mathfrak{m}B) \ge \dim(A) + \inf_{\mathfrak{p} \in \mathrm{Spec}(A)} \dim(B \otimes_A \kappa(\mathfrak{p})). \tag{2.1.1}$$

Proof. We have $\dim(A) = \sup_{\mathfrak{m}} \dim(A_{\mathfrak{m}})$, so it suffices to show the inequality

$$\dim(B) \ge \dim(A_{\mathfrak{m}}) + \dim(B/\mathfrak{m}B) \tag{2.1.2}$$

for each maximal ideal $\mathfrak{m}$ of A. In other words, we have to prove the inequality $\dim(B) \ge n + r$ if $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_n$ is a chain of prime ideals of A contained in $\mathfrak{m}$ and $\overline{\mathfrak{Q}}_0 \subset \cdots \subset \overline{\mathfrak{Q}}_r$ is a chain of prime ideals of $B/\mathfrak{m}B$. For $1 \le i \le r$, there exists a prime ideal $\mathfrak{Q}_{n+i}$ of B containing $\mathfrak{m}B$ such that $\overline{\mathfrak{Q}}_i = \mathfrak{Q}_{n+i}/\mathfrak{m}B$, and $\mathfrak{Q}_n \subset \cdots \subset \mathfrak{Q}_{n+r}$ is a chain of prime ideals of B. Let $\mathfrak{Q}$ be a prime ideal

lying over $\mathfrak{m}$, then by the going down property, there exists prime ideals $\mathfrak{Q}_0 \subset \cdots \subset \mathfrak{Q}_{n-1} \subset \mathfrak{Q}$ such that $\mathfrak{Q}_i$ is lying over $\mathfrak{p}_i$ for $0 \le i \le n-1$. Then we see $\mathfrak{Q}_0 \subset \cdots \subset \mathfrak{Q}_{n-1} \subset \mathfrak{Q}_n \subset \cdots \subset \mathfrak{Q}_{n+r}$ is a chain of prime ideals of B, whence $\dim(B) \ge n + r$. □

Corollary 16.2.3. *Let $\rho : A \to B$ be a ring homomorphism with the going-down property. Then for any ideal $\mathfrak{a}$ of A we have* $\mathrm{ht}(\mathfrak{a}) \le \mathrm{ht}(\mathfrak{a}^e)$.

Proof. Let $\mathfrak{P}$ be a prime ideal of B containing $\mathfrak{a}^e$, and $\mathfrak{p} = \mathfrak{P}^c$. By Proposition 7.3.20, the homomorphism $\rho_{\mathfrak{p}} : A_{\mathfrak{p}} \to B_{\mathfrak{P}}$ satisfies condition (PM), whence $\dim(A_{\mathfrak{p}}) \le \dim(B_{\mathfrak{P}})$ by Proposition 16.2.2. But $\mathrm{ht}(\mathfrak{a}) \le \dim(A_{\mathfrak{p}})$ since $\mathfrak{p}$ contains $\mathfrak{a}$, so $\mathrm{ht}(\mathfrak{a}) \le \dim(B_{\mathfrak{P}})$ for any prime ideal $\mathfrak{P}$ containing $\mathfrak{a}^e$, whence $\mathrm{ht}(\mathfrak{a}) \le \mathrm{ht}(\mathfrak{a}^e)$. □

Remark 16.2.1. Let $\rho : A \to B$ be a local homomorphism of Noetherian local rings satisfying the going down property. Then (Corollary 16.3.25) the equality holds in (2.1.1). On the other hand, the inequality in (2.1.1) can be strict (c.f. Exercise 16.2.1).

16.2.2 Dimension of a finitely generated algebra

Proposition 16.2.4. *Let $\rho : A \to B$ be a ring homomorphism. If $n = \sup_{\mathfrak{p}} \dim(B \otimes_A \kappa(\mathfrak{p}))$ with $\mathfrak{p}$ taking over prime ideals of A, then we have the inequality*

$$\dim(B) + 1 \le (n+1)(\dim(A) + 1).$$

In particular, if $\dim(A)$ *is finite and* $\dim(B \otimes_A \kappa(\mathfrak{p}))$ *is bounded from above, then* $\dim(B)$ *is finite.*

Proof. We may suppose that $\dim(A) < +\infty$ and $n < +\infty$. Let $\mathfrak{P}_0 \subset \cdots \subset \mathfrak{P}_m$ be a chain of prime ideals of B and set $\mathfrak{p}_i = \mathfrak{P}_i^c$. Then the sequence $\mathfrak{p}_i$ is increasing, so the set of its values is of cardinal $\le \dim(A) + 1$. For each $\mathfrak{p} \in \mathrm{Spec}(A)$, the set of $\mathfrak{P}_i$ such that $\mathfrak{P}_i = \mathfrak{p}$ is a chain of the subset $\rho^{*-1}(\mathfrak{p})$ of $\mathrm{Spec}(B)$, therefore has cardinality less than $\dim(B \otimes_A \kappa(\mathfrak{p})) + 1$, and concequent to $(n+1)$. It follows that $m + 1 \le (n+1)(dim(A) + 1)$, hence the proposition. □

Corollary 16.2.5. *Let A be a ring, then*

$$\dim(A) + 1 \le \dim(A[X]) \le 2\dim(A) + 1.$$

Proof. One direction is established. For the other, note that for any prime ideal $\mathfrak{p} \in \mathrm{Spec}(A)$, $A[X] \otimes_A \kappa(\mathfrak{p})$ is isomorphic to $\kappa(\mathfrak{p})[X]$, which is a PID hence of dimension 1. Thus the other side comes from Proposition 16.2.4. □

Corollary 16.2.6. *Let A be a ring and B a finitely generated A-algebra. If* $\dim(A) < +\infty$, *then* $\dim(B) < +\infty$.

Proof. It follows from Corollary 16.2.5 that the polynomial ring $A[X_1, \ldots, X_n]$ has finite dimension for all n, whence $\dim(B) < +\infty$. □

Lemma 16.2.7. *Let $\rho : A \to B$ be a ring homomorphism such that, for each prime ideal $\mathfrak{p}$ of A, the algebra $B \otimes_A \kappa(\mathfrak{p})$ is integral over $\kappa(\mathfrak{p})$. If $\mathfrak{P}$ and $\mathfrak{Q}$ are prime ideals of B such that $\mathfrak{P} \subset \mathfrak{Q}$, then $\mathfrak{P}^c \ne \mathfrak{Q}^c$.*

Proof. If $\mathfrak{P}^c = \mathfrak{Q}^c = \mathfrak{p}$, then $\mathfrak{P} \subset \mathfrak{Q}$ is a chain in $B \otimes_A \kappa(\mathfrak{p})$, whence $\dim(B \otimes_A \kappa(\mathfrak{p})) \geq 1$. But since $\kappa(\mathfrak{p})$ is a field and $B \otimes_A \kappa(\mathfrak{p})$ is integral over $\kappa(\mathfrak{p})$, we have $\dim(B \otimes_A \kappa(\mathfrak{p})) = 0$, a contradiction. □

Theorem 16.2.8. *Let $\rho : A \to B$ be a ring homomorphism such that B is integral over A, and $\rho^* : \operatorname{Spec}(B) \to \operatorname{Spec}(A)$ the induced map.*

(a) Let M be a finitely generated A-module. Then $\dim_B(M \otimes_A B) \leq \dim_A(M)$. If further ρ^* is surjective, then $\dim_B(M \otimes_A B) = \dim_A(M)$.

(b) Let $\mathfrak{b}$ be an ideal of B. Then $\operatorname{ht}(\mathfrak{b}) \leq \operatorname{ht}(\mathfrak{b}^c)$ and $\dim(B/\mathfrak{b}) = \dim(A/\mathfrak{b}^c)$. If further ρ^* is surjective, then $\operatorname{ht}(\mathfrak{a}^e) \leq \operatorname{ht}(\mathfrak{a})$ for any ideal $\mathfrak{a}$ of A.

(c) Suppose that B is a finitely generated A-module and let N be a finitely generated B-module. Then we have $\dim_B(N) = \dim_A(N)$. In particular, we have $\dim(B) = \dim_A(B)$.

Proof. By Corollary 13.1.17, the algebra $B \otimes_A \kappa(\mathfrak{p})$ is integral over $\kappa(\mathfrak{p})$. Let $\mathfrak{P}_0 \subset \cdots \subset \mathfrak{P}_m$ be a chain of prime ideals of B. Then by Lemma 16.2.7, the ideals $\mathfrak{p}_i = \mathfrak{P}_i^c$ are pairwise distinct, whence $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_m$ is a chain of prime ideals of A, and $m \leq \dim(A)$. This proves $\dim(B) \leq \dim(A)$.

Suppose further that ρ^* is surjective. Let $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_n$ be a chain of prime ideals of A. Then there exists a prime ideal $\mathfrak{P}_0$ of B lying over of $\mathfrak{p}_0$. According to Corollary 13.1.68, we can construct, by induction on n, a chain $\mathfrak{P}_0 \subset \cdots \subset \mathfrak{P}_n$ of prime ideals of B such that $\mathfrak{P}_i$ is lying over $\mathfrak{p}_i$ for each i. We therefore have $n \leq \dim(B)$ and consequently $\dim(A) = \dim(B)$.

This proves (a) in the case $M = A$. In the general case, let $\mathfrak{a}$ be the annihilator of M, so that the support of M is identified with $\operatorname{Spec}(A/\mathfrak{a})$, and we have $\dim_A(M) = \dim(A/\mathfrak{a})$. According to Proposition 10.4.40, the support of $M \otimes_A B$ is the inverse image by ρ^* of the support of M, therefore identifies with $\operatorname{Spec}(B/\mathfrak{a}^e)$, and we have $\dim_B(M \otimes_A B) = \dim(B/\mathfrak{a}^e)$. It remains to notice that the homomorphism $\bar{\rho} : A/\mathfrak{a} \to B/\mathfrak{a}^e$ deduced from ρ makes $B/\mathfrak{a}^e$ an integral $(A/\mathfrak{a})$-algebra, and that $\bar{\rho}^*$ is surjective when ρ^* is.

Now we prove (b). By the definition of height, it suffices to prove that $\operatorname{ht}(\mathfrak{b}) \leq \dim(A_\mathfrak{p})$ for any prime ideal $\mathfrak{p}$ of A containing $\mathfrak{b}^c$. Let $\mathfrak{p}$ be such an ideal, according to Corollary 13.1.68, there exists a prime ideal $\mathfrak{P}$ of B above $\mathfrak{p}$ and containing $\mathfrak{b}$, and we have $\operatorname{ht}(\mathfrak{b}) \leq \dim(B_\mathfrak{P})$. Now $B_\mathfrak{P}$ is identified with a ring of fractions of the integral $A_\mathfrak{p}$-algebra $B \otimes_A A_\mathfrak{p}$, from which we get

$$\dim(B_\mathfrak{P}) \leq \dim(B \otimes_A A_\mathfrak{p}) \leq \dim(A_\mathfrak{p})$$

by (a) and Proposition 16.1.3. We have thus proved the inequality $\operatorname{ht}(\mathfrak{b}) \leq \operatorname{ht}(\mathfrak{b}^c)$. Moreover, the homomorphism of $A/\mathfrak{a}$ in $B/\mathfrak{b}$ deduced from ρ is injective and makes $B/\mathfrak{b}$ an integral $(A/\mathfrak{a})$-algebra. We therefore have $\dim(B/\mathfrak{b}) = \dim(A/\mathfrak{a})$ according to (a). Assume now ρ^* surjective and let $\mathfrak{a}$ be an ideal of A and $\mathfrak{p}$ a prime ideal of A containing $\mathfrak{a}$. There exists by hypothesis a prime ideal $\mathfrak{P}$ of B above $\mathfrak{p}$. We have $\mathfrak{a}^e \subseteq \mathfrak{P}$, hence $\operatorname{ht}(\mathfrak{a}^e) \leq \operatorname{ht}(\mathfrak{P}) \leq \operatorname{ht}(\mathfrak{p})$ according to the above argument. Passing to the infimum, we obtain $\operatorname{ht}(\mathfrak{a}^e) \leq \operatorname{ht}(\mathfrak{a})$. Now part (c) follows from (b) by letting $\mathfrak{b}$ be the annihilator of N and noting that the annihilator of $\rho^*(N)$ is then $\mathfrak{b}^c$. □

Theorem 16.2.9. *Let A be an integrally closed ring, B a ring containing A and integral over A. Suppose that B is a torsion-free A-module, then*

(a) For any ideal $\mathfrak{a}$ of A, we have $\operatorname{ht}(\mathfrak{a}) = \operatorname{ht}(\mathfrak{a}^e)$.

(b) For any ideal $\mathfrak{b}$ *of* B*, we have* $\mathrm{ht}(\mathfrak{b}) = \mathrm{ht}(\mathfrak{b}^c)$.

Proof. Let $\rho : A \to B$ be the canonical homomorphism. Let $\mathfrak{a}$ be an ideal of A. If $\mathfrak{a} = A$, then (a) is clear by Theorem 16.2.8. Suppose $\mathfrak{a} \neq A$, so that $\mathfrak{a}^e \neq B$. Since ρ is injective, ρ^* is surjective by Theorem 13.1.67. Let $\mathfrak{P}$ be a prime ideal of B containing $\mathfrak{a}^e$ and $\mathfrak{p} = \mathfrak{P} \cap A$. We have $\mathfrak{a} \subseteq \mathfrak{p}$, whence $\mathrm{ht}(\mathfrak{a}) \leq \mathrm{ht}(\mathfrak{p})$. Let $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_n$ be a chain of prime ideals of A with $\mathfrak{p}_n = \mathfrak{p}$. According to the going down theorem (Corollary 13.1.78), we have a chain $\mathfrak{P}_0 \subset \cdots \subset \mathfrak{P}_n$ of prime ideals of B such that $\mathfrak{P}_n = \mathfrak{P}$ and $\mathfrak{P}_i$ is above $\mathfrak{p}_i$. We then have $n \leq \mathrm{ht}(\mathfrak{P})$, whence $\mathrm{ht}(\mathfrak{a}) \leq \mathrm{ht}(\mathfrak{P})$. By taking infimum we get $\mathrm{ht}(\mathfrak{a}) \leq \mathrm{ht}(\mathfrak{a}^e)$. The inequality $\mathrm{ht}(\mathfrak{a}^e) \leq \mathrm{ht}(\mathfrak{a})$ follows from Theorem 16.2.8, whence the first equality.

Let $\mathfrak{b}$ be an ideal of B and $\mathfrak{a} = \mathfrak{b}^c$. We have $\mathfrak{a}^e \subseteq \mathfrak{b}$, hence $\mathrm{ht}(\mathfrak{a}) = \mathrm{ht}(\mathfrak{a}^e) \leq \mathrm{ht}(\mathfrak{b})$. The inequality $\mathrm{ht}(\mathfrak{b}) \leq \mathrm{ht}(\mathfrak{a})$ follows from Theorem 16.2.8, hence the theorem. □

16.2.3 Dimension of finitely generated algebras over fields

In this part, k will denote a field, and we consider the finitely generated algebras over k.

Lemma 16.2.10. *Let* A *be a finitely generated* k*-algebra and* $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_m$ *a maximal chain of prime ideals of* A*. Then there exists an integer* $n \geq m$ *and a sequence* $(x_i)_{1\leq i\leq n}$ *of elements of* A *algebraically independent over* k *such that*

(a) A *is integral over* $B = k[x_1, \ldots, x_n]$.

(b) The ideal $\mathfrak{p}_j \cap B$ *is generated by* $x_1, \ldots, x_{n-m+j}$.

Proof. By Theorem 13.3.1, there exists an integer $n \geq 0$, a sequence $(x_i)_{1\leq i\leq n}$ of elements of A algebraically independent over k and an increasing sequence $(h_j)_{1\leq j\leq m}$ such that A is integral over $B = k[x_1, \ldots, x_n]$ and $\mathfrak{q}_j = \mathfrak{p}_j \cap B$ is generated by $x_1, \ldots, x_{h_j}$. By passing to the quotients, we deduce from the injective canonical homomorphism of B into A an injective homomorphism from $B/\mathfrak{q}_j$ into $A/\mathfrak{p}_j$ which makes $A/\mathfrak{p}_j$ an integral $(B/\mathfrak{q}_j)$-algebra. As the ring $B/\mathfrak{q}_j$ is isomorphic to a polynomial algebra in $n - h_j$ indeterminate over k, it is integrally closed. According to Theorem 16.2.9, we therefore have

$$1 = \mathrm{ht}(\mathfrak{p}_{j+1}/\mathfrak{p}_j) = \mathrm{ht}(\mathfrak{q}_{j+1}/\mathfrak{q}_j) \geq h_{j+1} - h_j.$$

whence $h_{j+1} \leq h_j + 1$. Since h_j is increasing and the ideals $\mathfrak{q}_j$ are pairwise distinct, we get $h_{j+1} = h_j + 1$. Also note that $h_m = n$ since $\mathfrak{q}_m$ is maximal ($\mathfrak{p}_m$ is maximal), so $h_j = n - m + j$ and the claim follows. □

Theorem 16.2.11. *Let* A *be a finitely generated* k*-algebra.*

(a) For every minimal prime ideal $\mathfrak{p}$ *of* A*, the maximal chains of prime ideals of* A *starting from* $\mathfrak{p}$ *have length* $\mathrm{tr.deg}_k(\kappa(\mathfrak{p}))$.

(b) The ring A *is catenary and its dimension is the supremum of the integers* $\mathrm{tr.deg}_k(\kappa(\mathfrak{p}))$*, where* $\mathfrak{p}$ *runs through minimal prime ideals of* A.

(c) Suppose that A *is an integral domain. Then the maximal chains of prime ideals of* A *have the same length, and the dimension of* A *equals to* $\mathrm{tr.deg}_k(K)$*, where* K *is the field of fraction of* A.

Proof. Suppose that A is an integral domain and consider a maximal chain $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_m$ of prime ideals of A. We have $\mathfrak{p}_0 = 0$. We then deduce from Lemma 16.2.10 the existence of a injective homomorphism $\varphi : k[X_1, \ldots, X_m] \to A$ of k-algebras which makes A an integral $k[X_1, \ldots, X_m]$-algebra. Consequently, the transcendence degree over k of the field of fractions of A is equal to m, hence (c). Assertion (a) follows from (c) applied to the ring $A/\mathfrak{p}$ and assertion (b) is an immediate consequence of (a). □

Corollary 16.2.12. *Let n be a positive integer, then* $\dim(k[X_1, \ldots, X_n]) = n$. *Moreover, for a finitely generated k-algebra A to be of dimension n, it is necessary and sufficient that there exists a injective k-homomorphism $\varphi : k[X_1, \ldots, X_n] \to A$ such that A is finite over $k[X_1, \ldots, X_n]$.*

Proof. This follows from Theorem 16.2.11, Theorem 13.3.1, and Theorem 16.2.8(a). □

Corollary 16.2.13. *Let A be a finitely generated k-algebra that is an integral domain. Then for any prime ideal $\mathfrak{p}$ of A, we have*

$$\mathrm{ht}(\mathfrak{p}) = \dim(A_{\mathfrak{p}}) = \dim(A) - \dim(A/\mathfrak{p}) = \dim(A) - \mathrm{tr.\,deg}_k(\kappa(\mathfrak{p})).$$

Proof. This is a concequence of Theorem 16.2.11 and Proposition 16.1.9. □

Corollary 16.2.14. *Let A be a finitely generated k-algebra and let f be an element of A which does not belong to any minimal prime ideal of A. Then* $\dim(A) = \dim(A_f)$.

Proof. The map $\mathfrak{p} \mapsto \mathfrak{p}A_f$ is a bijection between the set of minimal prime ideals of A and that of A_f. Since $A/\mathfrak{p}$ and $A_f/\mathfrak{p}A_f$ have the same field of fraction, it suffices to apply Theorem 16.2.11. □

Corollary 16.2.15. *Let A be a finitely generated k-algebra and $\mathfrak{p}$ a prime ideal of A.*

(a) For $\mathfrak{p}$ to be maximal, it is necessary and sufficient that $\kappa(\mathfrak{p})$ is a finite extension of k.

(b) Let $f \in A - \mathfrak{p}$. Then the ideal $\mathfrak{p}$ is a maximal ideal of A if and only if $\mathfrak{p}A_f$ is a maximal ideal of A_f.

Proof. If $\mathfrak{p}$ is a maixmal ideal of A, then $A/\mathfrak{p}$ is a field, whence a finitely generated extension of k of transcendence degree 0. It is therefore a finite extension of k (Theorem 16.2.11). Conversely, if the field $\kappa(\mathfrak{p})$ is a finite extension of k, we have $\dim(A/\mathfrak{p}) = 0$, so $\mathfrak{p}$ is maximal. The assertion (b) now follows from (a), taking into account that $A/\mathfrak{p}$ and $A_f/\mathfrak{p}A_f$ have the same field of fractions. □

Corollary 16.2.16. *Let A be a finitely generated k-algebra, $\mathfrak{p}$ a prime ideal of A and $(\mathfrak{p}_i)_{i\in I}$ the family of minimal prime ideals of A. Then we have*

$$\dim_{\mathfrak{p}}(A) = \sup_{i\in I_{\mathfrak{p}}} \dim(A/\mathfrak{p}_i) = \dim(A_{\mathfrak{p}}) + \dim(A/\mathfrak{p}) = \dim(A_{\mathfrak{p}}) + \mathrm{tr.\,deg}_k(\kappa(\mathfrak{p}))$$

where $I_{\mathfrak{p}}$ is the subset consists of $i \in I$ such that $\mathfrak{p}_i \subseteq \mathfrak{p}$.

Proof. We have $\dim_{\mathfrak{p}}(A) = \sup_{i\in I_{\mathfrak{p}}} \dim_{\mathfrak{p}/\mathfrak{p}_i}(A/\mathfrak{p}_i)$ by Proposition 16.1.3, since A is Noetherian. Also, from Corollary 16.2.14 we conclude that

$$\dim_{\mathfrak{p}/\mathfrak{p}_i}(A/\mathfrak{p}_i) = \inf_{f\notin\mathfrak{p}/\mathfrak{p}_i} \dim((A/\mathfrak{p}_i)_f) = \dim(A/\mathfrak{p}_i)$$

so the first equality follows. Now since $A/\mathfrak{p}_i$ is an integral domain, Corollary 16.2.13 shows $\dim(A/\mathfrak{p}_i) = \dim((A/\mathfrak{p}_i)_\mathfrak{p}) + \dim(A/\mathfrak{p})$. Other equalities then follows from the observation $\dim(A_\mathfrak{p}) = \sup_{i\in I_\mathfrak{p}} \dim((A/\mathfrak{p}_i)_\mathfrak{p})$ and Theorem 16.2.11. □

Corollary 16.2.17. *Let A be a finitely generated k-algebra, n a positive integer. Then the following conditions are equivalent:*

(i) For every $\mathfrak{p} \in \mathrm{Ass}(A)$, we have $\dim(A/\mathfrak{p}) = n$.

(ii) Every prime ideal associated with A is minimal and all irreducible components of $\mathrm{Spec}(A)$ are of dimension n.

(iii) There exists an injective homomorphism $\varphi : k[X_1, \dots, X_n] \to A$ such that A is a finitely generated torsion-free $k[X_1, \dots, X_n]$-module.

Proof. The equivalence of (i) and (ii) is immediate. Now suppose that (ii) holds. Then $\dim(A) = n$ and by Corollary 16.2.12 there is an injective k-homomorphism

$$\varphi : k[X_1, \dots, X_n] \to A$$

such that A is finite over $k[X_1, \dots, X_n]$. For any prime ideal $\mathfrak{p} \in \mathrm{Ass}(A)$, the ring $A/\mathfrak{p}$ is then integral over $k[X_1, \dots, X_n]$, and we have so $n = \dim(A/\mathfrak{p}) = \dim(k[X_1, \dots, X_n]/\varphi^{-1}(\mathfrak{p}))$ according to Theorem 16.2.8(a), which proves $\varphi^{-1}(\mathfrak{p}) = 0$. By Corollary 12.1.6, this shows the image by the injective homomorphism φ of a nonzero element of $k[X_1, \dots, X_n]$ is not a divisor of 0 in A, whence (c).

Conversely, assume that (iii) holds. For each prime ideal $\mathfrak{p} \in \mathrm{Ass}(A)$, the homomorphism $\varphi : k[X_1, \dots, X_n] \to A/\mathfrak{p}$ induced by φ is injective by Corollary 12.1.6, whence $\dim(A/\mathfrak{p}) = n$ by Corollary 16.2.12. □

Corollary 16.2.18. *Under the condition of Corollary 16.2.17, $\dim_\mathfrak{p}(A) = \dim(A)$ for every prime ideal $\mathfrak{p}$ of A.*

Proof. This follows from Corollary 16.2.16. □

Proposition 16.2.19. *Let A and B be finitely generated k-algebras and $\rho : A \to B$ a k-algebra homomorphism. Suppose that A is an integral domain and B is a torsion-free A-module, and let K be the field of fraction of A. Then we have*

$$\dim(B) = \dim(A) + \dim(B \otimes_A K).$$

Proof. Suppose that B is an integral domain. The algebra $B \otimes_A K$ is then a ring of fractions of B defined by a multiplicative part not containing 0. It therefore has field of fractions the field of fractions L of B. According to Theorem 16.2.11, we have

$$\dim(B) = \mathrm{tr.\,deg}_k(L), \quad \dim(A) = \mathrm{tr.\,deg}_k(K), \quad \dim(B \otimes_A K) = \mathrm{tr.\,deg}_K(L).$$

By the transitivity of transcendental degree, we see the claim is true in this case.

Let's consider to the general case. Every minimal prime ideal $\mathfrak{P}$ of B is formed by divisors of zero in B, so is lying over the ideal 0 of A. By Proposition 10.2.36 it follows that the map

$\mathfrak{P} \mapsto \mathfrak{P}(B \otimes_A K)$ is a bijection of the set of minimal prime ideals of B on the set of minimal prime ideals of $B \otimes_A K$. The proposition follows therefore from the first part of the proof and from Proposition 16.1.3. □

Corollary 16.2.20. *Let $\rho : A \to B$ be an injective homomorphism of finitely generated k-algebras. Then* $\dim(A) \leq \dim(B)$.

Proof. In fact, let $\mathfrak{p}$ be a minimal prime of A such that $\dim(A) = \dim(A/\mathfrak{p})$. Then there exists a prime ideal $\mathfrak{P}$ of A lying over $\mathfrak{p}$ by Proposition 10.2.43. According to Proposition 16.2.19 applied to $A/\mathfrak{p}$ and $B/\mathfrak{P}$, we have $\dim(A) = \dim(A/\mathfrak{p}) \leq \dim(B/\mathfrak{P}) \leq \dim(B)$, whence the corollary. □

Lemma 16.2.21. *Let A and B be k-algebras that are integral domains, M a torsion-free A-module, N a torsion-free B-module. Then the ring $A \otimes_k B$ is an integral domain, and $M \otimes_k N$ is a torsion-free $A \otimes_k B$ module.*

Proof. Let K (resp. L) be the field of fraction of A (resp. B). Then there exists a set I (resp. J) such that M (resp. N) is isomorphic to a submodule of $K^{\oplus I}$ (resp. $L^{\oplus J}$). The $(A \otimes_k B)$-module $M \otimes_k N$ is then isomorphic to a submodule of $K^{\oplus I} \otimes_k L^{\oplus J}$, which is isomorphic to $(K \otimes_k L)^{\oplus(I \times J)}$. As $K \otimes_k L$ is a ring of fractions of the ring $A \otimes_k B$, it is a torsion-free $A \otimes_k B$-module, hence the lemma. □

Proposition 16.2.22. *Let k' be an extension field of k, A a finitely generated k-algebra and B a finitely generated k'-algebra.*

(a) The k'-algebra $A \otimes_k B$ is finitely generated and we have

$$\dim(A \otimes_k B) = \dim(A) + \dim(B).$$

(b) Let $\mathfrak{r}$ be a prime ideal of $A \otimes_k B$. If $\mathfrak{p}$ (resp. $\mathfrak{q}$) is the contraction of $\mathfrak{r}$ to A (resp. B), then

$$\dim_{\mathfrak{r}}(A \otimes_k B) = \dim_{\mathfrak{p}}(A) + \dim_{\mathfrak{q}}(B).$$

Proof. Put $n = \dim(A)$ and $m = \dim(B)$. There exists according to Corollary 16.2.12 injective homomorphisms of algebras $\varphi : k[X_1, \ldots, X_n] \to A$ and $\psi : k'[Y_1, \ldots, Y_m] \to B$ making respectively of A and B finite algebras over $k[X_1, \ldots, X_n]$ and $k'[Y_1, \ldots, Y_m]$. The homomorphism $\varphi \otimes \psi$ is then injective and makes $A \otimes_k B$ a finite algebra over the k'-algebra $k[X_1, \ldots, X_n] \otimes_k k'[Y_1, \ldots, Y_m]$, which identifies with $k'[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$ (to see that $\varphi \otimes \psi$ is injective, we may consider the following commutative diagram

$$\begin{tikzcd}
k[X] \otimes k'[Y] \arrow[r, "1\otimes\psi"] \arrow[d, "\varphi\otimes 1"'] & k[X] \otimes B \arrow[d, "\varphi\otimes 1"] \\
A \otimes k'[Y] \arrow[r, "1\otimes\psi"] & A \otimes B
\end{tikzcd}$$

where $\varphi \otimes \psi$ is the composition homomorphism, and note that all modules are flat since we are tensoring over k). We then have $\dim(A \otimes_k B) = n + m$ by Corollary 16.2.12, which proves (a).

Note that when A and B are integral domains, the $k'[X_1, \dots, X_n, Y_1, \dots, Y_m]$-module $A \otimes_k B$ is torsion free by Lemma 16.2.21 and therfore we have

$$\dim_{\mathfrak{r}}(A \otimes_k B) = \dim(A \otimes_k B) = \dim(A) + \dim(B)$$

for any prime ideal $\mathfrak{r}$ of $A \otimes_k B$ by Corollary 16.2.18.

Now let us show (b). Let $\mathfrak{r}_0$ be a minimal prime ideal of $A \otimes_k B$ contained in $\mathfrak{r}$, and let $\mathfrak{p}_0$ (resp. $\mathfrak{q}_0$) be the contraction of $\mathfrak{r}_0$ to A (resp. B). The ring $(A \otimes_k B)/\mathfrak{r}_0$ is isomorphic to a quotient of the ring $(A/\mathfrak{p}_0) \otimes_k (B/\mathfrak{q}_0)$. Thus we have, by (a),

$$\dim((A \otimes_k B)/\mathfrak{r}_0) \leq \dim((A/\mathfrak{p}_0) \otimes_k (B/\mathfrak{q}_0)) = \dim(A/\mathfrak{p}_0) + \dim(B/\mathfrak{q}_0).$$

According to Corollary 16.2.16, this shows

$$\dim_{\mathfrak{r}}(A \otimes_k B) \leq \dim_{\mathfrak{p}}(A) + \dim_{\mathfrak{q}}(B).$$

Conversely, let $\mathfrak{p}_0$ (resp. $\mathfrak{q}_0$) be a minimal prime ideal of A (resp. B) contained in $\mathfrak{p}$ (resp. $\mathfrak{q}$). By the observation above, we have

$$\dim(A/\mathfrak{p}_0) + \dim(B/\mathfrak{q}_0) = \dim_{\bar{\mathfrak{r}}}((A/\mathfrak{p}_0) \otimes_k (B/\mathfrak{q}_0)) \leq \dim_{\mathfrak{r}}(A \otimes_k B)$$

where $\bar{\mathfrak{r}}$ is the image of $\mathfrak{r}$ by the canonical surjection $A \otimes_k B \to (A/\mathfrak{p}_0) \otimes_k (B/\mathfrak{q}_0)$. Applying Corollary 16.2.16, we deduce the inequality

$$\dim_{\mathfrak{p}}(A) + \dim_{\mathfrak{q}}(B) \leq \dim_{\mathfrak{r}}(A \otimes_k B)$$

whence (b) follows. □

Corollary 16.2.23. *Let A be a finitely generated k-algebra, k' an extension field of k, and A' the k'-algebra $A \otimes_k k'$.*

(a) We have $\dim(A') = \dim(A)$.

(b) Let $\mathfrak{p}'$ be a prime ideal of A and $\mathfrak{p}$ its contraction to A. Then $\dim_{\mathfrak{p}'}(A') = \dim_{\mathfrak{p}}(A)$.

(c) Let $\mathfrak{p}'$ be a minimal prime ideal of A and $\mathfrak{p}$ its contraction to A. Then $\mathfrak{p}$ is minimal and $\dim(A'/\mathfrak{p}') = \dim(A/\mathfrak{p})$.

(d) If k' is a purely inseparable extension of k, then the canonical map ${}^a\rho : \operatorname{Spec}(A') \to \operatorname{Spec}(A)$ is a homeomorphism.

Proof. Part (a) and (b) follows from Proposition 16.2.22 by setting $B = k'$. For (c), note that the homomorphism $\nu : k \to k'$ satisfies condition (PM), so the ideal $\mathfrak{p}'$ is minimal by Proposition 7.3.20(a) and (c). By corollary 16.2.16, we then have

$$\dim(A'/\mathfrak{p}') = \dim_{\mathfrak{p}'}(A') = \dim_{\mathfrak{p}}(A) = \dim(A/\mathfrak{p})$$

which completes the proof of (c).

Finally, assume that k'/k is purely inseparable, and let $\rho : A \to A'$ be the canonical homomorphism. Let $\mathfrak{p} \in \operatorname{Spec}(A)$, recall that the fiber of $\mathfrak{p}$ under ${}^a\rho$ is homeomorphic to

$\mathrm{Spec}(\kappa(\mathfrak{p})\otimes_k k')$. Now the set $\mathfrak{n}$ of nilpotent elements of $\kappa(\mathfrak{p})\otimes_k k'$ is a prime ideal by Corallary **??** and the quotient ring $(\kappa(\mathfrak{p})\otimes_k k')/\mathfrak{n}$ is a field by **??**. Therefore $({}^a\rho)^{-1}(\mathfrak{p})$ is reduced to a singleton. It follows that the map ${}^a\rho$ is a bijection of $\mathrm{Spec}(A')$ on $\mathrm{Spec}(A)$. Since we have observed that ρ has the going up property (Proposition 7.3.20), it follows from Proposition 13.1.82 that ${}^a\rho$ is a closed map, whence a homeomorphism. □

16.2.4 Exercise

Exercise 16.2.1. Let R be a DVR with fraction field K and n an integer. Let A be the subring of the polynomial ring $K[X_1,\dots,X_n]$ consists of polynomials whose constant terms are in R. Then the canonical homomorphism $\rho : R \to A$ satisfies the going down property and the canonical homomorphism $R/\mathfrak{m}_R \to A/\mathfrak{m}_R A$ is an isomorphism. On the other hand, we have $\dim(A) \geq n+1$ and $\dim(R) = 1$. As long as $n \geq 1$, we have $\dim(A) > \dim(R) + \dim(A/\mathfrak{m}_R A)$. Show that A is not Noetherian. By using formal series, construct an similar example where A is local and not Noetherian.

Proof. It is clear that A is a subring of $K[X_1,\dots,X_n]$ and $A/\mathfrak{m}_R A$ is isomomorphic to $R/\mathfrak{m}_R$; A is flat over R since it is torsion-free (Proposition 14.1.5). Since $\mathfrak{a}^{ec} = \mathfrak{a}$ for every ideal of R, by Proposition 7.3.15 we conclude that A is faithfully flat over R, whence the going down property is satisfied (Proposition 7.3.20). Let $\mathfrak{m}_R[X_1,\dots,X_n]$ be the ideal consists of polynomials with coefficients in $\mathfrak{m}_R$. Then it is clear that $\mathfrak{m}_R[X_1,\dots,X_n]$ is prime in A and we have a chain

$$0 \subset \mathfrak{m}_R[X_1,\dots,X_n] \subset \mathfrak{m}_R[X_1,\dots,X_n] + (X_1) \subset \cdots \subset \mathfrak{m}_R[X_1,\dots,X_n] + (X_1,\dots,X_n)$$

in the ring $K[X_1,\dots,X_n]$. Contracting this to A, we get a chain of length $n+1$ in A, so $\dim(A) \geq n+1$. Since $A/\mathfrak{m}_R A \cong R/\mathfrak{m}_R$ is a field, this shows

$$\dim(A) \geq n+1 > \dim(R) + \dim(A/\mathfrak{m}_R A)$$

as long as $n \geq 1$.

To see A is not Noetherian, we claim that the ideal $\mathfrak{p} = (X_1,\dots,X_n) \cap A$ in A is not finitely generated. In fact, if $f_1,\dots,f_n \in A$ generate $\mathfrak{p}$, then $\sum_i f_i(0)g_i(0)$ can take any element in K as g_i varies in A. But this is not possible since $f_i(0), g_i(0) \in R$.

Finally, replacing $K[X_1,\dots,X_n]$ with $K[\![X_1,\dots,X_n]\!]$, we see the resulting ring A is then local with maximal ideal $\mathfrak{m}_R[\![X_1,\dots,X_n]\!] + (X_1,\dots,X_n)$. □

Exercise 16.2.2. Let R be a DVR with fraction field K and residue field k. Put $A = K \times k$, and let $\rho : R \to A$ be the homomorphism deduced from the canonical homomorphisms $R \to K$ and $R \to k$. Then the homomorphism ρ is injective, the induced map $\rho^* : \mathrm{Spec}(A) \to \mathrm{Spec}(R)$ is surjective, A is a finitely generated R-algebra, and we have $\dim(A) < \dim(R)$.

Proof. Since $R \to K$ is injective, it is clear that ρ is injective. Also, we have $\mathrm{Spec}(A) = \mathrm{Spec}(K) \amalg \mathrm{Spec}(k)$, which consists of two elements $(0)_K$ and $(0)_k$. The image of $(0)_K$ under ρ is $(0)_R$, and that of $(0)_k$ is $\mathfrak{m}_R$. Therefore ρ^* is surjective. Since K and k are finitely generated R-algebra, so is A, and we have $\dim(A) = 0 < \dim(R) = 1$. □

Exercise 16.2.3. Let A be an integral domain and $\mathfrak{P}_0 \subset \mathfrak{P}_1 \subset \mathfrak{P}_2$ be a chain of prime ideals in $A[X]$. Show that $\mathfrak{P}_0, \mathfrak{P}_1, \mathfrak{P}_2$ can not have the same contraction in A. In particular, if A is

one-dimensional and $\mathfrak{P}_i$ are nonzero, then $\mathfrak{P}_0 \cap A = \{0\}$, $\mathfrak{P}_2 = (\mathfrak{P}_1 \cap A) \cdot A[X]$, and $\mathfrak{P}_2$ is maximal.

Proof. Let $\mathfrak{P}_0 \cap A = \mathfrak{P}_1 \cap A = \mathfrak{P}_2 \cap A = \mathfrak{p}$. Then $\mathfrak{P}_i = \mathfrak{p}A[X] + (X)$ for $i = 0, 1, 2$, which contradicts that $\mathfrak{P}_i$ are distinct. Now assume that $\dim(A) = 1$ and $\mathfrak{P}_i$ are nonzero. Recall that we have $2 \leq \dim(A[X]) \leq 3$ (Corollary 16.2.5), and since 0 is a prime ideal of $A[X]$, the chain $\mathfrak{P}_0 \subset \mathfrak{P}_1 \subset \mathfrak{P}_2$ shows that $\dim(A[X]) = 3$. Therefore $\mathfrak{P}_2$ is a maximal ideal in $A[X]$ and it contains (X). Now consider the contracted chain

$$0 \subseteq \mathfrak{P}_0^c \subseteq \mathfrak{P}_1^c \subseteq \mathfrak{P}_2^c.$$

Since A has dimension 1 and $\mathfrak{P}_2$ is maximal in $A[X]$, $\mathfrak{P}_2^c$ must be a maximal ideal in A. The inclusion $0 \subseteq \mathfrak{P}_0^c$ can not be strict since otherwise we have $\mathfrak{P}_0^c = \mathfrak{P}_1^c = \mathfrak{P}_2^c$. This proves $\mathfrak{P}_0^c = \{0\}$. We also note that $\mathfrak{P}_1^c \neq \{0\}$ since otherwise $\mathfrak{P}_0 = \mathfrak{P}_1 = (X)$ (again by Example 16.6.3). Therefore $\mathfrak{P}_1^c = \mathfrak{P}_2^c$ is a maximal ideal of A, and since $\mathfrak{P}_1 \neq \mathfrak{P}_2$, we have $X \notin \mathfrak{P}_2$ and $\mathfrak{P}_2 = \mathfrak{P}_2^c \cdot A[X]$. □

Exercise 16.2.4. Let A be an integrally closed domain with K the fraction field. For any element $x \in K$, we denote by $A[x]$ the sub-A-algebra of K generated by x. Let x be nonzero in K and $x^{-1} \notin A$; let $A[X]$ be the polynomial ring over A, and $\varphi : A[X] \to A[x]$ the canonical map $P \mapsto P(x)$.

(a) The kernel of φ is the ideal $\mathfrak{Q}$ generated by the polynomials of the form $aX + b$, where $a, b \in A$ and $ax + b = 0$.

(b) Let A be local with maximal ideal $\mathfrak{m}_A$. Then the ideal $\mathfrak{m}_A A[x]$ of $A[x]$ is prime, and is maximal if and only if $x \in A$.

Proof. Let φ be the canonical map. Assume that $P(X) = \sum_{i=0}^{n} a_i X^i$ and $P(x) = 0$. Then by multiplying a_n^{n-1}, we get

$$(a_n x)^n + a_{n-1}(a_n x)^{n-1} + \cdots + a_n^{n-2} a_1 (a_n x) + a_n^{n-1} a_0 = 0,$$

so $-b := a_n x$ is integral over A, hence belongs to A. Consider the polynomial $a_n X + b$: it has x as a root and the same leading coefficient with P. Hence $a_n X + b \mid P(X)$ and assertion (a) is proved. We also note that, since $x^{-1} \notin A$, the element b can not be invertible, hence $b \in \mathfrak{m}_A$.

Now by (a), we have

$$A[x]/\mathfrak{m}_A A[x] \cong A[X]/(aX + b, \mathfrak{m}_A) = \kappa_A[X]/(\bar{a}X + \bar{b}) = \kappa_A[X]/(\bar{a}X)$$

where a, b are the generators of $\ker \varphi$, and we have remarked that $b \in \mathfrak{m}_A$. Since these are irreducible elements, we conclude that $\mathfrak{m}_A A[x]$ is prime, and maximal iff there exists $a \in A$ in these generators such that $\bar{a} \neq 0$. But this just means $a \notin \mathfrak{m}_A$, hence invertible, and we then have $x = a^{-1} b \in A$. □

Exercise 16.2.5. Let A be an integrally closed domain with fraction field K. Given a prime ideal $\mathfrak{p}$ of A, an element x of K such that $x \notin A_{\mathfrak{p}}$, and $x^{-1} \notin A_{\mathfrak{p}}$, the ideal $\mathfrak{p}A[x]$ of $A[x]$ is prime; we have $\mathfrak{p}A[x] \cap A = \mathfrak{p}$ and the canonical homomorphism $(A/\mathfrak{p})[X] \to A[x]/\mathfrak{p}A[x]$ is an isomorphism.

Proof. Since $x \notin A_{\mathfrak{p}}$, and $x^{-1} \notin A_{\mathfrak{p}}$, we have $x \notin A$, so we can prove that $\mathfrak{p}A[x]$ is prime. Since A is integrally closed, it is not hard to se $\mathfrak{p}A[x] \cap A = \mathfrak{p}$. Since $x \notin A_{\mathfrak{p}}$ and $x^{-1} \notin A_{\mathfrak{p}}$, by Exericse 16.2.4, the kernel of the canonical map $\varphi : A[X] \to A[x]$ the ideal $\mathfrak{Q}$ generated by the polynomials of the form $aX + b$, where $a, b \in \mathfrak{p}$ and $ax + b = 0$. Since we have

$$A[x]/\mathfrak{p}A[x] = A[X]/(\mathfrak{p}, \mathfrak{Q}) = (A/\mathfrak{p})[X]/\bar{\mathfrak{Q}}$$

and the image of $\mathfrak{Q}$ in $A/\mathfrak{p}$ is zero, we see $(A/\mathfrak{p})[X]$ is isomorphic to $A[x]/\mathfrak{p}A[x]$. □

Exercise 16.2.6. We say an integral domain A is an ***F*-ring** if $\dim(A) = 1$ but $\dim(A[X]) > 2$.

(a) Using the previous exercise, show that if A is a one-dimensional integral domain then $\dim(A[X]) = 2$ if and only if the localization at any prime ideal of the integral closure of A is a valuation ring.

(b) Show that if we have $\dim(A) = n$ and $\dim(A[X]) > n + 1$, there exists a prime ideal $\mathfrak{p}$ of A such that $\mathrm{ht}(\mathfrak{p}) = 1$ and, either $\dim(A_{\mathfrak{p}}[X]) > 2$, or $\dim((A/\mathfrak{p})[X]) > \dim(A/\mathfrak{p}) + 1$.

Proof. Let A be as in (a) and by taking integral closure and note that if R is the integral closure of A, then $R[X]$ is the integral closure of $A[X]$, we may assume that A is integrally closed. Assume that there exists $0 \neq x \in K$ such that $x, x^{-1} \notin A_{\mathfrak{p}}$. Then by Exercise 16.2.4 applied to $A_{\mathfrak{p}}$, the ideal $\mathfrak{p}A_{\mathfrak{p}}[x]$ is not maximal in $A_{\mathfrak{p}}[x]$, whence $A_{\mathfrak{p}}[x]$ has dimension ≥ 2. But since $A_{\mathfrak{p}}[x]$ is a quotient of $A_{\mathfrak{p}}[X]$, this implies $\dim(A[X]) \geq \dim(A_{\mathfrak{p}}[X]) \geq 3$, so $\dim(A[X]) = 2$ iff there is not such x, or in other words $A_{\mathfrak{p}}$ is a valuation ring.

Now let A be n-dimensional and $\dim(A[X]) \neq n+1$. Suppose that for some minimal prime ideal $\mathfrak{p}$ of A, $\mathfrak{p}A[X]$ is not minimal in $A[X]$; that is, there exists a prime ideal $\mathfrak{P}$ of $A[X]$ such that

$$0 \subset \mathfrak{P} \subset \mathfrak{p}A[X].$$

Then $0 \subset \mathfrak{P}A_{\mathfrak{p}}[X] \subset \mathfrak{p} \cdot A_{\mathfrak{p}}[X]$ is also a chain of prime ideals in $A_{\mathfrak{p}}[X]$, as one easily verifies. Since $\mathfrak{p} \cdot A_{\mathfrak{p}}[X]$ is not maximal (for example $\mathfrak{p} \cdot A_{\mathfrak{p}}[X] + (X)$ contains it), this shows that $A_{\mathfrak{p}}$ is an F-ring. We pass then to the case that $\mathfrak{p}A[X]$ is minimal for every minimal prime ideal $\mathfrak{p}$ of A. Let

$$0 \subset \mathfrak{P}_1 \subset \cdots \subset \mathfrak{P}_{n+2}$$

be a chain of prime ideals in $A[X]$ (recall that $\dim(A[X]) \geq n+2$). If $\mathfrak{P}_1 \cap A = \mathfrak{p}$ is nonzero, then $A/\mathfrak{p}$ is at most $(n-1)$-dimensional, and $A[X]/\mathfrak{p}A[X]$ is a polynomial ring in one variable over $A/\mathfrak{p}$ and is at least $(n+1)$-dimensional, which proves the claim. So we may suppose $\mathfrak{P}_1 \cap A = 0$. But then $\mathfrak{P}_2 \cap A = \mathfrak{p}_2 \neq 0$ (by Exercise 16.2.3); let $\mathfrak{p}$ be a minimal prime ideal contained in $\mathfrak{p}_2$- such exists since A is finite dimensional; then $\mathfrak{p}A[x] \subseteq \mathfrak{P}_2$, properly, since $\mathfrak{p}A[X]$ is minimal but $\mathfrak{P}_2$ is not. Replacing $\mathfrak{P}_1$ by $\mathfrak{p}A[X]$, we come back to a previous case, and the proof is complete. □

Exercise 16.2.7. Let O be an integrally closed ring, with fraction field k. We put $d = \dim(O)$ and $t = \dim(O[X])$. Let k' be a non-trivial extension of k in which k is algebraically closed and let R be a discrete valuation ring (which is not a field) with residual field k'. We denote K the field of fractions of R and A the set of elements of R whose image in k' belongs to O.

(a) Show that the ring A is integrally closed with fraction field K.

(b) Let $\mathfrak{p}$ be the kernel of the surjective homomorphism $A \to O$. Show that every nonzero prime ideal of A contains $\mathfrak{p}$ and hence $\dim(A) = d + 1$.

(c) Considering an element x of R whose image in k' does not belong to k, show that the local ring $A_\mathfrak{p}$ is not not a valuation ring, and that $\mathfrak{p}A_\mathfrak{p}[x]$ is not minimal among non-zero prime ideals of $A_\mathfrak{p}[x]$. By using Exercise 16.2.6, deduce that we have $\dim(A[x]) \geq t + 2$. Conclude that we have $\dim(A[x]) = t + 2$ by a direct argument.

(d) Finally, show that for any pair (d, t) of integers with $d + 1 \leq t \leq 2d + 1$, there exists an integrally closed domain A of dimension d such that $\dim(A[X]) = t$.

Proof. Let v be the valuation of K associated with R. Note that any element in K can be written as a/b where $a, b \in R$. Moreover, we can assume that a, b has positive valuations, whence are in $\mathfrak{m}_R \subseteq A$. This shows the fraction field of A is K. Now let $x \in K$ be integral over A, and let

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

be an equation of integral dependence. Dividing this equation by x^s and supposing x^{-1} to have residue 0 in k', we get the contradiction $1 = 0$, so $x^{-1} \notin \mathfrak{m}_R$ and thus $x \in R$; we then have

$$\bar{x}^n + \bar{a}_{n-1}\bar{x}^{n-1} + \cdots + \bar{a}_0 = 0$$

where the bars indicate residues. Since each $\bar{a}_i$ is in O and k is algebraically closed in k' we deduce that $\bar{x} \in K$; whence $\bar{x} \in O$, since O is integrally closed. Hence A is integrally closed.

Let $\mathfrak{p}$ be the kernel of the canonical map $A \to O$. Then $\mathfrak{p}$ is a prime ideal. From the definitions one obtains $A/\mathfrak{p} \cong O$, whence A is at least $(n + 1)$-dimensional. If $\mathfrak{q}$ is a nonzero prime ideal in A, then $\mathfrak{q}$ contains $\mathfrak{p}$: In fact, let $x \in \mathfrak{q}$; since x is $A \subseteq R$, we have $v(x) = e \geq 0$. Since any element in $\mathfrak{p}$ has valuation ≥ 1, its $(e+1)$-th power is divisible by x, whence $\mathfrak{p}^{e+1} \subseteq \mathfrak{q}$ and so $\mathfrak{p} \subseteq \mathfrak{q}$. From this it follows that A is at most $(d + 1)$-dimensional, so $\dim(A) = d + 1$.

The quotient ring $A_\mathfrak{p}$ is integrally closed and has one nonzero prime ideal. Moreover it is not a valuation ring if $k \neq k'$. In fact, let $x \in R$ be an element having residue in k' but not in k (as in (c)). Note that x is in the quotient field of $A_\mathfrak{p}$, which is K; but neither x nor x^{-1} has residue in k, so neither x nor x^{-1} is in $A_\mathfrak{p}$. Thus $A_\mathfrak{p}$ is not a valuation ring, and hence is an F-ring (Exercise 16.2.6(a) applied to $A_\mathfrak{p}$). It follows that $\mathfrak{p}A[X]$ is not minimal among nonzero prime ideals in $A[X]$. Now

$$A[X]/\mathfrak{p}A[X] \cong (A/\mathfrak{p})[X] \cong O[X]$$

so $A[X]$ is at least $(t + 2)$-dimensional (recall that is integral).

Finally, let $0 = \mathfrak{P}_0 \subset \mathfrak{P}_1 \subset \cdots \subset \mathfrak{P}_n$ be a chain of prime ideals in $A[X]$. Assume that the chain $0 \subset \mathfrak{P}_1$ is saturated; then $\mathfrak{P}_1 \cap A = 0$, as otherwise

$$\mathfrak{p} \subset \mathfrak{P}_1 \cap A \quad \text{and} \quad \mathfrak{p} \cdot A[X] \subset \mathfrak{P}_1.$$

Similarly one concludes that if the chain $0 \subset \mathfrak{P}_1 \subset \mathfrak{P}_2$ is saturated, then

$$\mathfrak{P}_2 \cap A = \mathfrak{p} \quad \text{and} \quad \mathfrak{P}_2 = \mathfrak{p}A[X]$$

(by Exercise 16.2.3, $\mathfrak{P}_2 \cap A$ can not be 0). From this it follows at once that $A[X]$ is at most $(t+2)$-dimensional.

We say an integral domain A is *of type* (d,t) if $\dim(A) = d$ and $\dim(A[X]) = t$. Now any field is of type $(0,1)$, and from the above construction we get an integrally closed domain of type $(1,3)$. Note that a Noetherian integrally closed domain is of type $(1,2)$. We now prove (d) by induction on d. So suppose by induction that for some d and each t (where $d+1 \le t \le 2d+1$), we have an integrally closed ring of type (d,t). Note that if $d+3 \le t \le 2d+3$, then $d+1 \le t-2 \le 2d+1$ and from an integrally closed ring of type $(d,t-2)$ we get an integrally closed ring of type (d,t). If on the other hand $t = d+2$, then a Noetherian integrally closed domain of dimension $d+1$ (for example the ring $k[X_1,\dots,X_{d+1}]$ where k is a field) is of type $(d+1,d+2)$, so the claim is proved. □

Exercise 16.2.8.

(a) Let A be an integral domain, K its fraction field and n an integer. Let $t_1,\dots,t_n$ be elements of K and $\varphi : A[X_1,\dots,X_n] \to A[t_1,\dots,t_n]$ the homomorphism such that $\varphi(X_i) = t_i$. Show that the height of the kernel of φ equals to n.

(b) Deduce that for any n-tuple $(t_1,\dots,t_n)$ of elements of K, we have

$$\dim(A[t_1,\dots,t_n]) \le \dim(A[X_1,\dots,X_n]) - n.$$

Exercise 16.2.9. Let A be an integral domain with fraction field K. Let $0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n$ be a chain of prime ideals of A. Show that there exists a valuation ring R of K and a chain of prime ideals $0 \subset \mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_n$ of R such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$.

Exercise 16.2.10. Let A be an integral domain and K its fraction field. For any integer $k \ge 0$, the following properties are equivalent:

(i) Any subring B of K containing A has dimension $\le k$.

(ii) Any valuation ring R of K containing A has dimension $\le k$.

(iii) For any k elements $(t_1,\dots,t_k)$ of K, we have $\dim(A[t_1,\dots,t_k]) \le k$.

(iv) We have $\dim(A[X_1,\dots,X_m]) \le k+m$ for any integer $m \ge 0$.

16.3 Dimension of Noetherian rings

16.3.1 Dimension of a quotient ring

Proposition 16.3.1. *Let A be a Noetherian integral domain, x a nonzero element of A and $\mathfrak{p}$ a minimal prime belonging to x. Then $\mathfrak{p}$ has height* 1.

Proof. Let $\mathfrak{q} \subset \mathfrak{p}$ be a prime ideal distinct from $\mathfrak{p}$. Then $x \notin \mathfrak{q}$ by the hypothesis on $\mathfrak{p}$. Since A is integral, $A_\mathfrak{p}$ is identified with a subring of $A_\mathfrak{q}$. For any positive integer n, we denote by $\mathfrak{q}_n$ the ideal $\mathfrak{q}^n A_\mathfrak{q} \cap A_\mathfrak{p}$ of $A_\mathfrak{p}$. The minimal property of $\mathfrak{p}$ means that the local ring $A_\mathfrak{p}/xA_\mathfrak{p}$ is 0-dimensional. It is therefore Artinian and by Proposition 6.3.7 there is a positive integer n_0 such that

$$\mathfrak{q}_n + xA_\mathfrak{p} = \mathfrak{q}_{n+1} + xA_\mathfrak{p} \quad \text{for} \quad n \ge n_0.$$

Let's now fix an integer $n \geq n_0$. Given $y \in \mathfrak{q}_n$, there exists $a \in A_\mathfrak{p}$ such that $y - ax \in \mathfrak{q}_{n+1}$. We then have $ax \in \mathfrak{q}_n$, whence $a \in \mathfrak{q}_n$ since $x \notin \mathfrak{q}$, and finally we have $y \in \mathfrak{q}_{n+1} + x\mathfrak{q}_n$. So we have proved that

$$\mathfrak{q}_n = \mathfrak{q}_{n+1} + x\mathfrak{q}_n.$$

As x belongs to the maximal ideal of the Noetherian local ring $A_\mathfrak{p}$, the Nakayama lemma shows that we have $\mathfrak{q}_n = \mathfrak{q}_{n+1}$. As $\mathfrak{q}_n A_\mathfrak{q} = (\mathfrak{q}A_\mathfrak{q})^n$, we conclude that

$$(\mathfrak{q}A_\mathfrak{q})^n = (\mathfrak{q}A_\mathfrak{q})^{n+1} \quad \text{for} \quad n \geq n_0.$$

Since $A_\mathfrak{q}$ is a local Noetherian ring, we have $\bigcap_n (\mathfrak{q}A_\mathfrak{q})^n = \{0\}$ by Corollary 11.4.16, whence $(\mathfrak{q}A_\mathfrak{q})^{n_0} = 0$ and the prime ideal $\mathfrak{q}A_\mathfrak{q}$ of $A_\mathfrak{q}$ reduces to 0. Then we must have $\mathfrak{q} = 0$ and therefore $\mathfrak{p}$ has height 1. □

Lemma 16.3.2. *Let A be a Noetherian ring, $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_n$ a chain of prime ideals of A and x an element of $\mathfrak{p}_n$. Then there exists a chain $\mathfrak{p}'_0 \subset \cdots \subset \mathfrak{p}'_n$ of prime ideals of A such that $\mathfrak{p}'_0 = \mathfrak{p}_0$, $\mathfrak{p}'_n = \mathfrak{p}_n$, and $x \in \mathfrak{p}'_1$.*

Proof. We prove by induction. The case $n = 1$ is trivial, so suppose $n \geq 2$ and that x does not belong to $\mathfrak{p}_{n-1}$ (otherwise we can apply to $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_{n-1}$ the induction hypothesis). Let $\mathfrak{p}'_{n-1}$ be a minimal element of the set of prime ideals of A contained in $\mathfrak{p}'_n = \mathfrak{p}_n$ and containing $\mathfrak{p}_{n-2} + Ax$. According to Proposition 16.3.1, the ideal $\mathfrak{p}'_{n-1}/\mathfrak{p}_{n-2}$ of the ring $A/\mathfrak{p}_{n-2}$ is of height 1, and since $\mathfrak{p}_{n-2} \subset \mathfrak{p}_{n-1} \subset \mathfrak{p}_n$ is a chain of length 2, so is $\mathfrak{p}_{n-2} \subset \mathfrak{p}'_{n-1} \subset \mathfrak{p}'_n$. Since now $x \in \mathfrak{p}'_{n-1}$, the induction hypothesis applied to the chain $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}'_{n-1}$ shows that there is a chain $\mathfrak{p}'_0 \subset \cdots \subset \mathfrak{p}'_{n-1}$ with $x \in \mathfrak{p}'_1$ and $\mathfrak{p}'_0 = \mathfrak{p}_0$. The chain

$$\mathfrak{p}'_0 \subset \cdots \subset \mathfrak{p}'_{n-1} \subset \mathfrak{p}'_n$$

then satisfies the requirements. □

Proposition 16.3.3. *Let A be a Noetherian ring and $\mathfrak{a}$ an ideal contained in the Jacobson radical of A and generated by m elements. Then we have*

$$\dim(A/\mathfrak{a}) \leq \dim(A) \leq \dim(A/\mathfrak{a}) + m.$$

Proof. The inequality $\dim(A/\mathfrak{a}) \leq \dim(A)$ is clear. By induction it suffices to prove the inequality

$$\dim(A) \leq \dim(A/xA) + 1$$

for any element x contained in the Jacobson radical of A. That is, to show that $\dim(A/xA) \geq n - 1$ for any chain $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_n$ of prime ideals of A. Now since x is in the Jacobson radical of A, we may assume that $x \in \mathfrak{p}_n$. Then it suffices to construct a chain $\mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_n$ of prime ideals of A, with $x \in \mathfrak{q}_1$ and this follows from Lemma 16.3.2. □

Corollary 16.3.4.

(a) Every Noetherian semilocal ring is of finite dimension.

(b) Let A be a Noetherian ring. Then every proper ideal of A has finite height.

(c) *Any decreasing sequence of prime ideals of a Noetherian ring A is stationary.*

Proof. Let A be a Noetherian semilocal ring and $\mathfrak{r}$ its Jacobson radical. The quotient ring $A/\mathfrak{r}$ is then of dimension 0 by Proposition 10.1.5. If the ideal $\mathfrak{r}$ is generated by m elements, then we have $\dim(A) \leq m$ by Proposition 16.3.3.

Let A be Noetherian and $\mathfrak{a}$ a proper ideal of A. Let $\mathfrak{m}$ be a maximal ideal of A containing A, then $0 \leq \mathrm{ht}(\mathfrak{a}) \leq \dim(A_{\mathfrak{m}})$. Since $A_{\mathfrak{m}}$ is a Noetherian local ring, we have $\dim(A_{\mathfrak{m}}) < +\infty$ by (a), whence (b) follows.

Finally, any finite strictly decreasing sequence $(\mathfrak{p}_i)_{1\leq i\leq n}$ of prime ideals of a Noetherian ring A defines a chain $\mathfrak{p}_n \subset \cdots \subset \mathfrak{p}_0$, hence $n < \dim(A_{\mathfrak{p}_0}) < +\infty$ and (c) follows. □

Corollary 16.3.5. *Let A be a Noetherian local ring.*

(a) *Let $x \in \mathfrak{m}_A$. Then* $\dim(A) - 1 \leq \dim(A/xA) \leq \dim(A)$, *and* $\dim(A/xA) = \dim(A) - 1$ *if and only if x does not belong to any of the minimal prime ideals $\mathfrak{p}$ of A such that* $\dim(A/\mathfrak{p}) = \dim(A)$, *and it suffices that x is not a zero divisor in A.*

(b) *Let $\mathfrak{a}$ be a proper ideal of A such that* $\dim(A/\mathfrak{a}) < \dim(A)$. *Then there exists $x \in \mathfrak{a}$ such that* $\dim(A/xA) = \dim(A) - 1$.

(c) *If* $\dim(A) \geq 1$, *then there exists $x \in \mathfrak{m}_A$ such that* $\dim(A/xA) = \dim(A) - 1$.

Proof. By Proposition 16.3.3, we see $\dim(A) - 1 \leq \dim(A/xA) \leq \dim(A)$. For $\dim(A/xA) = \dim(A) = n$, it is necessary and sufficient that there exists a chain $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_n$ such that $x \in \mathfrak{p}_0$, and this is equivalent to say there exists a prime ideal $\mathfrak{p}_0$ containing x such that $\dim(A/\mathfrak{p}_0) = \dim(A)$. But such an ideal prime $\mathfrak{p}_0$ is necessarily minimal, and any element of $\mathfrak{p}_0$ is therefore a divisor of 0 in A. This proves (a).

Let Φ be the set of minimal prime ideals of A, and Φ' the subset $\mathfrak{p} \in \Phi$ such that $\dim(A) = \dim(A/\mathfrak{p})$. Since A is Noetherian, Φ is finite. Let $\mathfrak{a}$ be a proper ideal such that $\dim(A/\mathfrak{a}) < \dim(A)$. Then for every $\mathfrak{p} \in \Phi'$ we have $\dim(A/\mathfrak{a}) < \dim(A/\mathfrak{p})$, whence $\mathfrak{a} \not\subseteq \mathfrak{p}$. Then by Proposition 10.1.4, there exists $x \in \mathfrak{a}$ such that $x \notin \mathfrak{p}$ for all $\mathfrak{p} \in \Phi'$, and therefore $\dim(A/xA) = \dim(A) - 1$ by (a), whence (b). Now (c) follows from (b) by taking $\mathfrak{a} = \mathfrak{m}_A$. □

Example 16.3.6. The claim in Proposition 16.3.1 fails if A is not Noetherian. For example, let A be a valuation ring of dimension $d \geq 2$. Then the prime ideals of A form a chain of length d:

$$0 = \mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_d = \mathfrak{m}_A.$$

Therefore, for each i, there exists $x_i \in \mathfrak{p}_i \setminus \mathfrak{p}_{i-1}$, and it is easy to see $\mathfrak{p}_i$ is the only minimal prime belonging to x_i.

16.3.2 Dimension and secant sequences

Let A be a Noetherian, M a finitely generated A-module, S a subset of A contained in the Jacobson radical of A. Let I be the ideal generated by S and $\mathfrak{a}$ the annihilator of M. Then we have

$$\dim_A(M) = \dim(A/\mathfrak{a}) \leq \dim(A). \tag{3.2.1}$$

Moreover, the support of the A-module M/SM is equal to $V(\mathfrak{a}+I)$ by Corollary 10.4.38, hence

$$\dim_A(M/SM) = \dim(A/(\mathfrak{a}+I)). \tag{3.2.2}$$

By Proposition 16.3.3, we then have the following inequality

$$\dim_A(M/SM) \leq \dim_A(M) \leq |S| + \dim_A(M/SM). \tag{3.2.3}$$

Definition 16.3.7. *Let A be a Noetherian local ring and S a subset of $\mathfrak{m}_A$. Then S is said to be* ***secant for M*** *if*

$$\dim_A(M) = \dim_A(M/SM) + |S|. \tag{3.2.4}$$

A family $(x_i)_{i\in I}$ of element of $\mathfrak{m}_A$ is said to be ***secant for M*** *if*

$$\dim_A(M) = |I| + \dim(M/\sum x_i M)$$

and an element $x \in \mathfrak{m}_A$ is called secant for M if $\{x\}$ is secant for M.

By definition, if $\mathfrak{a}$ is the annihilator of M, then a subset S of $\mathfrak{m}_A$ is secant for M if and only if it is secant for the A-module $A/\mathfrak{a}$. Also note that, since A is Noetherian and local, we have $\dim(A) < +\infty$, so if S is M-secant then S is finite.

Proposition 16.3.8. *Let A be a Noetherian local ring, M a finitely generated A-module, and S, S' two disjoint subsets of $\mathfrak{m}_A$. Then the set $S \cup S'$ is secant for M if and only if S is secant for M and S' is secant for $M' = M/SM$.*

Proof. For this, we first observe that

$$M/(SM + S'M) = (M/SM)/((SM + S'M)/SM) = M'/S'M'$$

and therefore

$$\dim_A(M/(SM + S'M)) = \dim_A(M'/S'M') \geq \dim_A(M') - |S'| \geq \dim_A(M) - |S| - |S'|.$$

This proves the claim by the definition of secanteness. □

Corollary 16.3.9. *Let A be a Noetherian local ring and $x_1, \ldots, x_r$ be distinct elements of $\mathfrak{m}_A$. Define $M_1 = M$ and $M_{i+1} = M_i/x_iM_i$. Then the following conditions are equivalent.*

(i) The sequence $(x_1, \ldots, x_r)$ is M-secant.

(ii) The element x_i is M_i-secant for each i.

(iii) The element x_i is $M/(x_1M + \cdots + x_{i-1}M)$-secant for each i.

Proof. The equivalence of (i) and (ii) follows by applying Proposition 16.3.8 on the subsets $\{x_1\}, \ldots, \{x_n\}$, and that of (i) and (iii) follows similarly. □

Proposition 16.3.10. *Let A be a Noetherian local ring, M a finitely generated A-module, $x_1, \ldots, x_r$ elements of $\mathfrak{m}_A$ and $n_1, \ldots, n_r$ integers. Then the sequence $(x_1, \ldots, x_r)$ is secant for M if and only if the sequence $(x_1^{n_1}, \ldots, x_r^{n_r})$ is secant for M.*

Proof. We may reduce the case $r = 1$, so let $x \in \mathfrak{m}_A$ and n be a positive integer. If $\mathfrak{a}$ is the annihilator of M, then by Corollary 10.4.38,

$$\operatorname{supp}(M/xM) = V(\mathfrak{a}) \cap V(x), \quad \operatorname{supp}(M/x^n M) = V(\mathfrak{a}) \cap V(x^n).$$

By Proposition 10.4.3 we have $V(x^n) = V(x)$, whence the proposition. □

Proposition 16.3.11. *Let A be a Noetherian local ring and M a finitely generated A-module. For an element x in $\mathfrak{m}_A$ to be secant for M, it is necessary and sufficient that it does not belong to any minimal elements $\mathfrak{p}$ of* $\operatorname{supp}(M)$ *such that* $\dim(A/\mathfrak{p}) = \dim_A(M)$*, and it suffices that the homothety h_x with ratio x on M be injective.*

Proof. Let $\mathfrak{a}$ be the annihilator of M. Then x is secant for M means it is secant for $A/\mathfrak{a}$, and if h_x is injective on M, then x is not a zero divisor of $A/\mathfrak{a}$. The claim now follows from Corollary 16.3.5 applying to the ring $A/\mathfrak{a}$. □

Remark 16.3.1. A sequence $(x_1, \dots, x_r)$ is said to be **regular for M** (or an **M-regular sequence**) if for each i, the element x_i is not a zerodivisor on $M/(x_1M + \cdots + x_{i-1}M)$. By Corollary 16.3.9 and Proposition 16.3.11, it follows that every regular sequence for M is secant for M.

Theorem 16.3.12. *Let A be a Noetherian local ring, M a finitely generated A-module, and S a subset of $\mathfrak{m}_A$.*

(a) If M/SM has finite length, then $|S| \geq \dim_A(M)$.

(b) If S is secant for M, then $|S| \leq \dim_A(M)$.

(c) Any secant subset for M is contained in a maximal secant subset for M.

(d) The following conditions are equivalent:

(i) S is a maximal secant sequence for M;

(ii) S is a secant sequence for M and $|S| = \dim_A(M)$;

(iii) M/SM has finite length and $|S| = \dim_A(M)$;

(iv) S is a secant sequence for M and M/SM has finite length.

Proof. Since $S \subseteq \mathfrak{m}_A$, by Nakayama lemma we have $M/SM \neq 0$, whence $\dim_A(M/SM) \geq 0$ with equality if and only if M/SM is of finite length. Assertions (a) and (b) then follows from (3.2.3) and (3.2.4), as well as the equivalences of (ii), (iii), and (iv) in (d).

By (a), any secant subset for M with cardinality $\dim_A(M)$ is maximal. It remains to prove that, if S is secant for M and if $|S| < \dim_A(M)$, then S is not not maximum. Let $\mathfrak{a}$ be the annihilator of M, and B the local Noetherian ring $A/(\mathfrak{a} + I)$, where I is the ideal generated by S. According to Corollary 16.3.5(c), there exists an element x of $\mathfrak{m}_A$ such that $\dim(B/xB) = \dim(B) - 1$, whence $x \notin S$. According to Proposition 16.3.8, the subst $S \cup \{x\}$ of $\mathfrak{m}_A$ is secant for $A/\mathfrak{a}$, hence for M. This proves assertion (c), and the equivalence of (i) and (ii) in (d). □

Corollary 16.3.13. *Let A be a Noetherian local ring, M a finitely generated A-module. Then the dimension of M is the smallest of the positive integers d for which it d there exists a sequence $(x_1, \dots, x_d)$ of elements of $\mathfrak{m}_A$ such that the A-module $M/\sum_i x_i M$ is of finite length.*

Proof. As $\varnothing$ is a secant subset for M, Theorem 16.3.12(c) shows the existence of a secant sequence for M, say $(x_1, \dots, x_d)$. But then $d = \dim_A(M)$ and the A-module $M/\sum_i x_i M$ is of finite length by property (iii) of Theorem 16.3.12(d). Conversely if $(x_1, \dots, x_{d'})$ is a sequence of elements of $\mathfrak{m}_A$ such that the A-module of $M/\sum_i x_i M$ is of finite length, we have $d' \geq \dim_A(M)$ according to Theorem 16.3.12(a). □

If $\dim_A(M) = d$, then a sequence $(x_1, \dots, x_d)$ of elements of $\mathfrak{m}_A$ such that $M/\sum_i x_i M$ is of finite length is called a **system of parameters** for M. Note that such a sequence must be secant for M, by (iii) of Theorem 16.3.12(d).

Let A be a Noetherian local ring and $\mathfrak{m}_A$ be its maximal ideal. Endow A with its $\mathfrak{m}_A$-adic topology, recall that an ideal $\mathfrak{a}$ of A is called a **defining ideal** of A if the $\mathfrak{a}$-adic topology coincides with its $\mathfrak{m}_A$-adic topology.

Proposition 16.3.14. *Let A be a Noetherian local ring and $\mathfrak{a}$ an ideal of A. Then the following conditions are equivalent.*

(i) *$\mathfrak{a}$ is a defining ideal of A.*

(ii) *$\mathfrak{a}$ is $\mathfrak{m}_A$-primary.*

(iii) *There exist a positive integer n such that $\mathfrak{m}_A^n \subseteq \mathfrak{a} \subseteq \mathfrak{m}_A$.*

(iv) *$\mathfrak{a}$ is a proper ideal and $A/\mathfrak{a}$ is an A-module of finite legnth.*

Proof. By Example 12.2.2, we see (ii) and (iii) are equivalent, also (i) is equivalent to (iii) by the definition of adic topologies and the fact that $\mathfrak{m}_A$ is a prime ideal. Finally, the equivalence of (i) and (iv) follows from Proposition 12.2.14 and $\operatorname{supp}(A/\mathfrak{a}) = V(\mathfrak{a})$. □

Corollary 16.3.15. *The dimension of a local Noetherian ring A is the smallest of the positive integers d for which there exists a defining ideal of A generated by d elements.*

Proof. This follows from Corollary 16.3.13 and Proposition 16.3.14. □

Let A be a ring and $X = \operatorname{Spec}(A)$ be its spectrum. A closed subset of the form $V(x)$ with $x \in A$ of X is called a **hypersurface** of X.

Proposition 16.3.16. *Let A be a Noetherian ring, Y be a closed subset of $X = \operatorname{Spec}(A)$, $H_1, \dots, H_m$ be hypersurfaces of X, and $\tilde{Y} = Y \cap H_1 \cap \cdots \cap H_m$.*

(a) *For any closed subset V of Y contained in $\tilde{Y}$, we have $\operatorname{codim}(V, \tilde{Y}) \geq \operatorname{codim}(V, Y) - m$.*

(b) *For any irreducible componenet Z subset of $\tilde{Y}$, we have $\operatorname{codim}(Z, Y) \leq m$.*

(c) *If Z is an irreducible closed subset of X contained in Y such that $\operatorname{codim}(Z, Y) \leq m$, there are hypersurfaces $\tilde{H}_1, \dots, \tilde{H}_m$ such that Z is an irreducible component of $Y \cap \tilde{H}_1 \cdots \cap \tilde{H}_m$.*

Proof. Let $\mathfrak{a}$ be an ideal of A and $x_1, \dots, x_m$ be elements of A such that $Y = V(\mathfrak{a})$ and $H_i = V(x_i)$ for each i. Let $V(\mathfrak{p})$ be an irreducible closed subset contained in Y, where $\mathfrak{p}$ is a prime ideal of A containing $\mathfrak{a}$. Suppose first that Z is contained in $\tilde{Y}$ and denote by ξ_i the image of x_i in the Noetherian local ring $B = A_\mathfrak{p}/\mathfrak{a}A_\mathfrak{p}$. According to Proposition 16.1.5, we have

$$\operatorname{codim}(Z, Y) = \dim(B), \quad \operatorname{codim}(Z, \tilde{Y}) = \dim(B/(\xi_1 B + \cdots + \xi_m B))$$

so by Proposition 16.3.3 we have

$$\operatorname{codim}(Z, \tilde{Y}) \geq \operatorname{codim}(Z, Y) - m. \tag{3.2.5}$$

If Z is an irreducible component of $\tilde{Y}$, we have $\operatorname{codim}(Z, \tilde{Y}) = 0$, whence $\operatorname{codim}(Z, Y) \leq m$. This proves (b), and (a) follows by taking in both sides of (3.2.5) the lower bound on the set of irreducible components Z of V.

Conversely, suppose that we have $\operatorname{codim}(Z, Y) \leq m$, ie, $\dim(B) \leq m$. As any element of $A_{\mathfrak{p}}$ is the product of an invertible element of $A_{\mathfrak{p}}$ by the image of an element of A, Corollary 16.3.15 demonstrates the existence of elements $\tilde{x}_1, \ldots, \tilde{x}_m$ of A whose images in B generate a defining ideal of B. Set $\tilde{H}_i = V(\tilde{x}_i)$, it is then clear that Z is an irreducible component of $Y \cap \tilde{H}_1 \cap \cdots \cap \tilde{H}_m$. □

Corollary 16.3.17 (Krull's Hauptidealsatz). *Let A be a Noetherian ring and $x_1, \ldots, x_m$ be elements of A.*

(a) For any prime ideal $\mathfrak{p}$ belonging to $Ax_1 + \cdots + Ax_m$, we have $\operatorname{ht}(\mathfrak{p}) \leq m$.

(b) If $\mathfrak{p}$ is a prime ideal of A such that $\operatorname{ht}(\mathfrak{p}) \leq m$, then there exist elements $\tilde{x}_1, \ldots, \tilde{x}_m$ of A such that $\mathfrak{p}$ is a minimal prime belonging to $A\tilde{x}_1 + \cdots + A\tilde{x}_m$.

Proof. This is a reformulation of Proposition 16.3.16 in the case $Y = X$. □

Corollary 16.3.18. *Let A be a Noetherian ring and H be a hypersurface of $X = \operatorname{Spec}(A)$. Then the codimension of H in X is equal to 0 or 1. We have $\operatorname{codim}(H, X) = 1$ if and only if H does not contain any irreducible component of X. If so, all the irreducible components of H are of codimension 1 in X.*

Proof. By Proposition 16.3.16 we have $\operatorname{codim}(H, X) \leq 1$, and we have $\operatorname{codim}(H, X) = 0$ if and only if H contains an irreducible component of X. By definition,

$$\operatorname{codim}(H, X) = \inf_Z \operatorname{codim}(Z, X)$$

where Z runs through the set of irreducible components of H. The claim then follows from these remarks. □

Corollary 16.3.19. *Let A be a Noetherian ring, Y be an irreducible closed subset of $X = \operatorname{Spec}(A)$, and H a hypersurface in X. Then only three cases are possible:*

(a) $Y \subseteq H$;

(b) $Y \cap H$ is nonempty and each of its irreducible components satisfies $\operatorname{codim}(Z, X) = 1$;

(c) $Y \cap H$ is empty.

Proof. Suppose that $Y \cap H$ is nonempty and is not equal to Y. Then any irreducible component Z of $Y \cap H$ satisfies $\operatorname{codim}(Z, Y) \leq 1$ by Proposition 16.3.16. Since Z and Y are both irreducible closed subsets, $\operatorname{codim}(Z, Y) = 0$ iff $Y = Z$, which is impossible. □

Corollary 16.3.20. *If A is a Noetherian UFD, then the prime ideals of height 1 of A are the principal ideals generated by the irreducible elements of A. If moreover A is local, we have $\dim(A/\mathfrak{p}) = \dim(A) - 1$ for any prime ideal $\mathfrak{p}$ of height 1 of A.*

Proof. Let x be an irreducible element of A. Then Ax is a prime ideal because x is prime, of height 1 because A is integral. Let $\mathfrak{p}$ be a prime ideal of height 1 of A. Then $V(\mathfrak{p})$ is an irreducible component of a hypersurface $V(x)$ for some x (Proposition 16.3.16). Let $x = \prod_i p_i^{n_i}$ be a decomposition of x into products of irreducible elements. Then the irreducible components of $V(x)$ is the $V(p_i)$, so $\mathfrak{p} = Ap_i$ for some i. The last statement follows from Corollary 16.3.5. □

Proposition 16.3.21. *Let A be a Noetherian ring and $\mathfrak{p} \subset \mathfrak{q}$ be an unsaturated chain of prime ideals of A. Then the set E of prime ideals $\mathfrak{r}$ of A such that $\mathfrak{p} \subset \mathfrak{r} \subset \mathfrak{q}$ is infinite and we have*

$$\bigcap_{\mathfrak{r}\in E} \mathfrak{r} = \mathfrak{p}, \quad \bigcup_{\mathfrak{r}\in E} \mathfrak{r} = \mathfrak{q}.$$

Proof. By passing to the quotient ring, we may assume that $\mathfrak{p} = \{0\}$. Now by Lemma 16.3.2 we have $\bigcup_{\mathfrak{r}\in E} \mathfrak{r} = \mathfrak{q}$, and it follows from Proposition 10.1.4 that E is infinite.

Now let y be a nonzero element in $\bigcap_{\mathfrak{r}\in E} \mathfrak{r}$. Since the height of $\mathfrak{q}$ is finite by Corollary 16.3.4, by localization at a prime ideal of height 2, we may assume that $\mathrm{ht}(\mathfrak{q}) = 2$. Then the ring A/yA has dimension 1, hence each prime ideal $\mathfrak{r} \in E$ is minimal. But a Noetherian ring can have only finitely many minimal prime ideals, a contradiction. Therefore $\bigcap_{\mathfrak{r}\in E} \mathfrak{r} = \{0\}$, and the proof is finished. □

Proposition 16.3.22. *Let A be a Noetherian ring with dimension ≥ 2, and h an integer such that $0 < h < \dim(A)$.*

(a) The ring A has infinitely many prime ideals of A with height h.

(b) If A is of finite dimension, then there are infinitely many prime ideals $\mathfrak{p}$ such that $\mathrm{ht}(\mathfrak{p}) = h$, $\mathrm{coht}(\mathfrak{p}) = \dim(A) - h$.

Proof. Since a Noetherian local ring has finite dimension, each prime ideal of A has finite height. Since $h < \dim(A)$, there exist an integer $n > h$, a prime ideal $\mathfrak{p}$ with $\mathrm{ht}(\mathfrak{p}) = n$, and a chain $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_n = \mathfrak{p}$ of prime ideals of A. Then $\mathrm{ht}(\mathfrak{p}_i) = i$ for each i, so $\mathrm{ht}(\mathfrak{r}) = h$ for every prime ideal $\mathfrak{r}$ such that $\mathfrak{p}_{h-1} \subset \mathfrak{r} \subset \mathfrak{p}_{h+1}$. By Proposition 16.3.21 the set E of such prime ideals $\mathfrak{r}$ is infinite, whence (a).

If A is of finite dimension, then we may take $n = \dim(A)$ in the above proof. Then for each $\mathfrak{r} \in E$, we have $\mathrm{ht}(\mathfrak{r}) = h$ and $\mathrm{coht}(\mathfrak{r}) \leq n - h$. Since $\mathfrak{r} \subset \mathfrak{p}_{h+1} \subset \cdots \subset \mathfrak{p}_n$ is a chain of length $n - h$, we then get $\mathrm{coht}(\mathfrak{r}) = \dim(A) - h$. □

Example 16.3.23. There exist non-Noetherian integral domains of dimension 2 with only one prime ideal of height 1, for example the ring of a valuation of rank 2.

16.3.3 Extension of scalars

Proposition 16.3.24. *Let $\rho : A \to B$ be a local homomorphism of Noetherian local rings, M a finitely generated A-module and N a finitely generated B-module. If $\overline{B} = B \otimes_A \kappa_A$ and $\overline{N} = N \otimes_B \overline{B}$, then*

$$\dim_B(M \otimes_A N) \leq \dim_A(M) + \dim_{\overline{B}}(\overline{N})$$

and the equality holds if N is flat over A.

Proof. Let $S \subseteq \mathfrak{m}_A$ be a system of parameters for the A-module M and $T \subseteq \mathfrak{m}_B$ a system of parameters for the $\overline{B}$-module $\overline{N}$. Let E be the B-module $M \otimes_A N$. Since ρ is local, we have $\rho(S) \subseteq \mathfrak{m}_B$, and

$$\begin{aligned} E/(\rho(S)E + TE) &= E \otimes_B (B/(\rho(S)B + TB)) = M \otimes_A N \otimes_B (B/TB) \otimes_A (A/SA) \\ &= M \otimes_A (A/SA) \otimes_A N \otimes_B (B/TB) = (M/SM) \otimes_A (N/TN) \end{aligned}$$

Moreover, by Proposition 12.2.14, we have

$$\operatorname{supp}(M/SM) = \{\mathfrak{m}_A\}, \quad \operatorname{supp}(\overline{N}/T\overline{N}) = \{\mathfrak{m}_B\}$$

which implies, according to Proposition 10.4.37 and 10.4.40, that

$$\begin{aligned} \operatorname{supp}((M/SM) \otimes_A (N/TN)) &= \operatorname{supp}(N/TN) \cap \rho^{*-1}(\{\mathfrak{m}_A\}) \\ &= \operatorname{supp}((N/TN) \otimes_A \kappa_A) = \operatorname{supp}(\overline{N}/T\overline{N}) = \{\mathfrak{m}_B\}. \end{aligned}$$

Therefore the B-module $E/(\rho(S)E + TE)$ has finite length, which implies by Theorem 16.3.12 that

$$\dim_B(E) \leq |S| + |T| = \dim_A(B) + \dim_{\overline{B}}(\overline{N}).$$

Suppose now that N is flat over A. Let $\mathfrak{a}$ (resp. $\mathfrak{b}$) be the annihilator of M (resp. N). Then we have

$$\operatorname{supp}(E) = \operatorname{supp}(N) \cap \rho^{*-1}(\operatorname{supp}(N)) = V(\mathfrak{b}) \cap \rho^{*-1}(V(\mathfrak{a})) = V(\mathfrak{b} + \mathfrak{a}B),$$

and therefore $\dim_B(M \otimes_A N) = \dim(B/(\mathfrak{b} + \mathfrak{a}B))$. On the other hand,

$$\dim_A(M) + \dim_{\overline{B}}(\overline{N}) = \dim(A/\mathfrak{a}) + \dim(B/(\mathfrak{b} + \mathfrak{m}_A B)).$$

Let $A' = A/\mathfrak{a}$ and $B' = B/(\mathfrak{b} + \mathfrak{a}B)$ and let $\rho' : A' \to B'$ be the local homomorphism deduced from ρ by passing to quotients. Since the annihilator of N is $\mathfrak{b}$, N is a finitely generated $B/\mathfrak{b}$-module with support $\operatorname{Spec}(B/\mathfrak{b})$, and flat on A. By Proposition 10.4.37 and Example 7.3.19, the local homomorphism $A \to B/\mathfrak{b}$ deduced from ρ therefore has the property (PM). By extension of the scalars, we deduce that ρ' has the property (PM). According to Proposition 16.2.2, we have

$$\dim(B') \geq \dim(A') + \dim(B'/\mathfrak{m}_{A'}B')$$

and as the ring $B'/\mathfrak{m}_{A'}B'$ is isomorphic to $B/(\mathfrak{b} + \mathfrak{m}_A B)$, our assertion follows. □

Corollary 16.3.25. *Let $\rho : A \to B$ be a local homomorphism of Noetherian local rings.*

(a) We have $\dim(B) \leq \dim(A) + \dim(B \otimes_A \kappa_A)$, and the equality holds if B is flat over A.

(b) Suppose that B is flat over A, then a subset S of $\mathfrak{m}_A$ is secant for A if and only if $\rho(S)$ is secant for B.

Proof. The assertion in (a) follows from Proposition 16.3.24, by setting $M = A$, $N = B$. For (b), if B is flat over A, then

$$\dim(B) = \dim(A) + \dim(\overline{B})$$

where $\overline{B} = B \otimes_A \kappa_A$. Since ρ is injective by Proposition 7.3.15, we have $|\rho(S)| = |S|$. Finally $B' = B/\rho(S)B$ is a flat module on $A' = A/SA$, hence

$$\dim(B') = \dim(A') + \dim(\overline{B})$$

since $B'/\mathfrak{m}_{A'}B'$ is isomorphic to $\overline{B}$. The claim in (b) then follows from these equalities. □

Corollary 16.3.26. *Let $\rho : A \to B$ be a ring homomorphism of Noetherian rings. Then*

$$\dim(B) \leq \dim(A) + \sup_{\mathfrak{p}\in\operatorname{Spec}(A)} \dim(B \otimes_A \kappa(\mathfrak{p})).$$

Proof. Let $\mathfrak{P}$ be a prime ideal of B and $\mathfrak{p} = \mathfrak{P}^c$. By Corollary 16.3.25, we have

$$\dim(B_{\mathfrak{P}}) \leq \dim(A_{\mathfrak{p}}) + \dim(B_{\mathfrak{P}} \otimes_A \kappa(\mathfrak{p})) \leq \dim(A) + \dim(B \otimes_A \kappa(\mathfrak{p}))$$

takign supremum on $\mathfrak{P}$, we get the claim. □

Corollary 16.3.27. *Let $\rho : A \to B$ be a ring homomorphism of Noetherian rings and $\mathfrak{p} \subset \mathfrak{q}$ be prime ideals of A.*

(a) If the going-up property holds for ρ, then

$$\dim(B \otimes_A \kappa(\mathfrak{p})) \leq \dim(B \otimes_A \kappa(\mathfrak{q})).$$

(b) If the going-down property holds for ρ, then

$$\dim(B \otimes_A \kappa(\mathfrak{p})) \geq \dim(B \otimes_A \kappa(\mathfrak{q})).$$

Proof. First assume the going-up property for ρ. Let $\mathfrak{P}_0 \subset \cdots \subset \mathfrak{P}_r$ be a chain of prime ideals of B lying over $\mathfrak{p}$ and $\mathfrak{p} = \mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_s = \mathfrak{q}$ be a chain of prime ideals of A. Then by the going-up property, there is a chain $\mathfrak{P}_r \subset \cdots \subset \mathfrak{P}_{r+s}$ of prime ideals of B such that $\mathfrak{P}_{r+i}^c = \mathfrak{p}_i$. If $\mathfrak{Q} := \mathfrak{P}_{r+s}$, then $\mathfrak{Q}$ is lying over $\mathfrak{q}$ and $\operatorname{ht}(\mathfrak{Q}/\mathfrak{p}^e) \geq r + s$. Applying Corollary 16.3.26 to the homomorphism $(A/\mathfrak{p})_{\mathfrak{q}} \to (B/\mathfrak{p}^e)_{\mathfrak{Q}}$, we get

$$r + s \leq \operatorname{ht}(\mathfrak{Q}/\mathfrak{p}^e) \leq \operatorname{ht}(\mathfrak{q}/\mathfrak{p}) + \dim(B_{\mathfrak{Q}}/\mathfrak{q}B_{\mathfrak{Q}}) \leq s + \dim(B \otimes_A \kappa(\mathfrak{q}))$$

whence the claim in (a).

Now we prove (b), so assume the going down property for ρ. We may assume that $\operatorname{ht}(\mathfrak{q}/\mathfrak{p}) = 1$, and it is enough to prove that, given a chain $\mathfrak{Q}_0 \subset \cdots \subset \mathfrak{Q}_t$ of prime ideals of B lying over $\mathfrak{q}$ such that $\operatorname{ht}(\mathfrak{Q}_i/\mathfrak{Q}_{i-1}) = 1$, we can construct a chain of prime ideals $\mathfrak{P}_0 \subset \cdots \subset \mathfrak{P}_t$ of B lying over $\mathfrak{p}$ such that $\mathfrak{P}_i \subset \mathfrak{Q}_i$ and $\operatorname{ht}(\mathfrak{P}_i/\mathfrak{P}_{i-1}) = 1$ for all i.

The existence of $\mathfrak{P}_0$ is guaranteed by the going-down property, and if $\mathfrak{P}_0, \ldots, \mathfrak{P}_i$ is constructed, take $x \in \mathfrak{q} \setminus \mathfrak{p}$ and let $\mathfrak{T}_1, \ldots, \mathfrak{T}_s$ be the minimal prime ideals belonging to $\mathfrak{P}_i + xB$. Then by Proposition 16.3.1 we have $\operatorname{ht}(\mathfrak{T}_j/\mathfrak{P}_i) = 1$, while $\operatorname{ht}(\mathfrak{Q}_{i+1}/\mathfrak{P}_i) \geq 2$, so there exists an element $y \in \mathfrak{Q}_{i+1} \setminus \bigcup_{j=1}^s \mathfrak{T}_j$. Let $\mathfrak{P}_{i+1}$ be a minimal prime ideal of $\mathfrak{P}_i + yB$, then $\mathfrak{P}_{i+1} \neq \mathfrak{T}_j$ for all j and Proposition 16.3.1 shows that $\operatorname{ht}(\mathfrak{P}_{i+1}/\mathfrak{P}_i) = 1$, hence $\rho(x) \notin \mathfrak{P}_{i+1}$. Since $x \in \mathfrak{q}$ and $\operatorname{ht}(\mathfrak{q}/\mathfrak{p}) = 1$, we must have $\mathfrak{P}_{i+1}^c = \mathfrak{p}$, which finishes the induction process. □

Corollary 16.3.28. *Let A be a Noetherian ring and n a positive integer. Then*

$$\dim(A[X_1, \dots, X_n]) = \dim(A) + n.$$

Proof. Let $B = A[X_1, \dots, X_n]$, then for any prime ideal $\mathfrak{p}$ of A, $B \otimes_A \kappa(\mathfrak{p})$ is identified with the polynomial ring on $\kappa(\mathfrak{p})$ with indeterminates $X_1, \dots, X_n$, whence of dimension n. By Corollary 16.3.26 we then have $\dim(B) \leq \dim(A) + n$, and the reverse inequality is already established. □

Corollary 16.3.29. *Let $\rho : A \to B$ be a homomorphism of Noetherian rings and $\rho^* : \operatorname{Spec}(B) \to \operatorname{Spec}(A)$ be the induced map.*

(a) If ρ^* is surjective, then $\operatorname{ht}(\mathfrak{a}^e) \leq \operatorname{ht}(\mathfrak{a})$ for any ideal $\mathfrak{a}$ of A.

(b) If B is a faithfully flat A-module, then $\operatorname{ht}(\mathfrak{a}^e) = \operatorname{ht}(\mathfrak{a})$ for any ideal $\mathfrak{a}$ of A.

Proof. If B is faithfully flat, then ρ^* is surjective by Corollary 10.2.41 and we have $\operatorname{ht}(\mathfrak{a}) \leq \operatorname{ht}(\mathfrak{a}^e)$ by Proposition 7.3.20. Therefore it suffices to prove assertion (a). Assume that ρ^* is surjective and let $\mathfrak{p}$ be a prime ideal of A containing $\mathfrak{a}$ such that $\operatorname{ht}(\mathfrak{p}) = \operatorname{ht}(\mathfrak{a})$. Let $\mathfrak{P}$ be a prime ideal of B lying over $\mathfrak{p}$ whose image in $B \otimes \kappa(\mathfrak{p})$ is minimal. Then $\dim(B_{\mathfrak{P}} \otimes \kappa(\mathfrak{p})) = 0$ and Corollary 16.3.26 implies $\dim(B_{\mathfrak{P}}) \leq \dim(A_{\mathfrak{p}})$, whence

$$\operatorname{ht}(\mathfrak{a}^e) \leq \operatorname{ht}(\mathfrak{P}) = \dim(B_{\mathfrak{P}}) \leq \dim(A_{\mathfrak{p}}) = \operatorname{ht}(\mathfrak{p}) = \operatorname{ht}(\mathfrak{a}).$$

This proves the claim. □

Proposition 16.3.30. *Let A be a Noetherian ring, $\mathfrak{a}$ an ideal of A, and M a finitely generated A-module. Let $\widehat{A}$ (resp. $\widehat{M}$) be the Hausdorff completions of A (resp. M) under the $\mathfrak{a}$-adic topology.*

(a) Let $\mathfrak{p}$ be a prime ideal of A containing $\mathfrak{a}$. Then $\hat{\mathfrak{p}}$ is a prime ideal of $\widehat{A}$ and $\dim_{\widehat{A}_{\hat{\mathfrak{p}}}}(\widehat{M}_{\hat{\mathfrak{p}}}) = \dim_{A_{\mathfrak{p}}}(M_{\mathfrak{p}})$.

(b) We have $\dim_{\widehat{A}}(\widehat{M}) = \sup_{\mathfrak{m}} \dim_{\widehat{A}_{\hat{\mathfrak{p}}}}(\widehat{M}_{\hat{\mathfrak{p}}}) = \sup_{\mathfrak{m}} \dim_{A_{\mathfrak{m}}}(M_{\mathfrak{m}})$, where $\mathfrak{m}$ runs through prime (resp. maximal) ideals of A containing $\mathfrak{a}$. In particular, $\dim_{\widehat{A}}(\widehat{M}) \leq \dim_A(M)$.

Proof. Since the $\mathfrak{a}$-adic topology on $A/\mathfrak{p}$ is trivial, by Corollary 11.4.14 $\widehat{A}/\hat{\mathfrak{p}}$ is identified with $A/\mathfrak{p}$, so $\hat{\mathfrak{p}}$ is a prime ideal of $\widehat{A}$. Since $\widehat{A}$ is flat over A, $\widehat{A}_{\hat{\mathfrak{p}}}$ is flat over $A_{\mathfrak{p}}$. Moreover the canonical homomorphism of A in $\widehat{A}$ induces an isomorphism of $A/\mathfrak{a}$ on $\widehat{A}/\hat{\mathfrak{a}}$, therefore also an isomorphism of $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ on $\widehat{A}_{\hat{\mathfrak{p}}}/\mathfrak{p}\widehat{A}_{\hat{\mathfrak{p}}}$. We conclude assertion (a) by applying Proposition 16.3.24 to the homomorphism $A_{\mathfrak{p}} \to \widehat{A}_{\hat{\mathfrak{p}}}$ and to the modules $M_{\mathfrak{p}}$ and $\widehat{A}_{\hat{\mathfrak{p}}}$, noting that $M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} \widehat{A}_{\hat{\mathfrak{p}}}$ is isomorphic to $\widehat{M}_{\hat{\mathfrak{p}}}$.

By Proposition 11.4.22, the map $\mathfrak{m} \mapsto \hat{\mathfrak{m}}$ is a bijection from the set of maximal ideals of A containing $\mathfrak{a}$ to the set of maximal ideals of $\widehat{A}$. Thus assertion (b) follows from Proposition 16.1.12. □

Corollary 16.3.31. *Let A be a Noetherian Zariski ring. Then for any finitely generated A-module M, we have $\dim_A(M) = \dim_{\widehat{A}}(\widehat{M})$.*

Proof. The topology on A is $\mathfrak{a}$-adic, where $\mathfrak{a}$ is an ideal contained in the Jacobson radical of A. Thus the claim follows from Proposition 16.3.30. □

Corollary 16.3.32. *Let A be a Noetherian ring, $\mathfrak{a}$ an ideal of A, and $\widehat{A}$ the Hausdorff completion with respect to the $\mathfrak{a}$-adic topology. Then $\dim(\widehat{A}) \leq \dim(A)$, and the equality holds if A is local and $\mathfrak{a}$ is proper.*

Corollary 16.3.33. *Let A be a Noetherian ring and n a positive integer. Then*

$$\dim(A[\![X_1, \ldots, X_n]\!]) = \dim(A) + n.$$

Proof. The ring $A[\![X_1, \ldots, X_n]\!]$ is the Hausdorff completion of $A[X_1, \ldots, X_n]$ with respect to the $\mathfrak{m}$-adic topology, where $\mathfrak{m}$ is generated by $X_1, \ldots, X_n$. We then have

$$\dim(A[\![X_1, \ldots, X_n]\!]) \leq \dim(A[X_1, \ldots, X_n]) = \dim(A) + n$$

and the reverse inequality is already established. □

Corollary 16.3.34. *Let A be a Noetherian ring and $\mathfrak{a}$ an ideal of A. Suppose that A is Hausdorff and complete under the $\mathfrak{a}$-adic topology. Then for any positive integer n, we have*

$$\dim(A\{X_1, \ldots, X_n\}) = \dim(A) + n.$$

Proof. The ring $A\{X_1, \ldots, X_n\}$ is the $\mathfrak{a}$-adic completion of $A[X_1, \ldots, X_n]$, so

$$\dim(A\{X_1, \ldots, X_n\}) \leq \dim(A) + n.$$

The reverse inequality can be established just like the power series ring. □

Corollary 16.3.35. *Let A be a Noetherian local ring, identified with a subring of its completion $\widehat{A}$, and B a subring of $\widehat{A}$ containing A. Suppose that B is a Noetherian local ring and that we have $\mathfrak{m}_A B = \mathfrak{m}_B$. Then $\dim(A) = \dim(B)$.*

Proof. By Proposition 11.4.34 the canonical injection of A into B extends to an isomorphism of $\widehat{A}$ on the completion $\widehat{B}$ of B, whence $\dim(B) = \dim(A)$. □

16.3.4 Exersise

Exercise 16.3.1. Let k be a field, and set

$$A = k[x, y], \quad B = [x, y, x/y], \quad \mathfrak{p} = (x, y)A, \quad \mathfrak{q} = (y, x/y)B$$

check that

$$\mathfrak{p} = \mathfrak{q} \cap A, \quad \mathrm{ht}\mathfrak{p} = \mathrm{ht}\mathfrak{q} = 2, \quad \dim B_{\mathfrak{q}}/\mathfrak{p}B_{\mathfrak{q}} = 1$$

so that

$$\mathrm{ht}\mathfrak{q} < \mathrm{ht}\mathfrak{p} + \dim B_{\mathfrak{q}}/\mathfrak{p}B_{\mathfrak{q}}$$

Show also by a concrete example that the going-down property does not hold between A and B.

Proof. Clealry we can see $(x, y)A \subseteq (y, x/y)B$ so that $\mathfrak{p} \subseteq \mathfrak{q} \cap A$. Also, $\mathfrak{p}$ is a maximal ideal in A, hence $\mathfrak{p} = \mathfrak{q} \cap A$.

We have $(y) = (y, x/y)$ in B, so

$$(y, x/y) \supset (y, x) \supset (0)$$

is a maximal chain of $\mathfrak{q}$. For $\mathfrak{p}$, it is easy to verify height $\mathfrak{p} = 2$.

For $\dim B_{\mathfrak{q}}/\mathfrak{p}B_{\mathfrak{q}}$, note that

$$(x, y)B \subset (y, x/y)B$$

Since (x, y) is maximal in A, if there is an ideal Q sandwiched between them, then Q contains a polynomial in x/y, hence contains x/y since Q is prime. This implies $\dim B_{\mathfrak{q}}/\mathfrak{p}B_{\mathfrak{q}} = 1$.

Consider the following chain in A:

$$P_1 = (y)A \subset (x, y)A = P_2$$

And choose a prime $Q_2 = (x, y)B$ in B such that $Q_2^c = P_2$. If Q_1 is a prime ideal in B such that $Q_1^c = P_1$, then $(y)A \subseteq Q_1$, in particular $y \in Q_1$. Note that since $x/y \in B$, this implies $x = (x/y) \cdot y \in Q_1$. But this means $Q_2 \subseteq Q_1$, hence there is no prime ideal contained in Q_2 satisfying the condition, therefore the going down property does not hold. □

Exercise 16.3.2. Let A be a ring, U an open subset of $\operatorname{Spec}(A)$.

(a) Show that the map $\mathfrak{p} \mapsto V(\mathfrak{p}) \cap U$ induce a bijection of U onto the set of irreducible closed subsets of U.

(b) Show that $\dim(U)$ is the supremum of the length of chains of prime ideals of A contained in U.

(c) Let Φ be the set of minimal prime ideals of A contained in U. Show that

$$\dim(U) = \sup_{\mathfrak{p} \in \Phi} \dim(V(\mathfrak{p}) \cap U)$$

(d)

16.4 Hilbert-Samuel series

Let A be an Artinian ring and consider the power series ring $A[\![T]\!]$ with one indeterminate on A. In this section, we denote by $A((T))$ the fraction ring $A[\![T]\!]_T$ of $A[\![T]\!]$ at the element T, which is identified with the subring of the Laurent series ring $A[\![T, T^{-1}]\!]$ consisting of elements $\sum_{n \in \mathbb{Z}} a_n T^n$ that is **bounded below**, that is, there exist $n_0 \in \mathbb{N}$ such that $a_n = 0$ for all $n < n_0$. The ring $\mathbb{Z}((T))$ will be our main focus in this section.

For any $n, p \in \mathbb{Z}$, we extend the definition of the binomial coefficient $\binom{n}{p}$ by defining $\binom{n}{p} = 0$ if $p < 0$ or $p > n$.

Lemma 16.4.1. *The element $(1 - T)$ is invertible in $\mathbb{Z}((T))$, and for any $r > 0$ we have*

$$(1 - T)^{-r} = \sum_{n \in \mathbb{Z}} \binom{n + r - 1}{r - 1} T^n = \sum_{n \in \mathbb{N}} \binom{n + r - 1}{r - 1} T^n.$$

Proof. The element $1 - T$ is invertible with inverse $\sum_{n\in\mathbb{N}} T^n$, so

$$(1-T)^{-r} = \Big(\sum_{n\in\mathbb{N}} T^n\Big)^r = \sum_{n_1,\dots,n_r\in\mathbb{N}} T^{n_1+\cdots+n_r} = \sum_{n\in\mathbb{N}} \binom{n+r-1}{r-1} T^n$$

so the claim follows. □

Let $Q(T) \in \mathbb{Z}[T, T^{-1}]$ and r be a positive integer. If $P(T) = (1-T)^{-r}Q(T)$, then it is easy to see $P(T) \in \mathbb{Z}((T))$. In fact, if

$$Q(T) = \sum_{n\in\mathbb{Z}} a_n T^n, \quad P = \sum_{n\in\mathbb{Z}} b_n T^n$$

then

$$b_n = \sum_{i\in\mathbb{Z}} a_i \binom{n-i+r-1}{r-1} = \sum_{i\le n} a_i \binom{n-i+r-1}{r-1}$$

where the summation is finite since $Q(T)$ is bounded below. If n_0 is the supremum of the integers $i \in \mathbb{Z}$ such that $a_i \neq 0$, then for $n \ge n_0$, we can write

$$b_n = \sum_{i\in\mathbb{Z}} a_i \binom{n-i+r-1}{r-1} = \frac{1}{(r-1)!} \sum_{i\in\mathbb{Z}} a_i \prod_{j=1}^{r-1} (n-i+j).$$

If $c = Q(1) = \sum_i a_i$, then we get

$$b_n = c\frac{n^{r-1}}{(r-1)!} + \rho_n n^{r-2} \tag{4.0.1}$$

where the rational number ρ_n tends to a limit as n increases indefinitely. Therefore we deduce the relationship

$$Q(1) = (r-1)! \lim_{n\to\infty} n^{1-r} b_n. \tag{4.0.2}$$

For two elements $F = \sum_n a_n T^n$ and $G = \sum_n b_n T^n$ in $\mathbb{Z}((T))$, we denote $F \le G$ by the relation $a_n \le b_n$ for all n, which is an order relation compatible with the ring structure of $\mathbb{Z}((T))$. We have $(1-T)^{-r} \ge 1$, and if an element Q is bigger than 0, then the integer $Q(1)$ is positive.

Lemma 16.4.2. *Let P be a nonzero element in $\mathbb{Z}((T))$ such that $(1-T)^r P \in \mathbb{Z}[T, T^{-1}]$ for some $r \in \mathbb{Z}$. Then there exists a unique $Q \in \mathbb{Z}[T, T^{-1}]$ such that $P = (1-T)^{-d}Q$ and $Q(1) \neq 0$, for some $d \in \mathbb{Z}$. If $P \ge 0$, then $Q(1) \ge 0$.*

Proof. Since $(1-T)^r P \in \mathbb{Z}[T, T^{-1}]$, we can write $P = (1-T)^{-1}T^n R(T)$ with $R(T) \in \mathbb{Z}[T]$, and by Euclidean division we may assume that $R(1) \neq 0$, which proves the existence of d and Q. On the other hand, if we have

$$(1-T)^r Q(T) = (1-T)^s R(T)$$

with $r > s$ and $Q, R \in \mathbb{Z}[T, T^{-1}]$, then $R(T) = (1-T)^{r-s}Q(T)$, whence $R(1) = 0$. This proves the uniqueness part.

Finally, assume that $P \ge 0$. If $P = (1-T)^{-d}Q$ with $d < 0$ then $P(1) = 0$ and we must have $P = 0$, which is a contradiction. Therefore $d \ge 0$, and if $d = 0$ then $P(1) = Q(1) \ge 0$. If $d > 0$,

then $Q(1)$ is given by the formula (4.0.2), so $Q(1) \geq 0$. □

Lemma 16.4.3. *Let P, Q be elements of $\mathbb{Z}[T, T^{-1}]$, $p, q \in \mathbb{Z}$ and $P(1) > 0$. If*

$$(1-T)^{-p}P \leq (1-T)^{-q}Q$$

then, either $p < q$, or $p = q$ and $P(1) \leq Q(1)$.

Proof. Suppose $p \geq q$, then we have $(1-T)^{-p}[(1-T)^{p-q}Q - P] \geq 0$. Since $R = (1-T)^{p-q}Q - P \in \mathbb{Z}[T, T^{-1}]$, by Lemma 16.4.3 we have $R(1) \geq 0$. If $p > q$, then $R(1) = -P(1) \geq 0$, which is a contradiction. If $p = q$, then $R(1) = Q(1) - P(1)$, whence $P(1) \leq Q(1)$. □

16.4.1 Poincaré series of a graded module on a polynomial ring

Let A_0 be an Artinian ring, I a finite set and consider the ring $A = A_0[(X_i)_{i\in I}]$. For each $i \in I$, let d_i be a positive integer. Endow A with the graded ring structure of type $\mathbb{Z}$ such that the elements of A_0 are homogeneous of degree 0 and each X_i is homogeneous of degree d_i. If $d_i = 1$ for each i, we then get the usual graduation on the polynomial ring A.

Let M be a finitely generated graded A-module such that all the homogeneous components of M are A_0-module of finite length. The **Poincaré series** of M, denoted by P_M, is the elemnt in $\mathbb{Z}((T))$ defined by

$$P_M = \sum_{n\in\mathbb{Z}} \ell_{A_0}(M_n) \cdot T^n.$$

Theorem 16.4.4. *The element $Q_M = P_M \prod_{i\in I}(1 - T^{d_i})$ is in $\mathbb{Z}[T, T^{-1}]$.*

Proof. If $I = \varnothing$, then $A = A_0$, and the family $(\ell_{A_0}(M_n))_{n\in\mathbb{Z}}$ has finite support since M is a finitely generated A_0-module, whence has finite length. The theorem is therefore proved in this case.

Now we prove by induction on the cardinality of I. Fix $j \in I$, $J = I \setminus \{j\}$, and denote by A' the subring of A generated by A_0 and the X_i with $i \in J$. Consider the homothety h_{X_j} with ratio X_j with kernel R and cokernel S. Then for each $n \in \mathbb{Z}$, we have an exact sequence

$$0 \longrightarrow R_{n-d_j} \longrightarrow M_{n-d_j} \xrightarrow{h_{X_j}} M_n \longrightarrow S_n \longrightarrow 0$$

whence R_n and S_n have finite legnth, and we have

$$\ell_{A_0}(M_n) - \ell_{A_0}(M_{n-d_j}) = \ell_{A_0}(S_n) - \ell_{A_0}(R_{n-d_j}). \tag{4.1.1}$$

Since M is a finitely generated module over the Noetherian A, it is Noetherian so the A-modules R and S are finitely generated. Since they are both annihilated by X_j, they are finitely generated as A'-modules. According to the induction hypothesis, the elements Q_R and Q_S are in $\mathbb{Z}[T, T^{-1}]$. Moreover, due to (4.1.1), we have

$$(1 - T^{d_j})P_M = P_M - T^{d_j}P_M = P_S - T^{d_j}P_R \tag{4.1.2}$$

which implies

$$Q_M = P_M \prod_{i\in I}(1 - T^{d_i}) = P_S \prod_{i\in J}(1 - T^{d_i}) - T^{d_j}P_R \prod_{i\in J}(1 - T^{d_i}).$$

This shows Q_M is in $\mathbb{Z}[T, T^{-1}]$, and our conclusion is then proved. □

Example 16.4.5. Let M_0 be an A_0-module and $M = A \otimes_{A_0} M_0$. Then with the notations above, we have $R = 0$ and $S = A' \otimes_{A_0} M_0$, so $Q_M = Q_S$ by (4.1.2). Since $Q_{M_0} = \ell_{A_0}(M_0)$, by induction $Q_M = \ell_{A_0}(M_0)$, whence

$$P_M = \ell_{A_0}(M_0) \prod_{i \in I} (1 - T^{d_i})^{-1}.$$

Corollary 16.4.6. *Assume that $d_i = 1$ for all $i \in I$ and set $r = |I|$, $c_M = Q_M(1)$.*

(a) If $r = 0$, then $\ell_{A_0}(M) = c_M$.

(b) If $r = 1$, then $\ell_{A_0}(M_n) = c_M$ for n large enough.

(c) If $r > 1$, then $\ell_{A_0}(M_n) = \dfrac{c_M}{(r-1)!} n^{r-1} + \rho_n n^{r-2}$, where ρ_n has a limit when $n \to +\infty$.

Proof. In this case we have $P_M = Q_M(1 - T)^{-r}$, so this follows from the formula (4.0.2). □

For simplicity, we may endow A with the usual graduation henceforth, so we have

$$P_M = Q_M(1 - T)^{-r}.$$

Example 16.4.7 (Example of Poincaré series for graded modules).

(a) Let $0 \to M' \to M \to M'' \to 0$ be an exact sequence of graded A-modules and of homomorphisms of degree 0 such that M is finitely generated over A and M_n of finite length over A_0 for each n. Then by the additivity of legnth, we have

$$P_M = P_{M'} + P_{M''}, \quad Q_M = Q_{M'} + Q_{M''}, \quad c_M = c_{M'} + c_{M''}.$$

(b) Let $M(p)$ be the modulu deduced from M by shifting p from the graduation of M. Since $M(p)_n = M_{p+n}$, we have

$$P_{M(p)} = T^{-p} P_M, \quad Q_{M(p)} = T^{-p} Q_M, \quad c_{M(p)} = c_M.$$

(c) Let M be a free graded A-module generated by lineraly independent homogeneous elements of degrees $\delta_1, \ldots, \delta_s$. As M is isomorphic to $A(-\delta_1) \oplus \cdots \oplus A(-\delta_s)$, we have

$$P_M = \ell(A_0)\Big(\sum_{i=1}^{s} T^{\delta_s}\Big)(1 - T)^{-r}, \quad Q_M = \ell(A_0)\Big(\sum_{i=1}^{s} T^{\delta_s}\Big), \quad c_M = s \cdot \ell(A_0).$$

(d) Let M be a finitely generated A-module and suppose that there exists a long exact sequence of graded A-modules and of homomorphisms of degree 0

$$0 \longrightarrow L_n \longrightarrow L_{n-1} \longrightarrow \cdots \longrightarrow L_0 \longrightarrow M \longrightarrow 0$$

such that for each k, the module L_k is free and generated by linearly independent homogeneous elements of degrees $\delta_{k,1}, \ldots, \delta_{k,m_k}$. Then by (c),

$$Q_M = \ell(A_0) \sum_{k=0}^{n} \sum_{j=1}^{m_k} (-1)^k T^{\delta_{k,j}}, \quad c_M = \ell(A_0) \sum_{k=0}^{n} (-1)^k m_k.$$

Proposition 16.4.8. *Let M be a graded A-module. If M is generated by M_0 and M_0 is an A_0-module with finite length. Then we have*

$$P_M \leq (1-T)^{-r}\ell_{A_0}(M_0), \quad c_M \leq \ell_{A_0}(M_0).$$

Moreover, the following conditions are equivalent:

(i) $c_M = \ell_{A_0}(M_0)$.

(ii) $P_M = \ell_{A_0}(M_0)(1-T)^{-r}$.

(iii) The canonical homomorphism $\varphi : A \otimes_{A_0} M_0 \to M$ is bijective.

Proof. Let R be the kernel of φ. Then since φ is surjective, we have

$$P_M = P_{A\otimes_{A_0}M_0} - P_R = \ell_{A_0}(M_0)(1-T)^{-r} - P_R, \quad c_M = \ell_{A_0}(M_0) - c_R$$

which proves the first assertion. Now the conditions (i), (ii), and (iii) are equivalent to $c_R = 0$, $P_R = 0$, and $R = 0$, respectively, so we have (iii)⇒(ii)⇒(i). It remains to show that $c_R = 0$ implies $R = 0$. Now assume that $R \neq 0$ and let

$$0 = M^r \subset M^{r-1} \subset \cdots \subset M^0 = M_0$$

be a Jordan-Hölder series of the A_0-module M_0. Let R^k be the intersection of R and the image of $A \otimes_{A_0} M^k$ in $A \otimes_{A_0} M_0$. Then there exists an integer k such that $R^k \neq R^{k-1}$. Define $L = R^{k-1}/R^k$, we have $0 \leq c_L \leq c_R$, and it suffices to prove that $c_L \neq 0$. Now, if K is the quotient field of A_0 by the maximal ideal annihilating M^{k-1}/M^k, then L is identified with a nonzero graded submodule of $K[(X_i)_{i\in I}]$. So L contains a submodule isomorphic to a shifted module of $K[(X_i)_{i\in I}]$. As $c_{K[(X_i)_{i\in I}]} = 1$, we have $c_L \geq 1$, which proves the claim. □

Proposition 16.4.9. *Suppose that A_0 is a field and M is a finitely generated graded A-module. If K is the field of fraction of A, then c_M is equal to the rank of the A-module M, which is also the dimension of the K-vector space $M \otimes_A K$.*

Proof. This is clear if $M = A$, since $c_A = 1$. On the other hand, let $x \in A$, homogeneous of degree d, and not zero. We have $(A/xA) \otimes_A K = 0$. From the exact sequence

$$0 \longrightarrow A(-d) \xrightarrow{h_x} A \longrightarrow A/xA \longrightarrow 0$$

we get $c_{A/xA} = 0$. The proposition is therefore verified when M is generated by a homogeneous element. The general case follows, since any finite type graded A-module has a composition sequence whose quotients are of the previous form. □

Example 16.4.10. Let A_0 be a field, P a homogeneous polynomial in A of degree s, and M the module A/PA. Since the rank of M equals to the degree of P, by Proposition 16.4.9 we have $c_M = s$. On the other hand, it is not hard to compute that

$$\ell_{A_0}(M_n) = \binom{n+r-1}{r-1} - \binom{n-s+r-1}{r-1}$$

and therefore

$$c_M = (r-1)! \lim_{n\to\infty} n^{1-r}\left(\binom{n+r-1}{r-1} - \binom{n-s+r-1}{r-1}\right) = s$$

verifying our claim.

16.4.2 Hilbert-Samuel series of a good-filtered module

Let A be a Noetherian ring, $\mathfrak{a}$ an ideal of A, and M a finitely generated A-module. Recall that an exhaustive filtration $\mathcal{F} = (M_n)_{n\in\mathbb{Z}}$ on M consisting of submodules is called **$\mathfrak{a}$-good** if

(a) $\mathfrak{a}M_n \subseteq M_{n+1}$ for all $n \in \mathbb{Z}$.

(b) There exists an integer n_0 such that $\mathfrak{a}M_n = M_{n+1}$ for all $n \geq n_0$.

Similar to the case of series, we say the filtration $\mathcal{F}$ is **bounded below** if there exist $n_1 \in \mathbb{Z}$ such that $M_n = M$ for all $n \leq n_1$. Note that if the filtration $\mathcal{F}$ is exhaustive and M is finitely generated, then $\mathcal{F}$ is bounded below since M is then Noetherian.

Lemma 16.4.11. *Let (M_n) be an $\mathfrak{a}$-good filtration on M. If $M/\mathfrak{a}M$ has finite length, then M/M_{n+1} and M_n/M_{n+1} have finite length for all $n \in \mathbb{Z}$.*

Proof. Since $\mathcal{F}$ is bounded below, there exist n_1 such that $M_{n_1} = M$. Also, as (M_n) is $\mathfrak{a}$-good, there exist n_0 such that $\mathfrak{a}M_n = M_{n+1}$ for all $n \geq n_0$. Then for all $n \in \mathbb{Z}$,

$$\mathfrak{a}^{n-n_1}M \subseteq M_n \subseteq \mathfrak{a}^{n-n_0}M \tag{4.2.1}$$

where we define $\mathfrak{a}^n = A$ for $n \leq 0$. Then $\ell(M/M_n) \leq \ell(M/\mathfrak{a}^{n-n_1}M)$ and it suffices to prove that $\mathfrak{a}^nM/\mathfrak{a}^{n+1}M$ has finite length for each n. So we are reduced to the case of $\mathfrak{a}$-adic filtration. Let $(x_1, \ldots, x_r)$ be a finite generating system of the A-module $\mathfrak{a}$, and let I be the finite set of monomials of total degree n in r variables $X_1, \ldots, X_r$. The homomorphism from $(M/\mathfrak{a}M)^I$ to $\mathfrak{a}^nM/\mathfrak{a}^{n+1}M$ which maps $(u_m)_{m\in I}$ to $\sum_m m(x_1, \ldots, x_r)u_m$ is surjective. Since $M/\mathfrak{a}M$ has finite length, so does $\mathfrak{a}^nM/\mathfrak{a}^{n+1}M$. □

Suppose henceforth that $M/\mathfrak{a}M$ has finite length. Let $\mathcal{F} = (M_n)$ be an $\mathfrak{a}$-good filtration on M. We define therefore the **Hilbert-Samuel series** H_M of M with respect to the $\mathfrak{a}$-good filtration (M_n) by

$$H_{M,\mathcal{F}} = \sum_{n\in\mathbb{Z}} \ell_{A/\mathfrak{a}}(M_n/M_{n+1}) \cdot T^n$$

and the map $n \mapsto \ell_{A/\mathfrak{a}}(M_n/M_{n+1})$ is called the **Hilbert-Samuel function** of M with respect to (M_n).

Since there exists an integer n_1 such that $M_n = M$ for $n \leq n_1$, we see H_M is an element in $\mathbb{Z}((T))$. We denote by $H_{M,\mathfrak{a}}$ by the Hilbert-Samuel series of M with respect to the $\mathfrak{a}$-adic filtration, that is,

$$H_{M,\mathfrak{a}} = \sum_{n\in\mathbb{Z}} \ell_{A/\mathfrak{a}}(\mathfrak{a}^nM/\mathfrak{a}^{n+1}M) \cdot T^n.$$

If $P \in \mathbb{Z}((T))$ and $r \in \mathbb{N}$, we may use $P^{(1)}$ to denote the series $(1-T)^{-r}P$. In other words, if $P = \sum_{n\in\mathbb{Z}} a_nT^n$, then

$$P^{(1)} = \sum_{n\in\mathbb{Z}} \Big(\sum_{i\leq n} a_i\Big)T^n.$$

Proposition 16.4.12. *Let $\mathcal{F}$ be an $\mathfrak{a}$-good filtration on M. Then*

$$H^{(1)}_{M,\mathcal{F}} = \sum_{n\in\mathbb{Z}} \ell_A(M/M_{n+1}) \cdot T^n.$$

If $\mathcal{F}'$ is another $\mathfrak{a}$-good filtration on M, then there exists an integer m such that $H^{(1)}_{M,\mathcal{F}'} \geq T^m H^{(1)}_{M,\mathcal{F}}$.

Proof. Since $\ell_{A/\mathfrak{a}}(M_n/M_{n+1}) = \ell_A(M_n/M_{n+1})$, the first claim follows from the definition of $H_{M,\mathcal{F}}$ and the observation

$$\sum_{i\leq n} \ell_{A/\mathfrak{a}}(M_i/M_{i+1}) = \sum_{i\leq n} \ell_A(M_i/M_{i+1}) = \ell_A(M/M_{n+1}).$$

If $\mathcal{F} = (M'_n)$ is another filtration, then there exist an integer n_2 such that $M'_n \subseteq \mathfrak{a}^{n-n_2}M$ for all n, whence $M'_n \subseteq M_{n-(n_2-n_1)}$, and the second claim therefore follows. □

Theorem 16.4.13. *Let A be a Noetherian ring, $\mathfrak{a}$ an idela of A, M a finitely generated A-module such that $M/\mathfrak{a}M$ is nonzero and has finite length. Let $\mathcal{F}$ be an $\mathfrak{a}$-good filtration on M, then there exists a positive integer d and a uniquely determined element R in $\mathbb{Z}[T, T^{-1}]$ such that*

$$H_{M,\mathcal{F}} = (1-T)^{-d}R \quad \textit{and} \quad R(1) > 0.$$

Moreover, the integers d and $R(1)$ are independent of the filtration $\mathcal{F}$.

Proof. Consider the graded ring $\mathrm{gr}(A)$ and the graded module $\mathrm{gr}(M)$. Since $M_{n_1} = M$ and $\mathfrak{a}M_n = M_{n+1}$ for $n \geq n_0$, $\mathrm{gr}(M)$ is generated by $\bigoplus_{n_1\leq n\leq n_0} \mathrm{gr}_n(M)$, so is finitely generated. Furthermore, if $(x_1, \ldots, x_r)$ is a finite generating system of the A-module $\mathfrak{a}$, then $\mathrm{gr}(A)$ is generated by $\mathrm{gr}_0(A)$ and the classes of x_i modulo $\mathfrak{a}^2$, so is isomorphic to a graded ring quotient of $B = (A/\mathfrak{a})[X_1, \ldots, X_r]$. According to Theorem 16.4.4, we have

$$(1-T)^r H_{M,\mathcal{F}} \in \mathbb{Z}[T, T^{-1}].$$

Since $H_{M,\mathcal{F}} \neq 0$, by Lemma 16.4.2 there exist $d \in \mathbb{N}$ and $R \in \mathbb{Z}[T, T^{-1}]$ uniquely determined such that $R(1) > 0$ and $H_{M,\mathcal{F}} = (1-T)^{-d}R$.

If $\mathcal{F}'$ is another $\mathfrak{a}$-good filtration on M, then similarly

$$H_{M,\mathcal{F}'} = (1-T)^{-d'}R'.$$

By Proposition 16.4.12, there exists an integer m such that

$$(1-T)^{-d'-1}R' \geq T^m(1-T)^{-d-1}R$$

and due to Lemma 16.4.3, this implies $d' \geq d$, or $d' = d$ and $R'(1) \geq R(1)$. Exchange the role of $\mathcal{F}$ and $\mathcal{F}'$, we then get $d = d'$ and $R'(1) = R(1)$. □

Remark 16.4.1. In the notations of Theorem 16.4.13, if $R = \sum_{i\in\mathbb{Z}} a_i T^i$ and suppose that $d > 0$, then the relation $H_{M,\mathcal{F}} = (1-T)^{-d}R$ implies

$$\ell_{A/\mathfrak{a}}(M_n/M_{n+1}) = \sum_{i\in\mathbb{Z}} a_i \binom{n-i+d-1}{d-1} = \sum_{i\leq n} a_i \binom{n-i+d-1}{d-1}$$

Similarly, the relation $H^{(1)}_{M,\mathcal{F}} = (1-T)^{-d-1}R$ implies

$$\ell_A(M/M_{n+1}) = \sum_{i\in\mathbb{Z}} a_i \binom{n-i+d}{d} = \sum_{i\leq n} a_i \binom{n-i+d}{d}$$

Let A be a Noetherian ring, $\mathfrak{a}$ an idela of A, M a finitely generated A-module such that $M/\mathfrak{a}M$ has finite length. If $M \neq \mathfrak{a}M$, then by Theorem 16.4.13 there exists integers $d_\mathfrak{a}(M) \geq 0$ and $e_\mathfrak{a}(M) > 0$ such that, for any $\mathfrak{a}$-good filtration $\mathcal{F}$ on M,

$$H_{M,\mathcal{F}} = (1-T)^{-d_\mathfrak{a}(M)}R, \quad R(1) = e_\mathfrak{a}(M).$$

If $M = \mathfrak{a}M$, then we may set $d_\mathfrak{a}(M) = -\infty$ and $e_\mathfrak{a}(M) = 0$.

Corollary 16.4.14. *Let A be a Noetherian ring, $\mathfrak{a}$ an idela of A, M a finitely generated A-module such that $M/\mathfrak{a}M$ is nonzero and has finite length. Let $\mathcal{F}$ be an $\mathfrak{a}$-good filtration on M.*

(a) For $d_\mathfrak{a}(M) \leq 0$, it is necessary and sufficient that the sequence $(\mathfrak{a}^n M)$ be stationary, or that the sequence (M_n) is stationary. In this case, we have, for all n large enough,

$$\ell_A(M/M_{n+1}) = \ell_A(M/\mathfrak{a}^{n+1}M) = e_\mathfrak{a}(M).$$

(b) Suppose that $d_\mathfrak{a}(M) > 0$, then

$$\ell_{A/\mathfrak{a}}(M_n/M_{n+1}) = e_\mathfrak{a}(M)\frac{n^{d_\mathfrak{a}(M)-1}}{(d_\mathfrak{a}(M)-1)!} + \rho_n n^{d_\mathfrak{a}(M)-2} \tag{4.2.2}$$

and

$$\ell_A(M/M_{n+1}) = e_\mathfrak{a}(M)\frac{n^{d_\mathfrak{a}(M)}}{d_\mathfrak{a}(M)!} + \sigma_n n^{d_\mathfrak{a}(M)-1}. \tag{4.2.3}$$

where ρ_n and σ_n have limits when $n \to \infty$.

Proof. This follows from formulas (4.0.1)and(4.0.2), and the definitons above. □

Example 16.4.15. Let k be an algebraically closed field and $F \in k[X_1, \ldots, X_r]$ be an irreducible polynomial F in A contained in the maximal ideal $\mathfrak{m} = (X_1, \ldots, X_r)$, and let m be the largest integer such that $F \in \mathfrak{m}^m$. Set $A = (k[X_1, \ldots, X_r]/(F))_\mathfrak{m}$ and let $\mathfrak{a} = (\mathfrak{m}/(F))_\mathfrak{m}$ be the maximal ideal of A; we want to determine $d_\mathfrak{a}(A)$ and $e_\mathfrak{a}(A)$. For this, we first note that $A/\mathfrak{a} = k$ by the Nullstellensatz and

$$0 \longrightarrow \mathfrak{a}^n/\mathfrak{a}^{n+1} \longrightarrow A/\mathfrak{a}^{n+1} \longrightarrow A/\mathfrak{a}^n \longrightarrow 0$$

Therefore we are reduced to compute $\dim_k(A/\mathfrak{a}^n)$. To this end, we first note that

$$A/\mathfrak{a}^n \cong (k[X_1, \ldots, X_r]/(F))/(\mathfrak{m}^n/(F)) = k[X_1, \ldots, X_n]/(\mathfrak{m}^n + (F)).$$

and we can use the following exact sequence to compute $\dim_k(k[X_1, \ldots, X_r]/(\mathfrak{m}^n + (F)))$:

$$0 \to k[X_1, \ldots, X_r]/\mathfrak{m}^{n-m} \xrightarrow{\psi} k[X_1, \ldots, X_r]/\mathfrak{m}^n \to k[X_1, \ldots, X_r]/(\mathfrak{m}^n + (F)) \to 0$$

where ψ is the homomorphism given by $\psi(\bar{G}) = \overline{FG}$. Since

$$\dim_k(k[X_1, \dots, X_r]/\mathfrak{m}^n) = \sum_{k=0}^{n-1} \binom{k+r-1}{r-1} \tag{4.2.4}$$

it follows that

$$\dim_k(k[X_1, \dots, X_r]/(\mathfrak{m}^n + (F))) = \sum_{k=n-m}^{n-1} \binom{k+r-1}{r-1}. \tag{4.2.5}$$

Since $\binom{n+r-1}{r-1} = \frac{n^{r-1}}{(r-1)!} + \cdots$, from (4.2.5) we deduce that

$$\dim_k(k[X_1, \dots, X_r]/(\mathfrak{m}^n + (F))) = m\frac{n^{r-1}}{(r-1)!} + \cdots .$$

This shows $d_{\mathfrak{a}}(A) = r - 1$ and $e_{\mathfrak{a}}(A) = m$. In the language of algebraic geometry, the ring A is the coordinate ring of the variety $V = V(F)$, and the integer m is called the **multiplicity** of the point $p = (0, \dots, 0)$ in V.

Example 16.4.16. Suppose that $\mathfrak{a}$ is contained in the Jacobson radical of A. Then from the Nakayama lemma, the sequence $(\mathfrak{a}^n M)$ is stationary if and only if we have $\mathfrak{a}^n M = 0$ for n large enough. It then follows from part (a) of Corollary 16.4.14 that we have $d_{\mathfrak{a}}(M) \leq 0$ if and only if M is of finite length and in this case $e_{\mathfrak{a}}(M) = \ell_A(M)$.

Consider now the special case A is local, $\mathfrak{a} = \mathfrak{m}$ is the maximal ideal of A, and $M = A$. Then by Proposition 6.3.7, we see $\mathfrak{m}^n = 0$ if and only if A is Artinian. By Corollary 16.4.14, in this case we have $d_{\mathfrak{m}}(A) = 0$ and $e_{\mathfrak{m}}(A) = \ell_A(A)$.

Furthermore, to provide a concrete example, let consider $A = k[X]/(X^n)$ where k is an algebraically closed field. Then $\mathfrak{m} = (X)/(X^n)$ is the maximal ideal of A and $\mathfrak{m}^n = 0$, so $e_{\mathfrak{m}}(A) = n$.

Proposition 16.4.17. *Let A be a Noetherian ring, $x_1, \dots, x_r$ elements of A, I the ideal they generate and M a finitely generated A-module such that M/IM is non-zero and of finite length.*

(a) We have $d_I(M) \leq r$, and if $d_I(M) = r$ then $e_I(M) \leq \ell_A(M/IM)$.

(c) If $(x_1, \dots, x_r)$ is completely secant for M, then $d_I(M) = r$ and $e_I(M) = \ell_A(M/IM)$. The converse is also true if I belongs to the Jacobson radical of A.

Proof. Let R be the ring $(A/I)[X_1, \dots, X_r]$, and give $N = \bigoplus_n I^n M/I^{n+1}M$ be the graded R-module structure for which h_{X_i} is the multiplication by the class x_i mod I^2. Then we have

$$P_N = H_{M,I} = (1-T)^{-d_I(M)}R = (1-T)^{-r}Q_N$$

where $R(1) = e_I(M) > 0$ and $Q_N(1) = c_N$. By Lemma 16.4.3, we therefore have either $d_I(M) < r$ and $c_N = 0$, or $d_I(M) = r$ and $c_N = e_I(M)$. Furthermore, according to Proposition 16.4.8, we have $c_N \leq \ell_A(M/IM)$, and the equality holds if and only if canonical homomorphism

$$\varphi : (A/I)[X_1, \dots, X_r] \otimes_{A/I} (M/IM) \to \bigoplus_n I^n M/I^{n+1}M$$

is bijective. This proves the claim, in view of **??**. □

Proposition 16.4.18. *Let $0 \to M' \to M \to M'' \to 0$ be an exact sequence of finitely generated modules over an Noetherian ring A and $\mathfrak{a}$ be an ideal of A.*

(a) For $M/\mathfrak{a}M$ to have finite length, it is necessary and sufficient that $M'/\mathfrak{a}M'$ and $M''/\mathfrak{a}M''$ both have finite length.

(b) Suppose that $M/\mathfrak{a}M$ has finite length. Then there are exactly the following three cases:

(i) $d_{\mathfrak{a}}(M) = d_{\mathfrak{a}}(M') > d_{\mathfrak{a}}(M'')$ and $e_{\mathfrak{a}}(M) = e_{\mathfrak{a}}(M')$.

(ii) $d_{\mathfrak{a}}(M) = d_{\mathfrak{a}}(M'') > d_{\mathfrak{a}}(M')$ and $e_{\mathfrak{a}}(M) = e_{\mathfrak{a}}(M'')$.

(iii) $d_{\mathfrak{a}}(M) = d_{\mathfrak{a}}(M') = d_{\mathfrak{a}}(M'')$ and $e_{\mathfrak{a}}(M) = e_{\mathfrak{a}}(M') + e_{\mathfrak{a}}(M'')$.

Proof. By Proposition 12.2.14 and Corollary 10.4.38, for the module $M/\mathfrak{a}M$ to have finite length, it is necessary and sufficient that the element in

$$\operatorname{supp}(M/\mathfrak{a}M) = \operatorname{supp}(M) \cap V(\mathfrak{a})$$

is maximal. Since $\operatorname{supp}(M) = \operatorname{supp}(M') \cap \operatorname{supp}(M'')$, the assertion in (a) follows.

Now endow M with an $\mathfrak{a}$-good filtration $\mathcal{F}$ (for example the $\mathfrak{a}$-adic filtration), M' the submodule filtration $\mathcal{F}'$, and M'' the quotient filtration $\mathcal{F}''$. By Proposition 11.4.3, the filtrations $\mathcal{F}'$ and $\mathcal{F}''$ are $\mathfrak{a}$-good. Then we have for each n an exact sequence of A-modules

$$0 \longrightarrow M'_n/M'_{n+1} \longrightarrow M_n/M_{n+1} \longrightarrow M''_n/M''_{n+1} \longrightarrow 0$$

which implies $H_{M,\mathcal{F}} = H_{M',\mathcal{F}'} + H_{M'',\mathcal{F}''}$, and

$$(1-T)^{-d_{\mathfrak{q}}(M)}R = (1-T)^{-d_{\mathfrak{q}}(M')}R' + (1-T)^{-d_{\mathfrak{q}}(M'')}R''$$

with $R, R', R'' \in \mathbb{Z}[T, T^{-1}]$. Assertion (b) therefore follows. □

Theorem 16.4.19. *Let A be a Noetherian local ring, $\mathfrak{a}$ a proper ideal of A and M a finitely generated A-module such that $M/\mathfrak{a}M$ is non-zero and of finite length. Then the integer $d_{\mathfrak{a}}(M)$ equals to the dimension of the A-module M.*

Proof. We may suppose that $M \neq 0$. Let $(x_1, \ldots, x_r)$ be a system of parameters for M and I the ideal they generate. Then by Proposition 16.4.17 we have $d_I(M) \leq r$. Since $I \subseteq \mathfrak{a}$, we have $H^{(1)}_{M,\mathfrak{a}} \leq H^{(1)}_{M,I}$ and therefore (Lemma 16.4.3)

$$d_{\mathfrak{a}}(M) \leq d_I(M) \leq r = \dim_A(M).$$

We now prove the reverse inequality $\dim_A(M) \leq d_{\mathfrak{a}}(M)$ by induction on $\dim_A(M)$. The claim is clear when $\dim_A(M) = 0$. Suppose then we have $\dim_A(M) > 0$, and $\dim_A(N) \leq d_{\mathfrak{a}}(N)$ for any finitely generated A-module N such that $\dim_A(N) < \dim_A(M)$. If

$$0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$$

is a composition sequence of M, we have

$$\dim_A(M) = \sup(\dim_A(M_i/M_{i-1})), \quad d_{\mathfrak{a}}(M) = \sup(d_{\mathfrak{a}}(M_i/M_{i-1}))$$

by Proposition 16.1.12 and 16.4.18. Due to Proposition 12.1.17, we are now reduced to the case that M is of the form $A/\mathfrak{p}$, where $\mathfrak{p}$ is a prime ideal of A such that $\mathfrak{p} \neq \mathfrak{m}_A$ (otherwise $\dim(A/\mathfrak{p}) = 0$). Let $x \in \mathfrak{m}_A - \mathfrak{p}$, then the homothety h_x with ratio x is injective on M, and we have an exact sequence

$$0 \longrightarrow M \xrightarrow{h_x} M \longrightarrow M/xM \longrightarrow 0$$

By Proposition 16.3.11, the element x is secant for M, so we have $\dim_A(M/xM) = \dim_A(M) - 1$. On the other hand, since $e_{\mathfrak{a}}(M/xM) > 0$, from Proposition 16.4.18 we conclude $d_{\mathfrak{a}}(M/xM) \leq d_{\mathfrak{a}}(M) - 1$. Now by the induction hypothesis,

$$\dim_A(M) = \dim_A(M/xM) + 1 \leq d_{\mathfrak{a}}(M/xM) + 1 \leq d_{\mathfrak{a}}(M)$$

which finishes the induction process. □

Corollary 16.4.20. *Let A be a Noetherian ring, $\mathfrak{a}$ an idela of A, M a finitely generated A-module such that $M/\mathfrak{a}M$ is nonzero and has finite length. Then*

(a) $d_{\mathfrak{a}}(M)$ is the supremum of the integers $\dim_{A_{\mathfrak{m}}}(M_{\mathfrak{m}})$, where $\mathfrak{m}$ runs through the set $\operatorname{supp}(M) \cap V(\mathfrak{a})$.

(b) $e_{\mathfrak{a}}(M)$ is the sum of the integers $e_{\mathfrak{a}_{\mathfrak{m}}}(M_{\mathfrak{m}})$, where $\mathfrak{m}$ runs through the elements of $\operatorname{supp}(M) \cap V(\mathfrak{a})$ such that $\dim_{A_{\mathfrak{m}}}(M_{\mathfrak{m}}) = d_{\mathfrak{a}}(M)$.

Proof. By Corollary 12.2.18, the length of $M/\mathfrak{a}^n M$ is the sum of the $\ell_{A_{\mathfrak{m}}}(M_{\mathfrak{m}}/\mathfrak{a}_{\mathfrak{m}}^n M_{\mathfrak{m}})$ where $\mathfrak{m}$ runs through $\operatorname{Ass}(M/\mathfrak{a}^n M)$. Since $M/\mathfrak{a}^n M$ has finite length, the elements of $\operatorname{Ass}(M/\mathfrak{a}^n M)$ are maximal ideals and we have

$$\operatorname{Ass}(M/\mathfrak{a}^n M) = \operatorname{supp}(M/\mathfrak{a}^n M) = \operatorname{supp}(M) \cap V(\mathfrak{a}^n) = \operatorname{supp}(M) \cap V(\mathfrak{a})$$

(Proposition 12.2.14 and Corollary 10.4.38), so we have

$$H_{M,\mathfrak{a}} = \sum_{\mathfrak{m}} H_{M_{\mathfrak{m}},\mathfrak{a}_{\mathfrak{m}}}$$

where $\mathfrak{m}$ runs through prime ideals in $\operatorname{supp}(M) \cap V(\mathfrak{a})$. The claims then follow from this. □

Corollary 16.4.21. *Let A be a Noetherian ring, $\mathfrak{a}$ an ideal of A, and M a finitely generated A-module such that $M/\mathfrak{a}M$ has finite length. Let $\widehat{A}$ and $\widehat{M}$ be the Hausdorff completions of A and M under the $\mathfrak{a}$-adic topology. Then $d_{\mathfrak{a}}(M) = \dim_{\widehat{A}}(\widehat{M})$. If $\mathfrak{a}$ is contained in the Jacobson radical of A then $d_{\mathfrak{a}}(M) = \dim_A(M)$.*

Proof. By Proposition 16.3.30 and Corollary 16.4.20, we have

$$\dim_{\widehat{A}}(\widehat{M}) = \sup_{\mathfrak{m} \in V(\mathfrak{a})} \dim_{A_{\mathfrak{m}}}(M_{\mathfrak{m}}) = \sup_{\mathfrak{m} \in \operatorname{supp}(M) \cap V(\mathfrak{a})} \dim_{A_{\mathfrak{m}}}(M_{\mathfrak{m}}) = d_{\mathfrak{a}}(M).$$

If $\mathfrak{a}$ is contained in the Jacobson radical of A then we have $\dim_A(M) = \dim_{\widehat{A}}(\widehat{M})$, whence $d_{\mathfrak{a}}(M) = \dim_A(M)$. □

Lemma 16.4.22. *Let A be a ring, M an A-module, and (P_n), (Q_n) two filtrations on M of submodules with (Q_n) bounded below. Suppose that $Q_n \subseteq P_n$ and $\ell_A(P_n/Q_n) < +\infty$ for each $n \in \mathbb{Z}$. Then*

$$\begin{aligned}\sum_{n\in\mathbb{Z}} \ell_A((P_{n+1}\cap Q_n)/Q_{n+1})T^n &\le \sum_{n\in\mathbb{Z}} \ell_A(P_{n+1}/Q_{n+1})T^n \\ &\le (1-T)^{-1}\sum_{n\in\mathbb{Z}} \ell_A((P_{n+1}\cap Q_n)/Q_{n+1})T^n.\end{aligned} \tag{4.2.6}$$

Proof. It suffices to prove the following inequalities:

$$\ell_A((P_{n+1}\cap Q_n)/Q_{n+1}) \le \ell_A(P_{n+1}/Q_{n+1}) \le \sum_{i\le n} \ell_A((P_{n+1}\cap Q_n)/Q_{n+1}). \tag{4.2.7}$$

The first part is immediate. For the second part, since (Q_n) is bounded below, for i small enough we have $P_{n+1}\cap Q_i = P_{n+1}$, whence

$$\ell_A(P_{n+1}/Q_{n+1}) \le \sum_{i\le n} \ell_A((P_{n+1}\cap Q_i)/(P_{n+1}\cap Q_{i+1})).$$

On the other hand, the module $(P_{n+1}\cap Q_i)/(P_{n+1}\cap Q_{i+1})$ is isomorphic to $(P_{n+1}\cap Q_i + Q_{i+1})/Q_{i+1}$, which is a submodule of $(P_{i+1}\cap Q_i)/Q_{i+1}$ when $i \le n$. From these remarks we see (4.2.7) follows. □

Proposition 16.4.23. *Let A be a ring, M an A-module and $\mathcal{F}$ a bounded below filtration on M consisting of submodules such that M_n/M_{n+1} has finite length for all $n \in \mathbb{Z}$. Let ϕ be an endomorphism of M with kernel M' and cokernel M''. Endow M' with the submodule filtration $\mathcal{F}'$ and M'' the quotient filtration $\mathcal{F}''$. If there exist an integer δ such that $\phi(M_n) \subseteq M_{n+\delta}$ and $\mathrm{gr}(\phi)$ is the associated homomorphism on $\mathrm{gr}(M)$, then we have*

$$H_{M',\mathcal{F}'} \le P_{\ker \mathrm{gr}(\phi)}, \tag{4.2.8}$$

$$(1-T^\delta)H^{(1)}_{M,\mathcal{F}} + T^\delta P_{\ker \mathrm{gr}(\phi)} \le H^{(1)}_{M'',\mathcal{F}''} \le (1-T^\delta)H^{(1)}_{M,\mathcal{F}} + T^\delta P^{(1)}_{\ker \mathrm{gr}(\phi)}. \tag{4.2.9}$$

Proof. The sequence $N_n = \phi^{-1}(M_{n+\delta})$ forms a filtration on M and $M_n \subseteq N_n$ for all $n \in \mathbb{Z}$. By definition, we have $\ker(\mathrm{gr}(\phi)_n) = (N_{n+1}\cap M_n)/M_{n+1}$, and

$$P_{\ker \mathrm{gr}(\phi)} = \sum_{n\in\mathbb{Z}} \ell_A((N_{n+1}\cap M_n)/M_{n+1})T^n. \tag{4.2.10}$$

For each n, the module $(M'\cap M_n)/(M'\cap M_{n+1})$ is identified with the submodule $(M'\cap M_n + M_{n+1})/M_{n+1}$ of $(N_{n+1}\cap M_n)/M_{n+1}$, so follows from (4.2.10) that $H_{\mathcal{M}',\mathcal{F}'} \le P_{\ker \mathrm{gr}(\phi)}$. According to Lemma 16.4.22, we also have

$$P_{\ker \mathrm{gr}(\phi)} \le \sum_{n\in\mathbb{Z}} \ell_A(N_{n+1}/M_{n+1})T^n \le P^{(1)}_{\ker \mathrm{gr}(\phi)}. \tag{4.2.11}$$

For each $n \in \mathbb{Z}$, we have an exact sequence

$$0 \longrightarrow N_{n+1}/M_{n+1} \longrightarrow M/M_{n+1} \longrightarrow M/M_{n+\delta+1} \longrightarrow M''/M''_{n+\delta+1} \longrightarrow 0$$

This then implies, by the additivity of length, that

$$\ell_A(M''/M''_{n+\delta+1}) = \ell_A(M/M_{n+\delta+1}) - \ell_A(M/M_{n+1}) + \ell_A(N_{n+1}/M_{n+1}).$$

Multiply by $T^{n+\delta}$ on both sides and take summation on n, we then get

$$H^{(1)}_{M'',\mathcal{F}''} = (1 - T^\delta)H^{(1)}_{M,\mathcal{F}} + T^\delta \sum_{n\in\mathbb{Z}} \ell_A(N_{n+1}/M_{n+1})T^n. \tag{4.2.12}$$

The inequality (4.2.9) then follows from (4.2.11) and (4.2.12). □

Corollary 16.4.24. *Under the conditions of Proposition 16.4.23, we have $H_{M'',\mathcal{F}''} \geq (1 - T^\delta)H^{(1)}_{M,\mathcal{F}'}$, and the equality holds if and only if $\mathrm{gr}(\phi)$ is injective. In this case, we have $M' \subseteq \bigcap_n M_n$, and the following sequence is exact:*

$$0 \longrightarrow \mathrm{gr}(M) \xrightarrow{\mathrm{gr}(\phi)} \mathrm{gr}(M) \longrightarrow \mathrm{gr}(M'') \longrightarrow 0$$

Proof. The first assertion follows from (4.2.8). Suppose now $\mathrm{gr}(\phi)$ is injective. By Theorem 11.3.29 we have $\ker\phi \subseteq \phi^{-1}(M_{n+\delta}) = M_n$ for all n, whence $M' \subseteq \bigcap_n M_n$. Now consider the following exact sequence

$$0 \longrightarrow M/M' \xrightarrow{\bar\phi} M \longrightarrow M/\phi(M) \longrightarrow 0$$

Since $\mathrm{gr}(\phi)$ is injective, we have $\bar\phi^{-1}(M_n) = M_{n-\delta}/M'$. Hence the filtration on M/M' deduced by the filtration $\mathcal{F}$ on M is the filtration $(M_{n-\delta}/M')$. The associated graded module is $\mathrm{gr}(M)(-\delta)$ and we have an exact sequence of graded modules

$$0 \longrightarrow \mathrm{gr}(M)(-\delta) \longrightarrow \mathrm{gr}(M) \longrightarrow \mathrm{gr}(M'') \longrightarrow 0$$

which proves our claim. □

Proposition 16.4.25. *Let A be a Noetherian ring, M a finitely generated A-module, $\mathfrak{a}$ an ideal of A such that $M/\mathfrak{a}M$ has finite length, and $\mathcal{F}$ an $\mathfrak{a}$-good filtration on M. Let $(x_1, \dots, x_s)$ be a sequence of elements of A, $(\delta_1, \dots, \delta_s)$ a sequence of positive integers such that $x_i \in \mathfrak{a}^{\delta_i}$ for each i, and let ξ_i be the image of x_i in $\mathrm{gr}_{\delta_i}(A) = \mathfrak{a}^{\delta_i}/\mathfrak{a}^{\delta_i+1}$.*

(a) Endow the A-module $\overline{M} = M/\sum_i x_iM$ with the $\mathfrak{a}$-good filtration $\overline{\mathcal{F}}$. Then we have

$$H^{(s)}_{\overline{M},\overline{\mathcal{F}}} \geq \prod_{i=1}^{s}(1 - T^{\delta_i})H^{(s)}_{M,\mathcal{F}}. \tag{4.2.13}$$

(b) For the equality in (a) holds, it is necessary and sufficient that the sequence $(\xi_1, \dots, \xi_s)$ of elements of $\mathrm{gr}(A)$ is completely secant for $\mathrm{gr}(M)$. In this case, the canonical homomorphism

$$\theta : \mathrm{gr}(M)/\sum_i \xi_i \cdot \mathrm{gr}(M) \to \mathrm{gr}(\overline{M})$$

is bijective.

(c) *Suppose the condition in (b) hold, and the modules $M_i = M/(x_1M + \cdots + x_iM)$ is Hausdorff in the $\mathfrak{a}$-adic topology for each i. Then the sequence $(x_1, \ldots, x_s)$ is completely secant for M.*

Proof. When $s = 1$, we have $\bigcap_n M_n = \bigcap_n \mathfrak{a}^n M$ and the sequence $\{\xi_1\}$ is completely secant for $\mathrm{gr}(M)$ if and only if the homothety with ratio ξ_1 in $\mathrm{gr}(M)$ is injective. The claim then results immediately from Corollary 16.4.24 applied to the homothety $\phi = h_{x_1}$ in M.

Suppose then $s \geq 2$ and we prove by induction on s. By the induction hypothesis applied on $M_1 = M/x_1M$ with the quoteint filtration $\mathcal{F}_1$ and the sequence $(x_2, \ldots, x_s)$, we have

$$H^{(s-1)}_{\overline{M},\overline{F}} \geq \prod_{i=2}^{s}(1 - T^{\delta_i})H^{(s-1)}_{M_1,\mathcal{F}_1} \tag{4.2.14}$$

and the equality holds if and only if the sequence $(\xi_2, \ldots, \xi_s)$ is completely secant for the $\mathrm{gr}(A)$-module $\mathrm{gr}(M_1)$. Since the element $(1 - T^{\delta_1})/(1 - T)$ is positive, the case $s = 1$ already treated and the formula (4.2.14) provide the inequalities

$$H^{(s)}_{\overline{M},\overline{\mathcal{F}}} \geq \prod_{i=2}^{s}(1 - T^{\delta_i})H^{(s)}_{M_1,\mathcal{F}_1} \geq \prod_{i=1}^{s}(1 - T^{\delta_i})H^{(s)}_{M_1,\mathcal{F}_1} \tag{4.2.15}$$

which proves (a).

We can have equality in (4.2.13) only if we have simultaneously equality in (4.2.14) and equality

$$H^{(1)}_{M_1,\mathcal{F}_1} = (1 - T^{\delta_1})H^{(1)}_{M,\mathcal{F}}. \tag{4.2.16}$$

This last relation means that $\{\xi_1\}$ is completely secant for $\mathrm{gr}(M)$ and implies that the canonical homomorphism from $\mathrm{gr}(M)/\xi_1\mathrm{gr}(M)$ to $\mathrm{gr}(M_1)$ is a isomorphism. In other words, we have equality in (4.2.13) if and only if $\{\xi_1\}$ is completely secant for $\mathrm{gr}(M)$ and $\{\xi_2, \ldots, \xi_s\}$ is completely secant for $\mathrm{gr}(M)$. This means $\{\xi_1, \ldots, \xi_s\}$ is completely secant for $\mathrm{gr}(M)$. We have thus demonstrated the equivalence of the two conditions of (b).

Now suppose that $\{\xi_1, \ldots, \xi_s\}$ is completely secant for $\mathrm{gr}(M)$ and M_i is Hausdorff for the $\mathfrak{a}$-adic topology for all i. According to the above argument and the induction hypothesis, the sequence $(x_2, \ldots, x_s)$ is completely secant for M_1. As we have $M_1 = M/x_1M$ and that $\{x_1\}$ is completely secant for M, the sequence $(x_1, x_2, \ldots, x_s)$ is completely secant for M. □

16.5 Regular local rings

16.5.1 Regularity of a local ring

Let $(A, \mathfrak{m})$ be a Noetherian local ring and $(x_i)_{i\in I}$ a family of elements of $\mathfrak{m}$. In view of Corollary 10.3.8, it amounts to the same thing to suppose that the family $(x_i)_{i\in I}$ generates the ideal $\mathfrak{m}$ of A, or that the classes of x_i modulo $\mathfrak{m}^2$ generate the κ_A-vector space $\mathfrak{m}/\mathfrak{m}^2$. In this case, we have $\dim(A) \leq |I|$ by Corollary 16.3.15, and therefore

$$\dim(A) \leq [\mathfrak{m}/\mathfrak{m}^2 : \kappa_A] \leq |I|$$

for every generating family $(x_i)_{i\in I}$ of the ideal $\mathfrak{m}$.

Definition 16.5.1. *A Noetherian local ring $(A, \mathfrak{m})$ is called **regular** if $\dim(A) = [\mathfrak{m}/\mathfrak{m}^2, \kappa_A]$. A family of elements of $\mathfrak{m}$ whose calsses modulo $\mathfrak{m}^2$ form a basis of the κ_A-space $\mathfrak{m}/\mathfrak{m}^2$ is called a **system of parameters** for A.*

A system of parameters in a regular local ring A is therefore a finite family $(x_i)_{i\in I}$ generating the ideal $\mathfrak{m}$ of A and such that $|I| = \dim(A)$. Conversely, if the maximal ideal $\mathfrak{m}$ of a Noetherian local ring A is generated by d elements with $d \leq \dim(A)$, then the ring A is regular.

Example 16.5.2 (Examples of regular local rings).

(a) The regular local rings of dimension 0 (resp. 1) are the fields (resp. the discrete valuation rings). In fact, the claim is clear for dimension 0, and a discrete valuation ring is clearly regular (since it is a PID). Conversely, assume that $(A, \mathfrak{m})$ is a regular local ring of dimension one, with t its generator of $\mathfrak{m}$. For all $n \geq 0$ we have $\dim_{\kappa_A}(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = 1$ because it is generated by t^n (and it cannot be zero since otherwise $\mathfrak{m}$ will be the nilradical of A, which implies $\dim(A) = 0$, contradiction). In particular $\mathfrak{m}^n = (t^n)$ and the graded ring $\mathrm{gr}_{\mathfrak{m}}(A)$ is isomorphic to the polynomial ring $\kappa_A[T]$. For $x \in A \setminus \{0\}$, define $v(x)$ to be the largest integer n such that $x \in \mathfrak{m}^n$. Then we have $v(xy) = v(x) + v(y)$ for all $x, y \in A \setminus \{0\}$. We extend this to the field of fractions K of A. Then it is clear that A is the set of elements of K which have positive valuation. Hence we see that A is a discrete valuation ring. Note that if $(A, \mathfrak{m})$ is a discrete valuation ring, then an element t of $\mathfrak{m}$ is a uniformizer if and only if $\{t\}$ is a system of parameters of A.

(b) Let k be a field and n a positive integer. The ring $A = k[\![X_1, \dots, X_n]\!]$ is Noetherian and local with dimension n. Since its maximal ideal $\mathfrak{m}$ is generated by $X_1, \dots, X_n$, we see A is regular. Moreover, a sequence $(F_1, \dots, F_n)$ is a system of parameters if and only if their image in $\mathfrak{m}/\mathfrak{m}^2$ is lineraly independent, or equivalently the Jacobi matrix $(\partial F_i/\partial X_j)$ is nonsingular at the point 0.

More generally, let A be a regular local ring of dimension r. The ring $A[\![X_1, \dots, X_n]\!]$ is then a regular local ring of dimension $r + n$. If $(a_1, \dots, a_r)$ is a system of parameters for A, then $(a_1, \dots, a_r, X_1, \dots, X_n)$ is a system of parameters for $A[\![X_1, \dots, X_n]\!]$.

(c) Let A be a regular local ring of dimension r. The ring $A\{X_1, \dots, X_n\}$ of restricted formal power series is a regular local ring of dimension $n + r$. If $(a_1, \dots, a_r)$ is a system of parameters for A, then $(a_1, \dots, a_r, X_1, \dots, X_n)$ is a system of parameters for $A\{X_1, \dots, X_n\}$.

(d) Let k be a field, A a finitely generated k-algebra that is an integral domain and $\mathfrak{m}$ a maximal ideal of A. Then the Noetherian local ring $A_{\mathfrak{m}}$ is regular if and only if we have $\dim(A) = [\mathfrak{m}/\mathfrak{m}^2 : A/\mathfrak{m}]$. In fact, we have $\dim(A_{\mathfrak{m}}) = \dim(A)$ by Theorem 16.2.11 and the $A/\mathfrak{m}$-vector space $\mathfrak{m}A_{\mathfrak{m}}/(\mathfrak{m}A_{\mathfrak{m}})^2$ is isomorphic to $\mathfrak{m}/\mathfrak{m}^2$. In particular, if k is algebraically closed, this condition is equivalent to $\dim(A) = [\mathfrak{m}/\mathfrak{m}^2 : k]$ by the Nullstellensatz.

(e) Let A be a regular local ring. We will see later that the local ring $A_{\mathfrak{p}}$ is regular for any prime ideal $\mathfrak{p}$ of A.

Proposition 16.5.3. *Let $\rho : A \to B$ be a local homomorphism of Noetherian local rings such that B is flat over A. Suppose that $\mathfrak{m}_B = \mathfrak{m}_A^e$, then $\dim(B) = \dim(A)$ and B is regular if and only if A is regular.*

Proof. The first assertion follows from Proposition 16.3.24. Since B is flat over A, we can identify $\mathfrak{m}_B/\mathfrak{m}_B^2$ with $B \otimes_A (\mathfrak{m}_A/\mathfrak{m}_A^2)$ or with $\kappa_B \otimes_{\kappa_A} (\mathfrak{m}_A/\mathfrak{m}_A^2)$. We then have

$$[\mathfrak{m}_B/\mathfrak{m}_B^2 : \kappa_A] = [\mathfrak{m}_A/\mathfrak{m}_A^2 : \kappa_A]$$

so the second claim follows. □

Corollary 16.5.4. *A Noetherian local ring A is regular if and only if its completion $\widehat{A}$ is.*

Proof. The completion $\widehat{A}$ is flat over A and $\hat{\mathfrak{m}}$ is generated by $\mathfrak{m}$ in $\widehat{A}$, so we can apply Proposition 16.5.3. □

Theorem 16.5.5. *Let A be a Noetherian local ring. The following conditions are equivalent:*

(i) A is regular.

(ii) The ideal $\mathfrak{m}_A$ is generated by a subset of $\mathfrak{m}_A$ secant for A.

(iii) The ideal $\mathfrak{m}_A$ is generated by a subset of $\mathfrak{m}_A$ completely secant for A.

(iv) The homomorphism $\gamma : S(\mathfrak{m}_A/\mathfrak{m}_A^2) \to \mathrm{gr}(A)$ is bijective.

(v) There exists a positive integer r such that $H_{A,\mathfrak{m}_A} = (1-T)^{-r}$.

(vi) We have $H_{A,\mathfrak{m}_A} = (1-T)^{-d}$ where $d = \dim(A)$.

If these conditions are fulfilled, every system of parameters for A is a completely secant sequence for A.

Proof. Since every secant subset has cardinality smaller than $\dim(A)$, we see (iii)⇒(ii)⇒(i). To see (iv)⇒(iii), let $(x_1, \dots, x_r)$ be a sequence of elements of $\mathfrak{m}_A$ whose classes modulo $\mathfrak{m}_A^2$ form a basis $(\xi_1, \dots, \xi_r)$ for $\mathfrak{m}_A/\mathfrak{m}_A^2$. If property (iv) is satisfied, $\mathrm{gr}(A)$ is then the polynomial algebra $\kappa_A[\xi_1, \dots, \xi_r]$ and the sequence $(x_1, \dots, x_r)$ is completely secant by **??**. This also proves the last assertion of the theorem.

Let $r = [\mathfrak{m}_A/\mathfrak{m}_A^2 : \kappa_A]$. Then the Poincaré series of the graded module $S = S(\mathfrak{m}_A/\mathfrak{m}_A^2)$ over κ_A is equal to

$$P_S = \sum_{n\in\mathbb{N}} [S_n : \kappa_A] T^n = (1-T)^{-r}.$$

Suppose that the homomorphism γ is not bijective. As γ is surjective, there exists a homogeneous element u of S of degree $d > 0$, canceled by γ. Then

$$H_{A,\mathfrak{m}_A} = P_S - P_{\ker\gamma} \le P_S - P_{uS} = (1-T^d)(1-T)^{-r} = (1+T+\cdots+T^{d-1})(1-T)^{-(r-1)}.$$

By Theorem 16.4.19 and Lemma 16.4.3, we get $\dim(A) < r$, so A is not regular.

Finally, let us prove the equivalence of conditions (iv) and (vi). If we have $H_{A,\mathfrak{m}_A} = (1-T)^{-r}$ for some r, then by Theorem 16.4.19 we must have $r = \dim(A)$. Also, $[\mathfrak{m}_A/\mathfrak{m}_A^2 : \kappa_A] = r$ because $(1-T)^{-r} = 1 + rT + \cdots$. Therefore our claim follows. □

Corollary 16.5.6. *A regular local ring is integrally closed, and in particular an integral domain.*

Proof. If A is a regular local ring, then $\mathrm{gr}(A)$ is isomorphic to a polynomial algebra over a field, so it is integrally closed. Since A is a Zariski ring, by Proposition 13.1.37 we see A is integrally closed. □

Corollary 16.5.7. *Let $\rho : A \to B$ be a local homomorphism of Noetherian local rings. Suppose that A is complete and B is regular. Then for ρ to be bijective, it is necessary and sufficient that it induces bijections of κ_A on κ_B and of $\mathfrak{m}_A/\mathfrak{m}_A^2$ to $\mathfrak{m}_B/\mathfrak{m}_B^2$.*

Proof. These conditions are clearly necessary. Suppose now ρ induces bijections of κ_A on κ_B and of $\mathfrak{m}_A/\mathfrak{m}_A^2$ to $\mathfrak{m}_B/\mathfrak{m}_B^2$. Since the ring $\mathrm{gr}(A)$ is generated by $\mathrm{gr}_0(A)$ and $\mathrm{gr}_1(A)$, it follows that $\mathrm{gr}(\rho)$ is bijective. Therefore ρ is bijective by Theorem 11.3.29. □

Corollary 16.5.8. *Let k be a ring and A a Noetherian local k-algebra with residue field equal to k. Then A is regular if and only if the completion $\widehat{A}$ is isomorphic to a formal series ring $k[\![X_1, \dots, X_n]\!]$.*

Proof. This follows from Theorem 16.5.5 and Proposition 11.3.38. □

16.5.2 Quotients of regular local rings

Proposition 16.5.9. *Let A be a Noetherian local ring, $\boldsymbol{x} = (x_1, \dots, x_r)$ a sequence of elements of $\mathfrak{m}_A$ and $\mathfrak{x}$ the ideal it generates. The following conditions are equivalent.*

(i) A is regular and $\boldsymbol{x}$ can be extended to a system of parameters for A.

(ii) $A/\mathfrak{x}$ is regular and $\boldsymbol{x}$ is secant for A.

(iii) $A/\mathfrak{x}$ is regular and $\boldsymbol{x}$ is completely secant for A.

Moreover, if these conditions are satisfied, then $\mathfrak{x}$ is a prime ideal of A.

Proof. Clearly (iii) implies (ii). Suppose now that $\boldsymbol{x}$ is secant for A and the Noetherian local ring $A/\mathfrak{x}$ is regular. Let $(x_{r+1}, \dots, x_d)$ be a sequence of elements of A whose class modulo I form a system of parameters for $A/\mathfrak{x}$. Then the sequence $(x_1, \dots, x_d)$ generates the maixmal ideal $\mathfrak{m}_A$ of A, and we have

$$\dim(A) = r + \dim(A/\mathfrak{x}) = r + (d - r) = d.$$

Therefore, A is regular and $(x_1, \dots, x_d)$ is a system of parameters for A.

Finally, assume that (i) is satisfied. Then A is regular and $\boldsymbol{x}$ is completely secant for A, hence secant for A. Then we have

$$\dim(A/\mathfrak{x}) = \dim(A) - r$$

and the classes $x_1, \dots, x_r$ modulo $\mathfrak{m}_A^2$ is lineraly independent over κ_A, so

$$[\mathfrak{m}_A/(\mathfrak{m}_A^2 + \mathfrak{x}) : \kappa_A] = [\mathfrak{m}_A/\mathfrak{m}_A^2 : \kappa_A] - r.$$

Therefore we see $A/\mathfrak{x}$ is regular, and in particular $\mathfrak{x}$ is prime since $A/\mathfrak{x}$ is integral. □

Corollary 16.5.10. *Let A be a Noetherian local ring and x and element of $\mathfrak{m}_A$. The following conditions are equivalent.*

(i) A is regular, and x does not belong to $\mathfrak{m}_A$.

(ii) A/xA is regular and $\dim(A/xA) = \dim(A) - 1$.

(iii) A/xA *is regular and* x *is not a divisor of* 0 *in* A.

Proof. This follows by applying Proposition 16.5.9 on $\mathfrak{x} = xA$. □

Corollary 16.5.11. *Let* A *be a regular local ring and* $\mathfrak{a}$ *an ideal of* A*. Then* $A/\mathfrak{a}$ *is regular if and only if* $\mathfrak{a}$ *is generated by a subset of a system of parameters for* A.

Proof. The condition is sufficient by Proposition 16.5.9. Suppose now $A/\mathfrak{a}$ is regular, and $\boldsymbol{x} = (x_1, \dots, x_r)$ a sequence of elements of $\mathfrak{a}$ whose classes module $\mathfrak{m}_A^2$ form a basis for $(\mathfrak{a} + \mathfrak{m}_A^2)/\mathfrak{m}_A^2$ over κ_A. Let I be the ideal generated by $\boldsymbol{x}$, so we have $I \subseteq \mathfrak{a}$ and $\boldsymbol{x}$ is part of a system of parameters for A, so the local Noetherian ring A/I is regular. Moreover, the vector spaces $\mathfrak{m}_A/(\mathfrak{a} + \mathfrak{m}_A^2)$ and $\mathfrak{m}_A/(I + \mathfrak{m}_A^2)$ have the same dimension over κ_A. Consequently, the regular local rings $A/\mathfrak{a}$ and A/I have the same dimension. As the ideals $\mathfrak{a}$ and I are prime and we have $I \subseteq \mathfrak{a}$, we finally have $\mathfrak{a} = I$. □

Example 16.5.12. Let k be a field. Then the ring $A = k[\![X_1, \dots, X_n]\!]$ of power series is local. Let $\mathfrak{a}$ be a proper ideal of A. By Corollary 16.5.11, for $A/\mathfrak{a}$ to be regular, it is necessary and sufficient that we can find a positive integer r and elements $F_1, \dots, F_r$ of A, generating $\mathfrak{a}$, and such that the matrix $(\partial F_i/\partial X_j(0))$ is of rank r (Jacobian criterion). We then have $\dim(A/\mathfrak{a}) = n - r$.

16.5.3 Eisenstein polynomials

Let A be a ring, $\mathfrak{p}$ a prime ideal of A, and P a polynomial in $A[T]$. We say P is an **Eisenstein polynomial** for $\mathfrak{p}$ if it satisfies the following conditions:

(a) P is monic with degree $d \geq 2$;

(b) $P(T) \equiv T^d \bmod \mathfrak{p}A[T]$;

(c) $P(0) \notin \mathfrak{p}^2$.

In other words, an Eisenstein polynomial for $\mathfrak{p}$ is a polynomial of the form $P(T) = T^d + \sum_{i=0}^{d-1} a_i T^i$, with $d \geq 1$, $a_1, \dots, a_{d-1}$ belong to $\mathfrak{p}$ and $a_0 \in \mathfrak{p} \setminus \mathfrak{p}^2$.

We say P is an Eisenstein polynomial for $\mathfrak{p}A_\mathfrak{p}$ if the canonical image of P in the polynomial ring $A_\mathfrak{p}[T]$ is an Eisenstein polynomial for the ideal $\mathfrak{p}A_\mathfrak{p}$. This means P is an Eisenstein polynomial for $\mathfrak{p}$ and that it also satisfies the following condition, stronger than (c):

(c′) any element a in A such that $aP(0) \in \mathfrak{p}^2$ belongs to $\mathfrak{p}$.

Proposition 16.5.13. *Let* A *be a ring,* $\mathfrak{p}$ *a prime ideal of* A *and* $P \in A[T]$ *an Eisenstein polynomial for* $\mathfrak{p}$.

(a) P *has no decomposition of the form* $P = P_1P_2$*, where* P_1, P_2 *are two monic polynomials in* $A[T]$ *unequal to* 1.

(b) Suppose that A *is integrally closed with* K *its fraction field. Then* P *is irreducible in* $K[T]$.

Proof. Let π be the canonical map from A to the residue field $\kappa(\mathfrak{p})$ of $\mathfrak{p}$ and $\tilde{\pi} : A[T] \to \kappa(\mathfrak{p})[T]$ be the extension of π such that $\tilde{\pi}(T) = T$. Suppose that $P = P_1P_2$ where P_1, P_2 are two monic polynomials unequal to 1. Then we have $\tilde{\pi}(P) = T^d = \tilde{\pi}(P_1)\tilde{\pi}(P_2)$ in $\kappa(\mathfrak{p})[T]$, with d the degree of P. If d_i is the degree of P_i, we get $\tilde{\pi}(P_i) = T^{d_i}$, which means $P_i(T) \equiv T^{d_i} \bmod \mathfrak{p}A[T]$, in particular $P_i(0) \in \mathfrak{p}$. BUt then $P(0) = P_1(0)P_2(0) \in \mathfrak{p}^2$, which is a contradiction. The assertion (b) now follows from (a). □

Proposition 16.5.14. *Let A be a Noetherian local ring and $P_1, \dots, P_r$ be monic polynomials in $A[T]$ such that $P_i(T) \equiv T^{d_i}$ mod $\mathfrak{m}_A A[T]$ and $\deg(P_i) \geq 2$ for each i. Let $\mathfrak{q}$ be the ideal in $A[T_1, \dots, T_r]$ generated by $P_1(T_1), \dots, P_r(T_r)$ and B the A-algebra $A[T_1, \dots, T_r]/\mathfrak{q}$. For each i, we denote by d_i the degree of P_i, ξ_i the class of T_i mod $\mathfrak{q}$, and γ_i the class of $c_i = P_i(0)$ mod $\mathfrak{m}_A^2$.*

(a) B is a Noetherian local ring with maximal ideal

$$\mathfrak{m}_B = B\mathfrak{m}_A + \sum_{i=1}^{r} B\xi_i.$$

We have $\dim(A) = \dim(B)$ and $[\kappa_B : \kappa_A] = 1$. Moreover, the monomials $\xi_1^{\alpha_1} \cdots \xi_r^{\alpha_r}$, with $0 \leq \alpha_i < d$ for $1 \leq i \leq r$, form a basis for the A-module B.

(b) Let λ be the canonical homomorphism from $\mathfrak{m}_A/\mathfrak{m}_A^2$ to $\mathfrak{m}_B/\mathfrak{m}_B^2$. Then the kernel of λ is the κ_A-vector space generated by $\gamma_1, \dots, \gamma_r$ and the classes $\xi_1, \dots, \xi_r$ form a basis over κ_A for the cokernel of λ.

(c) For B to be regular, it is necessary and sufficient that A is regular and the $\gamma_1, \dots, \gamma_r$ is linearly independent in the κ_A-vector space $\mathfrak{m}_A/\mathfrak{m}_A^2$.

Proof. The A-algebra B is isomomorphic to the tensor product $B_1 \otimes_A \otimes \cdots \otimes_A B_r$ where $B_i = A[T]/(P_i)$ for each i. It then follows that the monomials $\xi_1^{\alpha_1} \cdots \xi_r^{\alpha_r}$, with $0 \leq \alpha_i < d$ for $1 \leq i \leq r$, form a basis for the A-module B. In particular, B is integral over A, so A and B has the same dimension.

By Corollary 12.2.22, B is Noetherian, and any maximal ideal of B contains $B\mathfrak{m}_A$. COnversely, from the hypothesis on $P_1, \dots, P_r$ and the relations $P_i(\xi_i) = 0$, we get $\xi_i^{d_i} \in B\mathfrak{m}_A$ for each i. Therefore any maximal ideal of B containing $\xi_1, \dots, \xi_r$ must contains the ideal $\mathfrak{n} = B\mathfrak{m}_A + B\xi_1 + \cdots + B\xi_r$. But we have $\mathfrak{m}_A = A \cap \mathfrak{n}$ and $B = A + \mathfrak{n}$, so $B/\mathfrak{n}$ is isomomorphic to $A/\mathfrak{m}_A$ and therefore is maixmal in B. This shows B is local with maximal ideal $B\mathfrak{m}_A + \sum_{i=1}^r B\xi_i$, and we have $[\kappa_B : \kappa_A] = 1$. This proves (a).

Let φ be the canonical homomorphism of $(A/\mathfrak{m}_A^2)[T_1, \dots, T_r]$ to $B/\mathfrak{m}_B^2$. By part (a), the kernel of φ is the ideal generated by the classes $\bar{P}_i(T_i)$ of $P_i(T_i)$ modulo $\mathfrak{m}_A^2 A[T_1, \dots, T_r]$, the monomials T_iT_j, and xT_i with $1 \leq i, j \leq r$ and $x \in \mathfrak{m}_A/\mathfrak{m}_A^2$. By hypothesis, we have $P_i(T) \equiv T^{d_i}$ mod $\mathfrak{m}_A A[T]$, so we can replace $\bar{P}_i(T_i)$ with γ_i in the description above. As a result, if we set $\mathfrak{r} = \mathfrak{m}_A^2 + \sum_{i=1}^r Ac_i$, the ring $B/\mathfrak{m}_B^2$ is then isomomorphic to $(A/\mathfrak{r})[T_1, \dots, T_r]$ quotient the ideal generated by the monomials T_iT_j and xT_i, with $1 \leq i, j \leq r$ and $x \in \mathfrak{m}_A/\mathfrak{r}$. If we denote by τ_i the class of ξ_i modulo $\mathfrak{m}_B^2$, this means

$$B/\mathfrak{m}_B^2 = (A/\mathfrak{r}) \oplus \kappa_A\tau_1 \oplus \cdots \oplus \kappa_A\tau_r. \tag{5.3.1}$$

and

$$\mathfrak{m}_B/\mathfrak{m}_B^2 = (\mathfrak{m}_A/\mathfrak{r}) \oplus \kappa_A\tau_1 \oplus \cdots \oplus \kappa_A\tau_r. \tag{5.3.2}$$

Assertion (b) now follows from these.

According to formula (5.3.2) and the relation $[\kappa_B : \kappa_A] = 1$, we get

$$[\mathfrak{m}_B/\mathfrak{m}_B^2 : \kappa_B] = [\mathfrak{m}_A/\mathfrak{m}_A^2 : \kappa_A] + (r - [\mathfrak{r}/\mathfrak{m}_A^2 : \kappa_A]). \tag{5.3.3}$$

But the κ_A-vector space $\mathfrak{r}/\mathfrak{m}_A^2$ is generated by $\gamma_1, \ldots, \gamma_r$, and we have

$$\dim(B) = \dim(A) \leq [\mathfrak{m}_A/\mathfrak{m}_A^2 : \kappa_A]. \tag{5.3.4}$$

Combine formula (5.3.3) and formula (5.3.4), we see assertion (c) follows. □

Corollary 16.5.15. *Let A be a regular Noetherian local ring and $P \in A[T]$ an Eisenstein polynomial for $\mathfrak{m}_A$. Then $B = A[T]/(P)$ is a Noetherian local regular ring, with the same dimension as A, and $[\kappa_B : \kappa_A] = 1$. In fact, we have $\mathfrak{m}_B = B\mathfrak{m}_A + B\xi$, where ξ is the class of T modulo (P).*

Proof. By definition we have $\deg(P) \geq 2$ and $P(T) \equiv T^d \bmod \mathfrak{m}_A$, so this is a special case of Proposition 16.5.14 with $r = 1$. □

Proposition 16.5.16. *Let A be an integral domain, with fraction field K, and L an algebraic extension of K. Let B be the integral closure of A in L and $\mathfrak{p}$ a prime ideal of A. Suppose that the local ring $A_\mathfrak{p}$ is regular and Noetherian; let ξ be a primitive element for L over K (i.e., $L = K(\xi)$) and suppose that the minimal polynomial of ξ over K is an Eisenstein polynomial $P \in A[T]$ for $\mathfrak{p}A_\mathfrak{p}$.*

(a) There exists in B a unique prime ideal $\mathfrak{P}$ lying over $\mathfrak{p}$.

(b) The local ring $B_\mathfrak{P}$ is Noetherian and regular, with the same dimension as $A_\mathfrak{p}$. Moreover, $B_\mathfrak{P} = A_\mathfrak{p}[\xi]$.

(d) The canonical homomorphism from $A/\mathfrak{p}$ to $B/\mathfrak{P}$ induces an isomorphism on the fraction fields.

Proof. Set $C = A_\mathfrak{p}[\xi]$ and let d be the degree of P. By Proposition 16.5.14 applied to the ring $A_\mathfrak{p}$, the Eisenstein polynomial P is irreducible in $K[T]$ and $(1, \xi, \ldots, \xi^{d-1})$ is a basis for L over K, and for C over $A_\mathfrak{p}$. Since P is monic, the kernel of the canonical homomorphism from $A_\mathfrak{p}[T]$ to C is equal to (P); in other words, $C = A_\mathfrak{p}[T]/(P)$, so we can apply Corollary 16.5.15: C is a regular Noetherian local with dimension equal to that of $A_\mathfrak{p}$, the maximal ideal $\mathfrak{m}_C$ of C is generated by $\mathfrak{p} \cup \{\xi\}$ and the residue field κ_C is a trivial extension of $\kappa(\mathfrak{p})$. To prove the proposition, it suffices to find a unique prime ideal $\mathfrak{P}$ of B lying over $\mathfrak{p}$, and such that $C = B_\mathfrak{P}$.

Let $S = A - \mathfrak{p}$, then the integral closure of $A_\mathfrak{p}$ in L is equal to $S^{-1}B$. But t is integral over $A_\mathfrak{p}$, and $C = A_\mathfrak{p}[\xi]$ is a regular local ring, hence integrally closed (Corollary 16.5.6). It then follows that $C = S^{-1}B$, so $S^{-1}B$ is local. By Theorem 13.1.67 and Corollary 13.1.63, there then exists a unique prime ideal of $S^{-1}B$ lying over $\mathfrak{p}A_\mathfrak{p}$, which corresponds to a unique prime ideal $\mathfrak{P}$ of B lying over $\mathfrak{p}$, and we have $B_\mathfrak{P} = S^{-1}B = C$ (Lemma 13.1.61). □

Corollary 16.5.17. *With the hypothesis in Proposition 16.5.16, suppose that $A_\mathfrak{p}$ is a DVR. Then $B_\mathfrak{P}$ is a DVR, ξ is a uniformizer for $B_\mathfrak{P}$, and we have*

$$f(B_\mathfrak{P}/A_\mathfrak{p}) = 1, \quad e(B_\mathfrak{P}/A_\mathfrak{p}) = [L : K]. \tag{5.3.5}$$

Proof. In fact, DVRs are regular Noetherian local rings with dimension 1; set $d = [L : K]$ and $P(T) = T^d + \sum_{i=0}^{d-1} a_i T^i$. Let $v_\mathfrak{P}$ be the valuation on $B_\mathfrak{P}$. Then since P is an Eisenstein polynomial, $a_0 \in \mathfrak{m}_{A_\mathfrak{p}} \setminus \mathfrak{m}_{A_\mathfrak{p}}^2$ and $a_i \in \mathfrak{m}_{A_\mathfrak{p}}$ for each i, whence

$$d = v_\mathfrak{P}(\xi^d) = v_\mathfrak{P}(-\sum_{i=0}^{d-1} a_i \xi^i) = \min_i\{v_\mathfrak{P}(a_i) + i\} = v_\mathfrak{P}(a_0).$$

This shows $d = e(B_{\mathfrak{P}}/A_{\mathfrak{p}})$. Since $[\kappa_B : \kappa_A] = 1$, we also have $f(B_{\mathfrak{P}}/A_{\mathfrak{p}}) = 1$. □

Example 16.5.18 (Examples of extensions by Eisenstein polynomials).

(a) Let $A = \mathbb{Z}$ and $L = \mathbb{Q}(p^{1/d})$, where p is a prime number and $d \geq 2$. Let B be the integral closure of $\mathbb{Z}$ in L. Then $P(T) = T^d - p$ is an Eisenstein polynomial in $\mathbb{Z}[T]$ for $p\mathbb{Z}_{(p)}$, and there exists a unique prime ideal $\mathfrak{P}$ of B lying over $p\mathbb{Z}$. Since $Z_{(p)}$ is a DVR, there exists on $Q(p^{1/d})$ a unique discrete valuation $v_{\mathfrak{P}}$ such that $v(p) > 0$. We have $[L : K] = v_{\mathfrak{P}}(p) = d$, and $B/\mathfrak{P}$ is a field with p elements. The valuation ring $B_{\mathfrak{P}}$ of $v_{\mathfrak{P}}$ is equal to $\mathbb{Z}_{(p)}[p^{1/d}]$.

(b) Let $A = \mathbb{Z}$ and $L = \mathbb{Q}(\zeta)$ where $\zeta = e^{2\pi i/p^f}$, with p a prime and $f \geq 1$. Let B be the integral closure of $\mathbb{Z}$ in L and P the polynomial in $\mathbb{Z}[T]$ defined by

$$P(T-1) = \frac{T^{p^f} - 1}{T^{p^{f-1}} - 1}.$$

Set $d = p^f - p^{f-1}$. We have $P(\zeta - 1) = 0$, $P(0) = p$, and

$$P(T-1) \equiv (T-1)^d \mod p\mathbb{Z}[T],$$

so $P(T) \equiv T^d$. Therefore P is an Eisenstein polynomial for $p\mathbb{Z}_{(p)}$. There exists a unique prime ideal $\mathfrak{P}$ of B lying over $\mathfrak{p}\mathbb{Z}$, and we have $B_{\mathfrak{P}} = \mathbb{Z}_{(p)}[\zeta]$. Moreover, $\zeta - 1$ is a uniformizer for $B_{\mathfrak{P}}$ and

$$[L : K] = d = p^f - p^{f-1}.$$

If $v_{\mathfrak{P}}$ is the unique normalized valuation on $\mathbb{Q}(\zeta)$ such that $v_{\mathfrak{P}}(p) > 0$, we have $v_{\mathfrak{P}}(p) = d$. Moreover, the field $B/\mathfrak{P}$ has p elements. We can prove that B is equal to $\mathbb{Z}[\zeta]$.

16.6 Dimension and graded rings

Let R be a graded ring of type $\mathbb{Z}$ and $(R_n)_{n\in\mathbb{Z}}$ its graduation; we assume that $R_n = 0$ for $n < 0$. For each $n \in \mathbb{Z}$, let $R_{\geq n} = \bigoplus_{i\geq n} R_i$. We have $R = R_{\geq 0}$ and each $R_{\geq n}$ is an homogeneous ideal of R. Denote by S the multiplicative subset $1 + R_{\geq n}$ consists of elements of R with degree zero term equals to 1, and consider the localization $S^{-1}R$. By identifying R with a subring of $\widehat{R} = \prod_n R_n$, we see S is invertible in the completion $\widehat{R}$, whence $S^{-1}R$ can be identified with a subring of $\widehat{R}$ containing R. For $s \in S$ and $a \in R_{\geq n}$, the element $s^{-1}a - a$ of $\widehat{R}$ belongs to $\prod_{i\geq n+1} R_i$; therefore we have $S^{-1}R_{\geq n} = (S^{-1}R) \cap \prod_{i\geq n} R_i$. From these we deduce the following results:

Proposition 16.6.1. *Let $R = \bigoplus_{n\geq 0} R_n$ be a graded ring and S be defined as above.*

(a) The ideals $S^{-1}R_{\geq n}$ form an exhaustive and separated filtration of $S^{-1}R$.

(b) The homomorphism $i_S : R \to S^{-1}R$ induces an isomorphism u_n of R_n to $S^{-1}R_{\geq n}/S^{-1}R_{\geq n+1}$ for each n; the u_n are homogeneous components of an isomorphism of R onto the graded ring associated with $S^{-1}R$, filtered by $S^{-1}R_{\geq n}$.

Remark 16.6.1. Rn element a/s of $S^{-1}R$ with $a \in R$, $s \in S$, is invertible if and only if the degree 0 component of a is invertible in R_0. Therefore, if R_0 is a local ring, so is $S^{-1}R$ and the canonical injection $R_0 \to S^{-1}R$ induces an isomorphism on residue fields.

Remark 16.6.2. Suppose that R is generated by R_0 and R_1; then for each n we have $R_{n+1} = R_1 \cdot R_n$, so $R_{\geq n+1} = R_1 \cdot R_{\geq n}$ and $S^{-1}R_{\geq n+1} = R_1 \cdot S^{-1}R_{\geq n}$. As a result, the filtration $(S^{-1}R_{\geq n})$ of $S^{-1}R$ is $S^{-1}R_{\geq 1}$-adic.

Example 16.6.2.

(a) Let $\mathfrak{p}$ be a homogeneous prime ideal of $\mathbb{C}[X_0, \ldots, X_n]$ different to the ideal generated by the X_i's (denoted by $\mathfrak{m}$). Let $X \subseteq \mathbb{CP}^n$ be the projective variety defined by $\mathfrak{p}$ and C the algebraic variety in $\mathbb{C}^{n+1}$ defined by $\mathfrak{p}$ (so that C the **cone** of X). Let $R = \mathbb{C}[X_0, \ldots, X_n]/\mathfrak{p}$ be the coordinate ring of C and consider the localization $S^{-1}R$. We claim that $S^{-1}R$ is the local ring at the origin, that is, $S^{-1}R = R_{\mathfrak{m}_0}$. This follows from the fact that a prime ideal $\mathfrak{q}$ is disjoint from S if and only if every element of $\mathfrak{q}$ has zero constant term, or equivalently is contained in the maximal ideal $\mathfrak{m}$. (Therefore S and $R \setminus \mathfrak{m}/\mathfrak{p}$ have the same saturation.)

(b) Let A be a local ring and $\mathfrak{a}$ a proper ideal of A. Then $R = \bigoplus_n \mathfrak{a}^n/\mathfrak{a}^{n+1}$ is a graded ring and $R_0 = A/\mathfrak{a}$ is local; it is generated by R_0 and R_1. The ring $S^{-1}R$ is then local and the filtration $(S^{-1}R_{\geq 1})$ is the $S^{-1}R_{\geq 1}$-adic filtration. Note that in general the rings A and $S^{-1}R$ are not isomorphic.

16.6.1 Dimension and chains of homogeneous ideals

In this part, we will use $\operatorname{dimgr}(R)$ to denote the supremum of the length of chains homogeneous prime ideals in R; similarly, if $\mathfrak{p}$ is a homogeneous ideal of R, we use $\operatorname{htgr}(\mathfrak{p})$ to denote the supremum of the length of chains homogeneous prime ideals in R for which $\mathfrak{p}$ is the largest element. Note that if $\mathfrak{p}$ is a homogeneous prime ideal of R, we have $\mathfrak{p} \cap S = \varnothing$; in fact, if $\mathfrak{p}$ contains an element with degree zero componenet 1, then $1 \in \mathfrak{p}$. The map $\mathfrak{p} \mapsto S^{-1}\mathfrak{p}$ from the set of homogeneous prime ideals of R to the set of prime ideals of $S^{-1}R$ is then injective and increasing. Concequently, we have

$$\operatorname{dimgr}(R) \leq \dim(S^{-1}R) \leq \dim(R), \quad \operatorname{htgr}(\mathfrak{p}) \leq \operatorname{ht}(S^{-1}\mathfrak{p}) = \operatorname{ht}(\mathfrak{p}). \tag{6.1.1}$$

Example 16.6.3. Let A be an arbitrary ring and consider the polynomial ring $A[X]$. For a homogeneous prime ideal $\mathfrak{p}$ of $A[X]$, we set $\mathfrak{p}_0 = \mathfrak{p} \cap A$ to be the constant part of elements in $\mathfrak{p}$. We distinguish two cases:

(a) If $X \in \mathfrak{p}$, then it is easy to see $\mathfrak{p} = \mathfrak{p}_0 + X \cdot A[X]$ because any polynomial $f \in \mathfrak{p}$ can be written as $f = f(0) + X \cdot g$.

(b) If $X \notin \mathfrak{p}$, then $\mathfrak{p} = \mathfrak{p}_0 \cdot A[X]$. In fact, let $f \in \mathfrak{p}$ and write

$$f(X) = a_0 + a_1 X + \cdots + a_n X^n$$

with $a_i \in A$. Then $a_0 \in \mathfrak{p}_0$ by definition, and we have $g = a_1 X + \cdots + a_n X^n \in \mathfrak{p}$. Note that g is divisible by X, so $g/X \in \mathfrak{p}$ since $\mathfrak{p}$ is prime and $X \notin \mathfrak{p}$. Replacing this process we eventually conclude that $a_i \in \mathfrak{p}_0$ for all i, whence $f \in \mathfrak{p}_0 \cdot A[X]$.

We now compute $\operatorname{htgr}(\mathfrak{p})$. Let $\mathfrak{q}_0 \subset \mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_n = \mathfrak{p}_0$ be a saturated chain in A, so that $n = \operatorname{ht}(\mathfrak{p}_0)$. Then by extending them in $A[X]$, we get a chain

$$\mathfrak{q}_0 \cdot A[X] \subset \mathfrak{q}_1 \cdot A[X] \subset \cdots \subset \mathfrak{q}_n \cdot A[X] = \mathfrak{p}_0 \cdot A[X].$$

In case (b), we have $\mathfrak{p} = \mathfrak{p}_0 \cdot A[X]$, and any homogeneous prime ideal $\mathfrak{p}' \subseteq \mathfrak{p}$ of $A[X]$ satisfies $\mathfrak{p}' = \mathfrak{p}'_0 \cdot A[X]$ (using the claim in (b)). From this, it is easy to conclude that $\operatorname{htgr}(\mathfrak{p}) = \operatorname{ht}(\mathfrak{p})$ in this case.

On the other hand, in case (a) we claim that the chain $\mathfrak{p}_0 \cdot A[X] \subseteq \mathfrak{p} = \mathfrak{p}_0 + X \cdot A[X]$ is saturated for homogeneous prime ideals of A, so that $\operatorname{htgr}(\mathfrak{p}) = \operatorname{ht}(\mathfrak{p}) + 1$. For this, let $\mathfrak{p}' \subseteq \mathfrak{p}$ be a homogeneous prime ideal containing $\mathfrak{p}_0 \cdot A[X]$ and choose $f \in \mathfrak{p}' \setminus (\mathfrak{p}_0 \cdot A[X])$; write $f = a_0 + a_1X + \cdots + a_nX^n$ as usual, and recall that $a_0 \in \mathfrak{p}_0$ with $a_i \notin \mathfrak{p}_0$. Since $f \notin \mathfrak{p}_0 \cdot A[X]$, we may assume that $a_d \notin \mathfrak{p}_0$ with $1 \leq d \leq n$. As $\mathfrak{p}'$ is homogeneous, each homogeneous componenet of f belongs to $\mathfrak{p}'$, so $a_dX^d \in \mathfrak{p}' \subseteq \mathfrak{p}$. But every element of $\mathfrak{p}$ has constant term in $\mathfrak{p}_0$ by definition and $\mathfrak{p}'$ is prime, so $X^d \in \mathfrak{p}'$, and therefore $X \in \mathfrak{p}'$. This shows $\mathfrak{p}' = \mathfrak{p}$ and justifies our claim.

In summary, we have proved the following equality

$$\operatorname{htgr}(\mathfrak{p}) = \begin{cases} \operatorname{ht}(\mathfrak{p}_0) + 1 & \text{if } X \in \mathfrak{p}, \\ \operatorname{ht}(\mathfrak{p}_0) & \text{if } X \notin \mathfrak{p}. \end{cases}$$

Now by taking $\mathfrak{p}$ to be the maximal ideals of $A[X]$, we deduce that $\operatorname{dimgr}(A[X]) \leq \dim(A) + 1$. However, it is easy to see this equality actually holds, for example we can take a saturated chain $\mathfrak{q}_0 \subset \mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_n$ in A, extending it to a chain

$$\mathfrak{q}_0 \cdot A[X] \subset \mathfrak{q}_1 \cdot A[X] \subset \cdots \subset \mathfrak{q}_n \cdot A[X] \subset \mathfrak{q}_n \cdot A[X] + X \cdot A[X].$$

It is easy to see the ideals above are homogeneous and prime, which shows $\operatorname{dimgr}(A[X]) \geq \dim(A) + 1$.

Finally, recall that in Exercise 16.2.7 we have shown that for any positive integers n and d with $n + 1 \leq d \leq 2n + 1$, there exists a ring A such that $\dim(A) = n$ $\dim(A[X]) = d$. In view of our previous result, we see the inequality in (6.1.1) can be strict. But also recall that for a Noetherian ring A, we always have $\dim(A[X]) = \dim(A) + 1$ (Corollary 16.3.28).

We now turn to our main theorem of this part, which asserts that if the graded ring R is Noetherian then $\operatorname{dimgr}(R) = \dim(R)$. First, we recall that for an arbitrary ideal $\mathfrak{a}$ of R, we denote by $\mathfrak{a}^h$ the ideal generated by homogeneous elements in $\mathfrak{a}$: in other words $\mathfrak{a}^h = \sum_n(\mathfrak{a} \cap R_n)$. We note that $\mathfrak{a}^h$ is a homogeneous and contained in $\mathfrak{a}$. Moreover, by Proposition 11.1.42, $\mathfrak{p}^h$ is prime if $\mathfrak{p}$ is prime.

Lemma 16.6.4. *Any maximal element of the set of homogeneous prime ideals of R is a maximal ideal of R containing $R_{\geq 1}$.*

Proof. Let $\mathfrak{m}$ be a proper homogeneous ideal of R. Then we have

$$\mathfrak{m} \subseteq (\mathfrak{m} \cap R_0) + R_{\geq 1} \neq R.$$

If $\mathfrak{m}$ is maximal, then $\mathfrak{m} = \mathfrak{m}_0 + R_{\geq 1}$, where $\mathfrak{m}_0$ is a maximal ideal of R_0. □

Lemma 16.6.5. *Let $\mathfrak{p}$ and $\mathfrak{q}$ be distinct prime ideals of R such that $\mathfrak{q} \subset \mathfrak{p}$. If $\mathfrak{q}^h = \mathfrak{p}^h$, then $\mathfrak{q}$ is homogeneous, $\mathfrak{p}$ is not homogeneous, and* $\operatorname{ht}(\mathfrak{p}/\mathfrak{q}) = 1$.

Proof. By replacing R with $R/\mathfrak{q}^h$, we can assume that $\mathfrak{q}^h = 0$, so that R is integral (since $\mathfrak{q}^h$ is prime), $\mathfrak{p}^h = 0$. It suffices to prove that $\operatorname{ht}(\mathfrak{p}) \leq 1$, because $\operatorname{ht}(\mathfrak{p}) = 0$ implies $\mathfrak{p} = \{0\}$ when R

is integral. Now since $\mathfrak{p}^h = \{0\}$, we have $\mathfrak{p} \cap R_n = \{0\}$ for each n, so $\mathfrak{p}$ is disjoint from the multiplicative subset $T = \bigcup_n (R_n \setminus \{0\})$. The ring $R_\mathfrak{p}$ is then isomomorphic to a subring of $T^{-1}R$, and we get

$$\mathrm{ht}(\mathfrak{p}) = \dim(R_\mathfrak{p}) \leq \dim(T^{-1}R).$$

However, by Lemma 13.1.56 the ring $T^{-1}R$ is isomomorphic to $K[X, X^{-1}]$, where K is a field. Therefore $\dim(T^{-1}R) \leq 1$ and $\mathrm{ht}(\mathfrak{p}) \leq 1$, which proves the claim. □

Proposition 16.6.6. *Let $\mathfrak{p}$ be a prime ideal of R. If $\mathfrak{p} \neq \mathfrak{p}^h$ then* $\mathrm{ht}(\mathfrak{p}^h) = \mathrm{ht}(\mathfrak{p}) - 1$.

Proof. By Proposition 11.1.42, $\mathfrak{p}^h$ is a prime ideal contained in $\mathfrak{p}$, so $\mathrm{ht}(\mathfrak{p}^h) \leq \mathrm{ht}(\mathfrak{p}) - 1$. The proposition is trivial if $\mathrm{ht}(\mathfrak{p}^h) = +\infty$, so we may assume that $\mathrm{ht}(\mathfrak{p}^h) < +\infty$. We now demonstrate the inequality $\mathrm{ht}(\mathfrak{p}) \leq \mathrm{ht}(\mathfrak{p}^h) + 1$ by proving that, for any prime ideal $\mathfrak{q}$ contained in $\mathfrak{p}$ and distinct from $\mathfrak{p}$, we have $\mathrm{ht}(\mathfrak{q}) \leq \mathrm{ht}(\mathfrak{p}^h)$.

We now proceed by induction on $\mathrm{ht}(\mathfrak{p})$. We distinguish two cases: if $\mathfrak{q}^h \neq \mathfrak{p}^h$, then we have $\mathrm{ht}(\mathfrak{q}^h) < \mathrm{ht}(\mathfrak{p}^h)$ since $\mathfrak{q}^h \subset \mathfrak{p}^h$; also, the equality

$$\mathrm{ht}(\mathfrak{q}) \leq \mathrm{ht}(\mathfrak{q}^h) + 1$$

holds by the induction hypothesis if $\mathfrak{q} \neq \mathfrak{q}^h$ and is trivial if $\mathfrak{q} = \mathfrak{q}^h$. Concequently, we get $\mathrm{ht}(\mathfrak{q}) \leq \mathrm{ht}(\mathfrak{q}^h) + 1 \leq \mathrm{ht}(\mathfrak{p}^h)$, which proves our claim. On the other hand, if $\mathfrak{q}^h = \mathfrak{p}^h$, then $\mathfrak{q} = \mathfrak{q}^h$ by Lemma 16.6.5, so $\mathrm{ht}(\mathfrak{q}) = \mathrm{ht}(\mathfrak{q}^h) = \mathrm{ht}(\mathfrak{p}^h)$. □

Theorem 16.6.7. *Suppose that the ring R is Noetherian.*

(a) Any chain of homogeneous prime ideals of R, saturated as a chain of homogeneous prime ideals, is saturated as a chain of prime ideals.

(b) For any homogeneous prime ideal $\mathfrak{p}$ of R, we have $\mathrm{htgr}(\mathfrak{p}) = \mathrm{ht}(S^{-1}\mathfrak{p}) = \mathrm{ht}(\mathfrak{p})$.

(c) We have $\mathrm{dimgr}(R) = \dim(S^{-1}R) = \dim(R)$.

Proof. To show (a), it suffices to prove that, if $\mathfrak{p}$ and $\mathfrak{q}$ are distinct homogeneous prime idelas of R such that $\mathfrak{q} \subset \mathfrak{p}$ and there exists no homogeneous prime ideals between $\mathfrak{q}$ and $\mathfrak{p}$, then $\mathrm{ht}(\mathfrak{p}/\mathfrak{q}) = 1$. By quotienting by $\mathfrak{q}$, we may assume that $\mathfrak{q} = \{0\}$ (the quotient ring is still Noetherian). In other words, it suffices to show that, if R is integral and Noetherian, and if $\mathfrak{p}$ is an homogeneous prime ideal of R minimal among nonzero homogeneous prime ideals, then $\mathrm{ht}(\mathfrak{p}) = 1$. Now let a be a nonzero homogeneous element of $\mathfrak{p}$ and $\mathfrak{r}$ a prime ideal of R such that $a \in \mathfrak{r} \subset \mathfrak{p}$ and is minimal with this property. Then $\mathfrak{r}^h$ is a nonzero prime ideal ($a \in \mathfrak{r}^h$) contained in $\mathfrak{r}$, so $\mathfrak{r}^h = \mathfrak{r}$, which means $\mathfrak{r}$ is homogeneous. By the hypothesis on $\mathfrak{p}$, this means $\mathfrak{p} = \mathfrak{r}$. Since R is Noetherian and integral, $\mathfrak{p}$ has height 1 (Proposition 16.3.1), which proves (a).

Let $\mathfrak{p}$ be a homogeneous prime ideal of R. We already have

$$\mathrm{htgr}(\mathfrak{p}) \leq \mathrm{ht}(S^{-1}\mathfrak{p}) \leq \mathrm{ht}(\mathfrak{p}).$$

We now prove the converse inequality by induction on $\mathrm{htgr}(\mathfrak{p})$. If $\mathrm{htgr}(\mathfrak{p}) = 0$, $\mathfrak{p}$ is minimal among the homogeneous prime ideals, so it is a minimal prime ideal of R (Corollary 11.1.43) and $\mathrm{ht}(\mathfrak{p}) = 0$. Suppose now $\mathrm{ht}(\mathfrak{p}) > 0$, we show the inequality $\mathrm{ht}(\mathfrak{q}) \leq \mathrm{htgr}(\mathfrak{p}) - 1$ for any prime

ideal $\mathfrak{q}$ contained in $\mathfrak{p}$ and distinct from $\mathfrak{p}$. We distinguish two cases: If $\mathfrak{q}$ is homogeneous, this is true from the induction hypothesis:

$$\mathrm{ht}(\mathfrak{q}) \leq \mathrm{htgr}(\mathfrak{q}) \leq \mathrm{htgr}(\mathfrak{p}) - 1.$$

If $\mathfrak{q}$ is not homogeneous, we have $\mathfrak{q}^h \subset \mathfrak{q} \subset \mathfrak{p}$, so $\mathrm{ht}(\mathfrak{q}^h) \leq \mathrm{htgr}(\mathfrak{q}^h)$ by the induction hypothesis. Recall that $\mathrm{ht}(\mathfrak{q}) = \mathrm{ht}(\mathfrak{q}^h)+1$ by Proposition 16.6.6, so $\mathrm{ht}(\mathfrak{q}) \leq \mathrm{htgr}(\mathfrak{q}^h)+1$. The proof will now be completed if we can prove the inequality $\mathrm{htgr}(\mathfrak{q}^h) \leq \mathrm{htgr}(\mathfrak{p}) - 2$. Assume on the contrary that we have $\mathrm{htgr}(\mathfrak{q}^h) = \mathrm{htgr}(\mathfrak{p}) - 1$; then the chain $\mathfrak{q}^h \subset \mathfrak{p}$ is saturated by part (a), which contradicts the fact $\mathfrak{q}^h \subset \mathfrak{q} \subset \mathfrak{p}$.

Finally, we show that inequality $\dim(R) \leq \mathrm{dimgr}(R)$, or equivalently $\mathrm{ht}(\mathfrak{p}) \leq \mathrm{dimgr}(R)$ for any prime ideal $\mathfrak{p}$ of R. If $\mathfrak{p}$ is homogeneous, we have $\mathrm{ht}(\mathfrak{p}) = \mathrm{htgr}(\mathfrak{p}) \leq \mathrm{dimgr}(R)$ by (b). If $\mathfrak{p}$ is not homogeneous, we have $\mathrm{ht}(\mathfrak{p}) = \mathrm{htgr}(\mathfrak{p}^h) + 1$ by Proposition 16.6.6; let $\mathfrak{m}$ be a homogeneous maximal ideal of R containing $\mathfrak{p}^h$ (note that the homogeneous ideal is not maximal among homogeneous prime ideals by Lemma 16.6.4, since we have $\mathfrak{p}^h \subset \mathfrak{p}$). Then by Lemma 16.6.4, $\mathfrak{m}$ is maximal, so distinct from $\mathfrak{p}^h$, and we have

$$\mathrm{htgr}(\mathfrak{p}^h) + 1 \leq \mathrm{htgr}(\mathfrak{m}) \leq \mathrm{dimgr}(R).$$

This shows $\mathrm{ht}(\mathfrak{p}) \leq \mathrm{dimgr}(R)$, which finishes the proof. □

16.6.2 Dimension of graded modules

Again R denote a graded ring with positive degrees and $S = 1 + R_{\geq 1}$. We now let M be a graded R-module of type $\mathbb{Z}$. Then $S^{-1}M$ is an $S^{-1}R$-module, and if we write $M_{\geq n} = \bigoplus_{i \geq n} M_i$, the submodules $S^{-1}M_{\geq n}$ form an exhaustive and separated filtration of $S^{-1}M$ and the canonical map $M \mapsto S^{-1}M$ induces an isomorphism of M onto the graded module of $S^{-1}M$ associated to this filtration.

Lemma 16.6.8. *Suppose that R is generated by $R_0 \cup R_1$ and that M is generated by $\bigoplus_{i \leq n_0} M_i$ for an integer n_0. Then the filtration $(S^{-1}M_{\geq n})$ of $S^{-1}M$ is good for the ideal $S^{-1}R_{\geq 1}$ of $S^{-1}R$.*

Proof. For $n \geq n_0$, we have $M_{\geq n+1} = R_1 \cdot M_{\geq n}$, so

$$S^{-1}M_{\geq n+1} = R_1 \cdot S^{-1}M_{\geq n} = S^{-1}R_{\geq 1} \cdot S^{-1}M_{\geq n},$$

which shows the filtration $(S^{-1}M_{\geq n})$ is $(S^{-1}R_{\geq 1})$-good. □

Proposition 16.6.9. *Suppose that R is Noetherian and M is finitely generated. Then* $\dim_R(M) = \dim_{S^{-1}R}(S^{-1}M)$.

Proof. Let $\mathfrak{a}$ be the annihilator of the R-module M, which is a homogeneous ideal of R. Since M is finitely generated, the annihilator of $S^{-1}M$ is the ideal $S^{-1}\mathfrak{a}$. We have $\dim_R(M) = \dim(R/\mathfrak{a})$ and $\dim_{S^{-1}R}(S^{-1}M) = \dim(S^{-1}R/S^{-1}\mathfrak{a})$ by definition. Since $R/\mathfrak{a}$ is Noetherian, an application of Theorem 16.6.7 proves the claim. □

Proposition 16.6.10. *Suppose that R_0 is an Artinian local ring, R is generated by $R_0 \cup R_1$, and R_1 is a finitely generated R_0-module. If M is nonzero and finitely generated as an R-module, then M_n is an*

R_0-module with finite length for each n, and there exists $Q(T) \in \mathbb{Z}[T, T^{-1}]$ such that $Q(1) > 0$ and the following equality holds in the ring $\mathbb{Z}((T))$:

$$\sum_{n\in\mathbb{Z}} \ell_{R_0}(M_n) \cdot T^n = (1 - T^{-d})Q(T),$$

where $d = \dim_R(M)$.

Proof. The ring $S^{-1}R$ is local and Noetherian by Remark 16.6.1, the $S^{-1}R$-module $S^{-1}M$ is finitely generated and nonzero, and $d = \dim_R(M)$ is nonzero. Also, by Lemma 16.6.8 the filtration $(S^{-1}M_{\geq n})$ is $S^{-1}R_{\geq 1}$-good and $S^{-1}R_{\geq 1}$ is a defining ideal of $S^{-1}R$ (Proposition 16.3.14). Finally, we have $\ell_{S^{-1}R}(S^{-1}M_{\geq n}/S^{-1}M_{\geq n+1}) = \ell_{R_0}(M_n)$ for each n, so it suffices to apply Theorem 16.4.13. □

Corollary 16.6.11. *If R is a Noetherian local ring and $\mathfrak{a}$ is a defining ideal of R, then* $\dim(R) = \dim(\mathrm{gr}_{\mathfrak{a}}(R))$.

Proof. Apply Proposition 16.6.10 on the module $M = B = \mathrm{gr}_{\mathfrak{a}}(R)$, we get

$$\sum_{n=0}^{\infty} \ell_{R/\mathfrak{a}}(\mathfrak{a}^n/\mathfrak{a}^{n+1}) \cdot T^n = (1 - T)^{-d}Q(T)$$

where $d = \dim(\mathrm{gr}_{\mathfrak{a}}(R))$ and $Q(1) \neq 0$. We have $d = \dim(R)$ by Theorem 16.4.19, whence the corollary. □

Corollary 16.6.12. *Suppose that M is a finitely generated R-module. Let a be a homogeneous element of R with positive degree, and not belonging to any minimal element $\mathfrak{p}$ in* $\mathrm{supp}(M)$ *such that* $\dim(R/\mathfrak{p}) = \dim_R(M)$. *Then* $\dim_R(M/aM) = \dim_R(M) - 1$.

Proof. Put $d = \dim_R(M)$; by the hypothesis on a, we have $\dim_R(M/aM) < d$. Also, by Proposition 16.6.9, we have

$$\dim_R(M/aM) = \dim_{S^{-1}M}(S^{-1}M/(b/1) \cdot S^{-1}M)$$

and the formula (3.2.3) implies the following inequality:

$$\dim_{S^{-1}R}(S^{-1}M/(b/1) \cdot S^{-1}M) \geq \dim_{S^{-1}R}(S^{-1}M) - 1.$$

Finally, $\dim_{S^{-1}R}(S^{-1}M) = \dim_R(M) = d$ by Proposition 16.6.9. We then conclude that $\dim_R(M/bM) \geq d - 1$, which proves the claim. □

Proposition 16.6.13. *Suppose that R_0 is an Artinian local ring, R is an R_0-algebra of finite type and M is a finitely generated R-module.*

(a) Let $a_1, \ldots, a_n$ be homogeneous elements of R with positive degrees and φ the homomorphism from $R_0[X_1, \ldots, X_n]$ to R mapping X_i to a_i for each i. Then $S^{-1}M/\sum_{i=1}^{n}(a_i/1) \cdot S^{-1}M$ has finite length over $S^{-1}R$ if and only if $\varphi^*(M)$ is a finitely generated module over $R_0[X_1, \ldots, X_n]$.

(b) There exists a family $(a_1, \ldots, a_d)$ of elements of R, homogeneous with the same positive degree, where $d = \dim_R(M)$, such that $(a_1/1, \ldots, a_d/1)$ is a maximal secant sequence for the $S^{-1}R$-module $S^{-1}M$. If moreover R is generated by R_1 as an R_0-algebra and the residue field of R_0 is infinite, each a_i can be taken to have degree 1.

Proof. Put $N = M/\sum_{i=1}^n a_i M$, we have $\dim_R(N) = \dim_{S^{-1}R}(S^{-1}N)$ by Proposition 16.6.9. Also, the $S^{-1}R$-module $S^{-1}N$ is of finite length if and only if the R-module N has finite length, that is, N is a finitely generated R_0-module. If $\varphi^*(M)$ is the pullback module over $R_0[X_1, \dots, X_n]$, we have $\varphi^*(N) = \varphi^*(M)/\sum_{i=1}^n X_i \cdot \varphi^*(M)$. Therefore $\varphi^*(M)$ is a finitely generated $R_0[X_1, \dots, X_n]$-module if and only if N is a finitely generated R_0-module, which proves (a).

Let's assume the hypothesis in Proposition 16.6.13(b). We may assume that $\dim_R(M) > 0$. Note that any minimal element of $\operatorname{supp}(M)$ is homogeneous (Corollary 11.1.43). According to Proposition 11.1.49, there exists a homogeneous element a of R with positive degree, not belonging to any minimal element $\mathfrak{p}$ in $\operatorname{supp}(M)$ such that $\dim(R/\mathfrak{p}) = \dim_R(M)$. By Corollary 16.6.12, we have $\dim_R(M/aM) = \dim_R(M) - 1$. Suppose further that R is generated by R_1 as an R_0-algebra and the residue field k of R_0 is infinite. For any minimal element $\mathfrak{p}$ in $\operatorname{supp}(M)$ such that $\dim(R/\mathfrak{p}) = \dim_R(M)$, consider the subspace $V_\mathfrak{p} = (\mathfrak{p} \cap R_1) \otimes_{R_0} k$ of the k-vector space $V = R_1 \otimes_{R_0} k$. These subspaces are proper: if $V_\mathfrak{p} = V$, then $\mathfrak{p} \cap H_1 = H_1$ by Corollary 7.1.4, so $H_1 \subseteq \mathfrak{p}$ and $\dim_R(M) = \dim(R/\mathfrak{p}) \leq \dim(R/R_1) = 0$, which contradicts to our assumption. Since k is infinite, the union of $V_\mathfrak{p}$'s is distinct from V. If $a \in R_1$ is such that $a \otimes 1$ is not contained in any of the $V_\mathfrak{p}$, then a is not contained in the minimal element $\mathfrak{p}$ such that $\dim(R/\mathfrak{p}) = \dim_R(M)$, whence $\dim_R(M/aM) = \dim_R(M) - 1$.

By induction on the dimension $d = \dim_R(M)$, we can construct a sequence $(b_1, \dots, b_d)$ of elements in R, with $n_i = \deg(b_i) > 0$, wuch that $M/\sum_{i=1}^d b_i M$ is a R-module of finite length. Moreover, if R is generated by R_1 as an R_0-algebra and the residue field of R_0 is infinite, each b_i can be taken to have degree 1. Now by Proposition 16.6.9, $\dim_{S^{-1}R}(S^{-1}M) = d$ and

$$\dim_{S^{-1}R}(S^{-1}M/\sum_{i=1}^d (b_i/1) \cdot S^{-1}M) = 0.$$

Therefore $(b_1/1, \dots, b_d/1)$ is a maximal secant sequence for $S^{-1}M$. Put $a_i = b_i^{(n_1 \cdots n_d)/n_i}$, we see the a_i's have the same degree, and $(a_1/1, \dots, a_d/1)$ is a maximal secant sequence for $S^{-1}M$ by Proposition 16.3.10. □

Corollary 16.6.14. *Suppose that R_0 is a field and R is an R_0-algebra of finite type. Put $n = \dim(R)$. Then there exists homogeneous elements $a_1, \dots, a_n$ of R with the same positive degree such that the R_0-homomorphism $\varphi : R_0[X_1, \dots, X_n] \to R$, defined by $\varphi(X_i) = a_i$ for each i, is injective and makes R a finitely generated $R_0[X_1, \dots, x_n]$-module. If R is generated by R_1 as an R_0-algebra and R_0 is infinite, each a_i can be taken to have degree* 1.

Proof. There exists by Proposition 16.6.13 an R_0-homomorphism φ of the indicated form making R a finitely generated $R_0[X_1, \dots, X_n]$-module. By Theorem 16.2.8, we also have

$$\dim(R) = n = \dim(R_0[X_1, \dots, X_n]).$$

Since the ring $R_0[X_1, \dots, X_n]$ is integral and $R \cong R_0[X_1, \dots, X_n]/\ker\varphi$, we conclude that $\ker\varphi = 0$. □

Remark 16.6.3. Assume the hypothesis in Corollary 16.6.14. Let $(h_1, \dots, h_r)$ be a basis for the R_0-vector space R_1. For $\lambda = (\lambda_1, \dots, \lambda_r) \in R_0^r$, put $h_\lambda = \lambda_1 h_1 + \cdots + \lambda_r h_r$. Then Proposition 16.6.13 and Corollary 16.6.14 imply the following result: the set of elements $(\lambda^{(1)}, \dots, \lambda^{(n)})$

of $(R_0^r)^n$ such that the elements $a_i = h_{\lambda_i} \in R_1$ satisfies the conclusion of Corollary 16.6.14 contains the complement of the union of a finite number of vector subspaces of $(R_0^r)^n$ distinct from the entire space.

Corollary 16.6.15. *Let A be a Noetherian local ring and d a non-negative integer. For $\dim(A) \geq n$, it is necessary and sufficient that for any integer $r \geq 0$ we have*

$$[\mathfrak{m}_A^r/\mathfrak{m}_A^{r+1} : \kappa_A] \geq \binom{n+r-1}{n-1}.$$

Moreover, the equality holds if and only if A is regular of dimension n.

Proof. By Theorem 16.4.19 and Theorem 16.5.5, this condition is sufficient. We now demonstrate the necessity, so assume that $\dim(A) \geq n$. Consider the graded ring $\mathrm{gr}(A) = \mathrm{gr}_{\mathfrak{m}_A}(A)$; let k be a extension of the residue field κ_A such that k is infinite, and put $R = k \otimes_{\kappa_A} \mathrm{gr}(A)$. The ring R has dimension $\geq n$ by Corollary 16.6.11. We deduce by Corollary 16.6.14 the existence of an injective k-algebra homomorphism $\varphi : R_0[X_1, \ldots, X_n] \to R$. Therefore for any integer $r \geq 0$,

$$[\mathfrak{m}_A^r/\mathfrak{m}_A^{r+1} : \kappa_A] = [R_r : R_0] \geq \binom{n+r-1}{n-1},$$

and the equality holds if and only if φ is bijective, whence A is regular (Theorem 16.5.5). □

Remark 16.6.4. Note that we have the equality

$$\binom{n+r}{n} = \sum_{i=0}^{r} \binom{n+i-1}{n-1}, \quad \ell_A(A/\mathfrak{m}_A^{r+1}) = \sum_{i=0}^{r} [\mathrm{gr}_i(A) : \kappa_A].$$

Therefore the condition in Corollary 16.6.15 is equivalent to $\ell_A(A/\mathfrak{m}_A^{r+1}) \geq \binom{n+r}{n}$.

16.6.3 Dimension and graded algebras

Lemma 16.6.16. *Let A be a ring, $\mathfrak{r}$ its Jacobson radical, $R = \bigoplus_{i\in\mathbb{Z}} R_i$ a graded A-algebra, and $M = \bigoplus_{i\in\mathbb{Z}} M_i$ a graded R-module. Suppose that each M_i is a finitely generated A-module and $M/\mathfrak{r}M$ is a finitely generated $R/\mathfrak{r}R$ module. Then M is a finitely generated R-module.*

Proof. Let $m_1, \ldots, m_n$ be homogeneous elements of M whose images generate $M/\mathfrak{r}M$. Let N be the graded submodule of M generated by $m_1, \ldots, m_n$. We have $M_i = N_i + \mathfrak{r}M_i$ for each i, whence $M_i = N_i$ (Corollary 7.1.4); this shows $M = N$. □

Lemma 16.6.17. *Let $\rho : A \to B$ be a ring homomorphism and S be a multiplicative subset of A. Suppose that B is an A-algebra of finite type and $S^{-1}B$ is a finitely generated $S^{-1}A$-module. Then there exists $f \in S$ such that B_f is a finitely generated A_f-module.*

Proof. Let X be a generating set of the A-algebra B. For each $x \in X$, the image of x in $S^{-1}B$ is integral over $S^{-1}A$, so there exist an integer $n(x) \geq 0$, elements $b_1(x), \ldots, b_{n(x)}(x)$ of A, and an element $f(x) \in S$, such that

$$f(x)x^{n(x)} + b_1(x)x^{n(x)-1} + \cdots + b_{n(x)} = 0.$$

Let $f = \prod_{x \in X} f(x)$; the image of $x \in X$ in B_f is then integral over A_f, so B_f is a finitely generated A_f-module. □

Proposition 16.6.18. *Suppose that R is an R_0-algebra of finite type. Then the function $\mathfrak{p} \mapsto \dim(R \otimes_{R_0} \kappa(\mathfrak{p}))$ is upper semi-continuous on $\operatorname{Spec}(A_0)$.*

Proof. Since R is an R_0-algebra of finite type, each R_i is finitely generated as an R_0-module (Corollary 11.1.34). Let $\mathfrak{p} \in \operatorname{Spec}(R_0)$ and suppose $\dim(R \otimes_{R_0} \kappa(\mathfrak{p})) = n \geq 0$. By Corollary 16.6.14, there exists $a_1, \ldots, a_n$ in R, homogeneous of degree $d > 0$, such that the $\kappa(\mathfrak{p})$-homomorphism $\bar{\varphi} : \kappa(\mathfrak{p})[X_1, \ldots, X_n] \to R \otimes_{R_0} \kappa(\mathfrak{p})$ mapping X_i to $a_i \otimes 1$ for each i, makes $R \otimes_{R_0} \kappa(\mathfrak{p})$ a finitely generated $\kappa(\mathfrak{p})[X_1, \ldots, X_n]$-module. Let φ be the R_0-homomorphism from $R_0[X_1, \ldots, X_n] = H$ to R mapping X_i to a_i for each i.

For $m \in \mathbb{Z}$, define

$$\tilde{R}_m = \bigoplus_{(m-1)d < i \leq md} R_i.$$

Then $(\tilde{R}_m)$ is a graduation of type $\mathbb{Z}$ on R which is compatible with the $R_0[X_1, \ldots, X_n]$-module structure induced by φ; moreover, each $\tilde{R}_m$ is finitely generated over R_0. Now note that the Jacobson radical of $(R_0)_\mathfrak{p}$ is $\mathfrak{p}(R_0)_\mathfrak{p}$ and

$$R_\mathfrak{p}/\mathfrak{p}(R_0)_\mathfrak{p}R_\mathfrak{p} = R \otimes_{R_0} \kappa(\mathfrak{p}), \quad H_\mathfrak{p}/\mathfrak{p}(R_0)_\mathfrak{p}H_\mathfrak{p} = \kappa(\mathfrak{p})[X_1, \ldots, X_n].$$

By using Lemma 16.6.16, we conclude that $R_\mathfrak{p}$ is a finitely generated $H_\mathfrak{p}$-module. Now apply Lemma 16.6.17, there then exists $f \in R_0 \setminus \mathfrak{p}$ such that R_f is finitely generated H_f-module. For any $\mathfrak{q} \in \operatorname{Spec}((R_0)_f)$, $R \otimes_{R_0} \kappa(\mathfrak{q})$ is then a finitely generated $\kappa(\mathfrak{q})[X_1, \ldots, X_n]$-module, whence $\dim(R \otimes_{R_0} \kappa(\mathfrak{q})) \leq n$ by Theorem 16.2.8. This completes the proof. □

From now on, we assume that R_0 is a field and R is an R_0-algebra of finite type. In this case, we set $R_+ = R_{\geq 1}$, which is a maximal ideal of R. The ring $S^{-1}R$ can be then identified with the local ring R_{R_+}, whose maximal ideal is $(R_+)_{R_+} = S^{-1}R_+$ with residue field A_0.

Proposition 16.6.19. *Suppose that R_0 a field and R is a finite type R_0-algebra.*

(a) We have $\dim(R) \leq [R_+/R_+^2 : R_0]$.

(b) The following conditions are equivalent:

- *(i)* $\dim(R) = [R_+/R_+^2 : R_0]$.
- *(ii) The Noetherian local ring $S^{-1}R$ is regular.*
- *(iii) R is generated as an R_0-algebra by a family of homogeneous elements with positive degrees, algebraically independent over R_0.*

(c) Suppose that the conditions in (b) holds, and let $a_1, \ldots, a_n \in R$ be homogeneous elements with positive degrees. Then the following conditions are equivalent:

- *(i′) The images of a_i's form a basis for the R_0-vector space R_+/R_+^2.*
- *(ii′) The images of a_i's form a system of parameters in the Noetherian local ring $S^{-1}R$.*
- *(iii′) The a_i's are algebraically independent over R_0 and generate R as an R_0-algbera.*

Proof. Since R is Noetherian, we have $\dim(R) = \dim(S^{-1}R)$ by Theorem 16.6.7; also,

$$[R_+/R_+^2 : R_0] = [(S^{-1}R_+)/(S^{-1}R_+)^2 : R_0]$$

by Corollary 10.2.31. These together prove (a) and the equivalences (i)⇔(ii), (i′)⇔(ii′). The implications (iii)⇒(i) and (iii′)⇒(i′) are trivial. To establish (i)⇒(iii), suppose that $\dim(R) = [R_+/R_+^2 : R_0]$ and let $a_1, \dots, a_n$ be homogeneous elements of R with positive degrees whose classes in R_+/R_+^2 form a basis. Consider the homomorphism $\varphi : R_0[X_1, \dots, X_n]$ to R mapping X_i to a_i. The ideal R_+ of R is generated by a_i, so the homomorphism φ is surjective. Thus we have

$$\dim(R_0[X_1, \dots, X_n]) = n = \dim(R) = \dim(R_0[X_1, \dots, X_n]/\ker\varphi)$$

which implies $\ker\varphi = 0$ (recall that $R_0[X_1, \dots, X_n]$ is an integra ldomain). This implies (iii), and the implication (i′)⇒(iii′) can be done similarly. □

If R satisfies the hypothesis in (b), we say R is an regular graded R_0-algebra, or an polynomial graded R_0-algebra. In this case, any family $(a_1, \dots, a_n)$ satisfying the hypothesis in (c) will be called a system of parameters of R.

Remark 16.6.5. In the notations of (c), let d_i be the degree of a_i for each i. Then the Poincaré series of H is given by

$$P_R = \sum_{n\in\mathbb{Z}} [R_n : R_0] \cdot T^n = \prod_{i=1}^{n} (1 - T^{d_i})^{-1}.$$

Conversely, if there exist integers $d_i > 0$ such that $P_R = \prod_i (1 - T^{d_i})^{-1}$, we may conclude that R is a polynomial graded algebra. For example, if R is generated by X with degree 1 and Y with degree 2 with the sole relation $X^2 = 0$, we have $P_R = (1 - T)^{-1}$, so R is regular.

16.7 Multiplicity

16.7.1 Multiplicity of a module relative to an ideal

Let A be a Noetherian ring and M be a finitely generated A-module. Let $\mathfrak{a}$ be an ideal of A contained in the Jacobson radical of A and such that $M/\mathfrak{a}M$ is of finite length. Suppose that M is nonzero and put $d = \dim_A(M)$. Recall that (Corollary 16.4.14) there exists a unique integer $e_\mathfrak{a}(M) > 0$ such that, for $n \geq 1$,

$$\ell_A(M/\mathfrak{a}^{n+1}M) = e_\mathfrak{a}(M)\frac{n^d}{d!} + \beta_n n^{d-1} \tag{7.1.1}$$

where β_n has a limit when n goes to infinity. The integer $e_\mathfrak{a}(M)$ (or $e_\mathfrak{a}^A(M)$ if we want to emphasize the ring A) is called the **multiplicity** of M relative to $\mathfrak{a}$. If A is a local ring and $\mathfrak{m}$ is the maximal ideal of A, we write $e(M)$ or $e^A(M)$ for $e_\mathfrak{m}^A(M)$. Recall that equivalently, we have

$$\ell_A(\mathfrak{a}^n M/\mathfrak{a}^{n+1}M) = e_\mathfrak{q}(M)\frac{n^{d-1}}{(d-1)!} + \alpha_n n^{d-1}$$

where α_n has a limit when n goes to infinity.

Remark 16.7.1. Let $\mathfrak{b}$ be an ideal of A contained in the Jacobson radical of A and contains $\mathfrak{a}$. Then $M/\mathfrak{b}^n M$ is a quotient of $M/\mathfrak{a}^n M$, whence $e_{\mathfrak{b}}(M) \leq e_{\mathfrak{a}}(M)$ by the formula (7.1.1). Moreover, if the $\mathfrak{b}$-adic filtration on M is $\mathfrak{a}$-good, then $e_{\mathfrak{a}}(M) = e_{\mathfrak{b}}(M)$ by Theorem 16.4.13.

Recall that we can reduce the calculus of the multiplicities to the case where A is local since, according to Corollary 16.4.20, we have

$$e_{\mathfrak{a}}(M) = \sum_{\mathfrak{m}} e_{\mathfrak{a}_{\mathfrak{m}}}(M_{\mathfrak{m}})$$

where $\mathfrak{m}$ runs through the elements of $\operatorname{supp}(M) \cap V(\mathfrak{a})$ such that $\dim_{A_{\mathfrak{m}}}(M_{\mathfrak{m}}) = d_{\mathfrak{a}}(M)$.

Proposition 16.7.1. *Let $\widehat{A}$ (resp. $\widehat{M}$) be the $\mathfrak{a}$-adic completion of A (resp. M), then $e_{\mathfrak{a}}^{A}(M) = e_{\hat{\mathfrak{a}}}^{\widehat{A}}(\widehat{M})$.*

Proof. This follows from the fact that $\operatorname{gr}_{\mathfrak{a}}(M) \cong \operatorname{gr}_{\hat{\mathfrak{a}}}(\widehat{M})$. □

Proposition 16.7.2. *If A is regular, then $e(A) = 1$.*

Proof. If A is regular then $H_{A,\mathfrak{m}_A} = (1-T)^{-r}$ (Theorem 16.5.5), whence $e(A) = 1$. □

Example 16.7.3. By definition $e_{\mathfrak{a}^r}(M) = r^d e_{\mathfrak{a}}(M)$ where $d = \dim_A(M)$. Concequently, if A is a regular local ring, we have $e_{\mathfrak{m}_A^r}(A) = r^d$. For example, if A is a discrete valuation ring, then $e_{\mathfrak{m}_A^r}(A) = r$, whence $e_{\mathfrak{a}}(A) = \ell(A/\mathfrak{a})$ for any ideal $\mathfrak{a}$.

For an ideal $\mathfrak{a}$ of A contained in the Jacobson radical of A, we let $C(\mathfrak{a})$ denote the set of classes of finitely generated A-modules M such that $M/\mathfrak{a}M$ is of finite length. For each $d \in \mathbb{N}$, let $C(\mathfrak{a})_{\leq d}$ be the subset of $C(\mathfrak{a})$ consists of classes of A-modules of dimension $\leq d$. We have a map $e_{\mathfrak{a},d} : C(\mathfrak{a})_{\leq d} \to \mathbb{Z}$ such that $e_{\mathfrak{a},d}(M) = e_{\mathfrak{a}}(M)$ if $\dim_A(M) = d$ and $e_{\mathfrak{a},d}(M) = 0$ otherwise. This map is additive by Proposition 16.4.18, so we get an induced homomorphism, still denoted by $e_{\mathfrak{a},d}$, from the Grothendieck group $K(C(\mathfrak{a})_{\leq d})$ to $\mathbb{Z}$, which is zero on $K(C(\mathfrak{a})_{\leq d-1})$.

Proposition 16.7.4. *Let M be a finitely generated A-module with dimension $d \geq 0$. Let $\mathfrak{a}$ be an ideal of A contained in the Jacobson radical of A such that $M/\mathfrak{a}M$ has finite length. Then*

$$e_{\mathfrak{a}}(M) = \sum_{\operatorname{coht}(\mathfrak{p})=d} \ell_{A_{\mathfrak{p}}}(M_{\mathfrak{p}}) \cdot e_{\mathfrak{a}}(A/\mathfrak{p})$$

Proof. By Theorem 12.1.18, M has a composition series $(M_i)_{0\leq i\leq n}$ such that M_i/M_{i+1} is isomomorphic to $A/\mathfrak{p}_i$, where $\mathfrak{p}_i$ is a prime ideal of M. Also, by Remark 12.2.2, the number $\ell_{A_{\mathfrak{p}}}(M_{\mathfrak{p}})$ is the times of i such that $M_i/M_{i+1} \cong A/\mathfrak{p}$. The proposition then follows from Proposition 16.4.18. □

Corollary 16.7.5. *Suppose that A is Noetherian semi-local and let $\mathfrak{a}$ be a defining ideal for A.*

(a) We have $e_{\mathfrak{a}}(A) = \sum_{\mathfrak{p}} \ell_{A_{\mathfrak{p}}}(A_{\mathfrak{p}}) \cdot e_{\mathfrak{a}}(A/\mathfrak{p})$, where $\mathfrak{p}$ turns through minimal primes of A such that $\operatorname{coht}(\mathfrak{p}) = \dim(A)$.

(b) Suppose that A is integral and M is a finitely generated A-module such that $\dim_A(M) = \dim(A)$. Then $e_{\mathfrak{a}}(M) = \operatorname{rank}(M) \cdot e_{\mathfrak{a}}(A)$.

Proof. Part (a) follows directly from Proposition 16.7.4 by applying on $M = A$. Under the hypothesis of (b), the minimal prime ideal of A is (0), and $\ell_{A_{(0)}}(M_{(0)}) = \operatorname{rank}(M)$, so the claim follows. □

16.7.2 Multiplicity and base change

Proposition 16.7.6. *Let $\rho : A \to B$ be a local homomorphism of Noetherian local rings. Let N be a finitely generated B-module, flat over A, and such that $N \otimes_A \kappa_A$ is a B-module of finite length. If M is a nonzero finitely generated A-module and $\mathfrak{a}$ is a proper ideal of A such that $M/\mathfrak{a}M$ is of finite length, then $(M \otimes_A N)/\mathfrak{a}^e(M \otimes_A N)$ is a B-module of finite length, and we have*

$$e^B_{\mathfrak{a}^e}(M \otimes_A N) = \ell_B(N \otimes_A \kappa_A) \cdot e^A_{\mathfrak{a}}(M).$$

Proof. Let L be an A-module of finite length r. Then by Theorem 12.1.18 and Proposition 12.2.14, L has a composition series of length r, with quotients κ_A. Since N is flat over A, the B-module $L \otimes_A N$ possesses a composition series of length r, with quotients $N \otimes_A \kappa_A$. Therefore the length of $L \otimes_A N$ is $r \cdot \ell_B(N \otimes_A \kappa_A)$. The B-module $(M \otimes_A N)/(\mathfrak{a}^e)^n(M \otimes_A N)$ is isomomorphic to $(M/\mathfrak{a}^n M) \otimes_A N$ for each $n \in \mathbb{N}$, the proposition then follows from the definition of multiplicity. □

Corollary 16.7.7. *Suppose that $\rho : A \to B$ be a local homomorphism of Noetherian local rings, B is flat over A and $\mathfrak{m}_A^e = \mathfrak{m}_B$. Then*

$$e^B_{\mathfrak{a}^e}(M \otimes_A B) = e^A_{\mathfrak{a}}(M).$$

Proof. In this case we have $B \otimes_A \kappa_A = B/\mathfrak{m}_A^e$, which has length 1 over B, so the claim follows from Proposition 16.7.6. □

Example 16.7.8. Let X be a complex algebraic variety, $\mathcal{O}_{X,x}$ the local ring of X at a rational point x, and X^{an} the analytic space associated with X. Let $\mathcal{O}_{X^{an},x}$ be the local ring of X^{an} at x. Then $e(\mathcal{O}_{X^{an},x}) = e(\mathcal{O}_{X,x})$.

Proposition 16.7.9. *Suppose that A is Noetherian semi-local and let $\rho : A \to B$ be a ring homomorphism making B a finitely generated A-module. Let N be a nonzero finitely generated B-module and $\mathfrak{a}$ an ideal of A contained in the Jacobson radical of A such that $N/\mathfrak{a}N$ has finite length. Let $\mathfrak{m}_1, \dots, \mathfrak{m}_r$ be the maximal ideals of B such that $\dim_{B_{\mathfrak{m}_i}}(N_{\mathfrak{m}_i}) = \dim_B(N)$ (by Corollary 12.2.22 B is semi-local). Put $B_i = B_{\mathfrak{m}_i}$ and $\mathfrak{a}_i = \mathfrak{a}B_i$ for each i. Then we have the equalities*

$$\dim_A(N) = \dim_B(N), \quad e^B_{\mathfrak{a}^e}(N) = \sum_{i=1}^r e^{B_i}_{\mathfrak{a}_i}(N_{\mathfrak{m}_i}), \quad e^A_{\mathfrak{a}}(N) = \sum_{i=1}^r [B/\mathfrak{m}_i : A/\mathfrak{m}_i^c] \cdot e^{B_i}_{\mathfrak{a}_i}(N_{\mathfrak{m}_i}).$$

Proof. Since B is integral over A, we have $\dim_A(N) = \dim_B(N)$. The second equality follows from Corollary 16.4.20 (note that $\mathfrak{m}_i$ is in $V(\mathfrak{a}^e)$ for each i since $\mathfrak{m}_i^c \supset \mathfrak{a}$ by Corollary 13.1.63). Now let E be a B-module of finite length; we have

$$\ell_A(E) = \sum_{\mathfrak{m}} [B/\mathfrak{m} : A/\mathfrak{m}^c] \cdot \ell_{B_{\mathfrak{m}}}(E_{\mathfrak{m}}),$$

where $\mathfrak{m}$ runs through maximal ideals of B: this is evident when E is one of the $B/\mathfrak{m}$, and the general case follows since E has a composition sequence with quotients isomomorphic to $B/\mathfrak{m}$, with $\mathfrak{m}$ a maximal ideal of B. Apply this formula to the B-module $N/\mathfrak{a}^{n+1}N$, we deduce the equality from the definition of multiplicity. □

Corollary 16.7.10. *If $[B/\mathfrak{m}_i : A/\mathfrak{m}_i^c] = 1$ for each i, then $e^A_{\mathfrak{a}}(N) = e^B_{\mathfrak{a}^e}(N)$.*

Lemma 16.7.11. *Let $\rho : A \to B$ be a ring homomorphism and $\mathfrak{p}$ a prime ideal of A. Consider the following conditions:*

(i) The canonical homomorphism $\tilde{\rho} : A_{\mathfrak{p}} \to A_{\mathfrak{p}} \otimes_A B$ is bijective.

(ii) There is only one prime ideal $\mathfrak{P}$ of B lying over $\mathfrak{p}$ and the canonical homomorphism $\rho_{\mathfrak{p}} : A_{\mathfrak{p}} \to B_{\mathfrak{P}}$ is bijective.

We have (i)⇒(ii). If $\mathfrak{p}$ is minimal, or if B is integral over A, then (i)⇔(ii).

Proof. The ring $A_{\mathfrak{p}} \otimes_A B$ can be identified with the localization $S^{-1}B$ by the multiplicative subset $S = \rho(A - \mathfrak{p})$. The prime ideals of $S^{-1}B$ are of the form $S^{-1}\mathfrak{P}$, wherer $\mathfrak{P}$ is a prime ideal of B such that $\mathfrak{P}^c \subseteq \mathfrak{p}$. If $\mathfrak{P}$ is such an ideal, $(S^{-1}B)_{S^{-1}\mathfrak{P}}$ is identified with $B_{\mathfrak{P}}$.

If condition (i) is satisfied, there exists (Lemma 13.1.61) a unique prime ideal $\mathfrak{P}$ of B such that $\mathfrak{P}^c = \mathfrak{p}$. Moreover, $B_{\mathfrak{P}}$ is identified with the ring $(S^{-1}B)_{S^{-1}\mathfrak{P}}$, hence with $(A_{\mathfrak{p}})_{\mathfrak{q}}$, where $\mathfrak{q}$ is the inverse image of $S^{-1}\mathfrak{P}$ under the isomorphism $\tilde{\rho} : A_{\mathfrak{p}} \to S^{-1}B$; then $\tilde{\rho}^{-1}(S^{-1}\mathfrak{P}) = (A - \mathfrak{p})^{-1}\mathfrak{p} = \mathfrak{p}A_{\mathfrak{p}}$, hence (ii).

Conversely, asssume (ii) and let $\mathfrak{P}$ be the unique prime ideal of B lying over $\mathfrak{p}$. Since $(S^{-1}B)_{S^{-1}\mathfrak{P}}$ is identified with $B_{\mathfrak{P}}$, it suffices to prove that $S^{-1}B$ is a local ring with maximal ideal $S^{-1}\mathfrak{P}$, which means any prime ideal $\mathfrak{Q}$ of B such that $\mathfrak{Q}^c \subseteq \mathfrak{p}$ is contained in $\mathfrak{P}$. If $\mathfrak{p}$ is minimal, we have $\mathfrak{Q}^c = \mathfrak{p}$, whence $\mathfrak{Q} = \mathfrak{P}$. If B is integral over A, then by the going up theorem, there exists a prime ideal $\mathfrak{P}'$ of B such that $\mathfrak{Q} \subseteq \mathfrak{P}'$ and $(\mathfrak{P}')^c = \mathfrak{p}$. Then $\mathfrak{P}' = \mathfrak{P}$, whence $\mathfrak{Q} \subseteq \mathfrak{P}$. □

Lemma 16.7.12. *Suppose that A is Noetherian and semi-local. Let $\mathfrak{a}$ be a defining ideal of A, and $\rho : A \to B$ a ring homomorphism making B a finitely generated A-module. Suppose that, for any prime ideal $\mathfrak{p}$ (necessarily minimal) of A such that $\dim(A/\mathfrak{p}) = \dim(A)$, there exists a unique prime ideal $\mathfrak{P}$ of B lying over $\mathfrak{p}$ such that the canonical homomorphism $\rho_{\mathfrak{p}} : A_{\mathfrak{p}} \to B_{\mathfrak{P}}$ is bijective. Then $\dim_A(B) = \dim(A)$ and $e_{\mathfrak{a}}^A(B) = e_{\mathfrak{a}}^A(A)$.*

Proof. Let $\mathscr{P}_A$ (resp. $\mathscr{P}_B$) be the set of prime ideals of A such that $\dim(A/\mathfrak{p}) = \dim(A)$ (resp. $\dim_A(B/\mathfrak{p}^e) = \dim_A(B)$); we have $\mathscr{P}_A \neq \varnothing$. Let $\mathfrak{p} \in \mathscr{P}_A$; there exists by hypothesis a unique ideal of B lying over $\mathfrak{p}$. By Proposition 10.2.40 we have $\mathfrak{p}^{ec} = \mathfrak{p}$, and Theorem 16.2.8 then shows that $\dim(A/\mathfrak{p}) = \dim(B/\mathfrak{p}^e) = \dim_A(B/\mathfrak{p}^e)$, whence

$$\dim_A(B) \geq \dim_A(B/\mathfrak{p}^e) = \dim(A/\mathfrak{p}) = \dim(A) \geq \dim_A(B).$$

This implies $\mathscr{P}_A \subseteq \mathscr{P}_B$ and $\dim(A) = \dim_A(B)$. Conversely, if $\mathfrak{p} \in \mathscr{P}_B$, we have the inequalities

$$\dim_A(B/\mathfrak{p}^e) = \dim_A(B) = \dim(A) \geq \dim(A/\mathfrak{p}) \geq \dim_A(B/\mathfrak{p}^e)$$

so $\mathfrak{p} \in \mathscr{P}_B$ and therefore $\mathscr{P}_A = \mathscr{P}_B$. Now by Proposition 16.7.4 and Corollary 16.7.5, we have

$$e_{\mathfrak{a}}^A(A) = \sum_{\mathfrak{p} \in \mathscr{P}_A} \ell_{A_{\mathfrak{p}}}(A_{\mathfrak{p}}) \cdot e_{\mathfrak{a}}^A(A/\mathfrak{p}), \quad e_{\mathfrak{a}}^A(B) = \sum_{\mathfrak{p} \in \mathscr{P}_B} \ell_{A_{\mathfrak{p}}}(A_{\mathfrak{p}} \otimes_A B) \cdot e_{\mathfrak{a}}^A(A/\mathfrak{p}).$$

Also, by Lemma 16.7.11, under the hypothesis on ρ we have $\ell_{A_{\mathfrak{p}}}(A_{\mathfrak{p}} \otimes_A B) = \ell_{A_{\mathfrak{p}}}(A_{\mathfrak{p}}) = 1$ for every $\mathfrak{p} \in \mathscr{P}_A$, so $e_{\mathfrak{a}}^A(A) = e_{\mathfrak{a}}^A(B)$. □

Proposition 16.7.13. *Suppose that A is a Noetherian semi-local ring and reduced; let $\mathfrak{a}$ be a defining ideal of A; let $Q(A)$ be the total ring of fraction of A, and B a sub A-algebra of $Q(A)$ that is finitely generated as an A-module. Then B is semi-local and $\mathfrak{a}^e$ is a defining ideal of B. Moreover, if for any maximal ideal $\mathfrak{m}$ of B such that $\dim(B_{\mathfrak{m}}) = \dim(B)$ we have $[B/\mathfrak{m} : A/\mathfrak{m}^c] = 1$, then $e^A_{\mathfrak{a}}(A) = e^B_{\mathfrak{a}^e}(B)$.*

Proof. By Corallary 12.2.22, B is semi-local with defining ideal $\mathfrak{a}^e$. Then $e^B_{\mathfrak{a}^e}(B) = e^A_{\mathfrak{a}}(B)$ by Corollary 16.7.10. Recall that $Q(A)$ can be identified with the ring $\prod_{\mathfrak{p}} A_{\mathfrak{p}}$, where $\mathfrak{p}$ runs through minimal prime ideals of A (Proposition 12.2.24), so the canonical map $A_{\mathfrak{p}} \to A_{\mathfrak{p}} \otimes_A B$ is bijective for any minimal prime $\mathfrak{p}$ of A. The proposition them follows from Lemma 16.7.11 and Lemma 16.7.12. □

Example 16.7.14. Let k be a field with $\mathrm{char}(k) \neq 2$ and let A be the local ring $k[\![X, Y]\!]/(X^2+Y^2)$, with residue field k. It is easy to compute that $e^A_{\mathfrak{m}_A}(A) = 2$. Put $B = k[\![X, T]\!]/(T^2 + 1)$ where $T = Y/X$, we distinguish two cases:

(a) If -1 is a squre of an element i in k, then B has two maximal ideals generated by $\{X, T+i\}$ and $\{X, T - i\}$, respectively, with residue field k. We have $e^B_{\mathfrak{m}_A B}(B) = 2$.

(b) If -1 is not a squre in k, then B has a unique maximal ideal (X) with residue field $k[T]/(T^2 + 1)$, and we have $e^B_{\mathfrak{m}_A B}(B) = 1$.

16.7.3 Multiplicity and secant sequences

Proposition 16.7.15. *Suppose that A is a Noetherian local ring and $s \geq 1$ be an integer. For $1 \leq i \leq s$, let δ_i be a positive integer, x_i an element of $\mathfrak{m}_A^{\delta_i}$, and ξ_i the its class in $\mathfrak{m}_A^{\delta_i}/\mathfrak{m}_A^{\delta_i+1}$. Suppose that $(x_1, \ldots, x_s)$ is a secnat sequence for A and let $\mathfrak{x}$ be the ideal of A generated by $(x_1, \ldots, x_s)$. Then $e(A/\mathfrak{x}) \geq \delta_1 \cdots \delta_s e(A)$ and the equality holds if $(\xi_1, \ldots, \xi_s)$ is a completely secant sequence for $\mathrm{gr}(A)$.*

Proof. Put $B = A/\mathfrak{x}$, and consider the formal series

$$H_A = \sum_{n=0}^{\infty} \ell_{\kappa_A}(\mathfrak{m}_A^n/\mathfrak{m}_A^{n+1}) \cdot T^n, \quad H_B = \sum_{n=0}^{\infty} \ell_{\kappa_B}(\mathfrak{m}_B^n/\mathfrak{m}_B^{n+1}) \cdot T^n.$$

Recall that, by Proposition 16.4.25, we have the following inequality in $\mathbb{Z}[\![T]\!]$:

$$H_B^{(r)} \geq \prod_{i=1}^{s} (1 - T^{\delta_i}) H_A^{(s)} \tag{7.3.1}$$

and the equality holds if and only if $(\xi_1, \ldots, \xi_s)$ is completely secnat for $\mathrm{gr}(A)$. Put $d = \dim(A)$, so that $\dim(B) = d - s$ since $(x_1, \ldots, x_s)$ is secant for A. By Theorem 16.4.13, there then exists elements R_A and R_B in $\mathbb{Z}[T, T^{-1}]$ such that

$$H_A = (1 - T)^{-d} R_A, \quad H_B = (1 - T)^{-d+s} R_B$$

and we have $R_A(1) = e(A)$, $R_B(1) = e(A/\mathfrak{x})$. Plug this into (7.3.1), we find that

$$(1 - T)^{-d} R_B(T) = H_B^{(s)} \geq \prod_{i=1}^{s} (1 - T^{\delta_i}) H_A^{(s)} = (1 - T)^{-d} R(T) R_A(T)$$

where $R(T)$ is the polynomial in $\mathbb{Z}[T]$ given by

$$R(T) = \prod_{i=1}^{s} \frac{1 - T^{\delta_i}}{1 - T}.$$

Since $R(1) = \delta_1 \cdots \delta_s$, we conclude that $e(B) \geq \delta_1 \cdots \delta_s e(A)$, and the equality holds if and only if $(\xi_1, \ldots, \xi_s)$ is completely secant for $\mathrm{gr}(A)$. □

Remark 16.7.2. We can show conversely that, if A is a regular local ring and $(x_1, \ldots, x_s)$ is an arbitrary sequence of elements in $\mathfrak{m}$, then $e(A/\mathfrak{x}) = \delta_1 \cdots \delta_s$ if and only if the sequence $(\xi_1, \ldots, \xi_s)$ is completely secant for $\mathrm{gr}(A)$. The point is that in this case we do not need to assume that $(x_1, \ldots, x_s)$ is secant for A.

Example 16.7.16. Let A be the formal series ring $k[\![X_1, \ldots, X_n]\!]$ over a field k; let $F_1, \ldots, F_s$ be elements of A, $\mathfrak{a}$ the ideal they generate, and $B = A/\mathfrak{a}$. Let $P_1, \ldots, P_s \in k[X_1, \ldots, X_n]$ be the initial forms of the series $F_1, \ldots, F_s$ and $\delta_1, \ldots, \delta_s$ be their degrees, respectively. By Proposition 16.7.15, if the sequence $(F_1, \ldots, F_s)$ is secant for A, we have $e(B) \geq \delta_1, \ldots, \delta_s$, and the equality holds if and only if if the sequence $(P_1, \ldots, P_s)$ is completely secant for the ring $k[X_1, \ldots, X_n]$.

Consider for example the ring $B = k[\![X, Y]\!]/\mathfrak{a}$, where $\mathfrak{a}$ is generated by $X^2 + Y^3$ and $X^2 + Y^4$; the preceding inequality is $e(B) \geq 4$, and this inequality is strict because (X^2, X^2) is not completely secant. On the other hand, note that $\mathfrak{a}$ is also generated by $X^2 + Y^3$ and $Y^4 - Y^3$, for which the sequence of initial forms, namely (X^2, Y^3), is completely secant, so we obtain that $e(B) = 6$.

From now on, let A be a Noetherian ring, $\mathfrak{a}$ an ideal of A contained in the Jacobson radical of A, and M a finitely generated A-module such that $M/\mathfrak{a}M$ has finite length. Recall that in this case we can talk about the multiplicity $e_{\mathfrak{a}}(M)$ of M relative to $\mathfrak{a}$.

Proposition 16.7.17. *Let δ be a positive integer, x an element of $\mathfrak{a}^\delta$, ξ its class in $\mathfrak{a}^\delta/\mathfrak{a}^{\delta+1}$, and φ the multiplication by ξ on* $\mathrm{gr}(M)$.

(a) The dimension of the A-module M/xM is equal to $\dim_A(M)$ *or* $\dim_A(M) - 1$. *In the second case, we have $e_{\mathfrak{a}}(M/xM) \geq \delta e_{\mathfrak{a}}(M)$.*

(b) Suppose that $\dim_A(M) \geq 1$ *and the kernel of φ has finite length over $A/\mathfrak{a}$. Then we have* $\dim_A(M/xM) = \dim_A(M) - 1$. *Moreover:*

(i) If $\dim_A(M) > 1$, *then $e_{\mathfrak{a}}(M/xM) = \delta e_{\mathfrak{a}}(M)$.*

(ii) If $\dim_A(M) = 1$, *then for any $n \geq 0$ we have*

$$n\delta e_{\mathfrak{a}}(M) \leq \ell_A(M/x^nM) \leq n\delta e_{\mathfrak{a}}(M) + \ell_{A/\mathfrak{a}}(\ker \varphi^n)$$

and $\delta e_{\mathfrak{a}}(M) = e_{xA}(M) \leq \ell_A(M/xM)$.

Proof. Put $M' = M/xM$; consider the Hilbert-Samuel series $H_M = H_{M,\mathfrak{a}}$ and $H_{M'} = H_{M',\mathfrak{a}}$, as well as the Poincare series $P(T) = \sum_{n=0}^{\infty} \ell_{A/\mathfrak{a}}(\ker \varphi_n) \cdot T^n$ (where φ_n is the restriction of φ on $\mathrm{gr}_n(M)$). By Theorem 16.4.13, there then exists elements R_M and $R_{M'}$ in $\mathbb{Z}[T, T^{-1}]$ such that

$$H_M = (1 - T)^{-d} R_M, \quad H_{M'} = (1 - T)^{-d'} R_{M'}$$

where $d = \dim_A(M)$, $d' = \dim_A(M')$, $R_M(1) = e_{\mathfrak{a}}(M)$, and $R_{M'} = e_{\mathfrak{a}}(M')$. By Proposition 16.4.23, we have the inequality

$$(1 - T^\delta)H_M^{(1)} \leq H_{M'}^{(1)} \leq (1 - T^\delta)H_M^{(1)} + T^\delta P^{(1)}$$

in the ring $\mathbb{Z}((T))$. Posing $R(T) = (1 - T^\delta)/(1 - T)$, this in equivalent to

$$(1 - T)^{-d}R(T)R_M(T) \leq (1 - T)^{-d'-1}R_{M'}(T) \leq (1 - T)^{-d}R(T)R_M(T) + (1 - T)^{-1}T^\delta P(T). \quad (7.3.2)$$

By Lemma 16.4.3, the first inequality implies that, either $d < d'+1$, or $d = d'+1$ and $R(1)R_M(1) \leq R_{M'}(1)$, which means $e_{\mathfrak{a}}(M') \geq \delta e_{\mathfrak{a}}(M)$. Since we always have $d' \leq d$, this proves (a).

Under the hypothesis of (b), we have $P(T) \in \mathbb{Z}[T]$ and $P(1) = \ell_A(\ker \varphi)$. The second inequality of (7.3.2) shows

$$(1 - T)^{-d'-1}R_{M'}(T) \leq (1 - T)^{-d}[R(T)R_M(T) + T^\delta(1 - T)^{-d-1}P(T)].$$

Suppose that $d > 1$, again by Lemma 16.4.3, either $d'+1 < d$, or $d'+1 = d$ and $R_{M'}(1) = R(1)R(1)$, which means $e_{\mathfrak{a}}(M') = \delta e_{\mathfrak{a}}(M)$. This demonstrate the case (i) in (b), in view of part (a).

Suppose now $d = 1$. Then by the same reasoning, we have $d' = 0$ and

$$R_{M'}(1) \leq R(1)R_M(1) + P(1).$$

Recall that if $d' = 0$ then $R_{M'}(1) = \ell_A(M')$; therefore we conclude that

$$\delta e_{\mathfrak{a}}(M) \leq \ell_A(M/xM) \leq \delta e_{\mathfrak{a}}(M) + \ell_A(\ker \varphi). \quad (7.3.3)$$

Since $\ker \varphi$ has finite length, φ_m is injective for m large enough, so $(\varphi^n)_m$ is also injective for m large enough for each integer $n \geq 1$, which means $\ker \varphi^n$ has finite length. By replacing x with x^n in (7.3.3), we then get

$$n\delta e_{\mathfrak{a}}(M) \leq \ell_A(M/x^nM) \leq n\delta e_{\mathfrak{a}}(M) + \ell_A(\ker \varphi^n). \quad (7.3.4)$$

Now the submodules $\ker \varphi^n$ of the $\mathrm{gr}(A)$-Noetherian module $\mathrm{gr}(M)$ form an increasing sequence therefore stationary and that each of them is of finite length over $A/\mathfrak{a}$. Dividing by n in inequality (7.3.4) and letting n tend to $+\infty$, we find that $e_{xA}(M) = \delta e_{\mathfrak{a}}(M)$ by definition of $e_{xA}(M)$ (Corollary 16.4.14). □

Lemma 16.7.18. *Let R be a Noetherian graded ring with positive degrees, E a finitely generated graded R-module such that E_n has finite length over R_0 for each $n \in \mathbb{Z}$. The following conditions are equivalent:*

(i) E is an R-module of finite length;

(ii) there exists an integer n_0 such that $E_n = 0$ for $n \geq n_0$;

(iii) every associated prime of E contains R_+.

Proof. The equivalence of (i) and (ii) is clear. Let $\mathfrak{p}$ be an associated prime of E. If (iii) is satisfied, we have $\mathfrak{p} = \mathfrak{p}_0 + R_+$, where $\mathfrak{p}_0$ is a prime ideal of R_0, and the R-module $R/\mathfrak{p}$ is isomomorphic to $R_0/\mathfrak{p}_0$. By Corollary 12.2.33, the R_0-module $R_0/\mathfrak{p}_0$ is isomomorphic to a submodule of one

of the E_k, hence has finite length. Concequently, $\mathfrak{p}_0$ is a maximal ideal of R_0, and $\mathfrak{p}$ is then maximal. Since $\mathfrak{p}$ is arbitrary, it follows from Proposition 12.2.14 that E has finite length.

Conversely, assume that E has finite length and let $\mathfrak{p}$ be an associated prime of E. Then $\mathfrak{p}$ is homogeneous by Proposition 12.2.32 and maximal by Proposition 12.2.14, hence contains R_+ (Lemma 16.6.4). □

Proposition 16.7.19. *Let $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ be the prime ideals of $\mathrm{gr}(A)$ associated with the graded module $\mathrm{gr}(M)$ and not containing $\mathrm{gr}_1(A)$. Let $\delta > 0$ be an integer, ξ an element of $\mathrm{gr}_\delta(A)$, and φ the homothety of $\mathrm{gr}(M)$ with ratio ξ. Then for φ_n to be injective for all n large enough, it is necessary and sufficient that ξ does not belong to any of the $\mathfrak{p}_i$.*

Proof. In fact, the prime ideals associated with the $\mathrm{gr}(A)$-module $\ker \varphi$ is the primes associated with $\mathrm{gr}(M)$ and contain ξ. By Lemma 16.7.18, $(\ker \varphi)_n$ is zero for n large enough, if and only if these prime ideals contain $\mathrm{gr}_+(A)$ (or equivalently they contain $\mathrm{gr}_1(A)$), whence the proposition. □

An element x of A is said to be **superficial** for M relative to $\mathfrak{a}$ if it is contained in $\mathfrak{a}$ and if, for n large enough, the map $\mathfrak{a}^n M/\mathfrak{a}^{n+1}M \to \mathfrak{a}^{n+1}M/\mathfrak{a}^{n+2}M$ induced by the multiplication by x is injective. If moreover $x \in \mathfrak{a}^\delta$, then x is said to be superficial of order δ for M. In the notation of Proposition 16.7.19, we see x is superficial of order δ for M if its class ξ in $\mathrm{gr}(A)$ belongs to $\mathrm{gr}_\delta(A)$ and is not contained in the $\mathfrak{p}_i$.

By Proposition 11.1.49, there exists a homogeneous element of $\mathrm{gr}(A)$ with positive degree that does not belong to any $\mathfrak{p}_i$. Concequently, there exists an integer $\delta > 0$ and an element of A that is superficial of order δ for M.

Remark 16.7.3. We note that, by Lemma 16.7.18, an element x of A satisfies the hypothesis in Proposition 16.7.17 if and only if it is superficial for M relative to $\mathfrak{a}$.

Example 16.7.20. Suppose that A is local with maximal ideal $\mathfrak{m}$ and residue field k, and consider the canonical surjection $\pi : \mathfrak{a} \to \mathfrak{a} \otimes_A k$. Since $\mathfrak{a} \otimes_A k = \mathfrak{a}/\mathfrak{a}\mathfrak{m}$ and $\mathfrak{a} \subseteq \mathfrak{m}$, we see π factors through the canonical map $\mathfrak{a} \to \mathfrak{a}/\mathfrak{a}^2$:

$$\mathfrak{a} \longrightarrow \mathfrak{a}/\mathfrak{a}^2 \xrightarrow{\bar{\pi}} \mathfrak{a} \otimes_A k$$

By Nakayama lemma, the subspace $V_i = \bar{\pi}(\mathfrak{p}_i \cap (\mathfrak{a}/\mathfrak{a}^2))$ of $\mathfrak{a} \otimes_A k$ is proper. If $\alpha \in \mathfrak{a} \otimes_A k$ is not contained in any of the V_i, then $\pi^{-1}(\alpha)$ consists of superficial elements for M by Proposition 16.7.19. In particular, if k is infinite, the union of V_i is distinct from $\mathfrak{a} \otimes_A k$ so there exists a superficial element for M.

Theorem 16.7.21. *Let A be a Noetherian ring, $\mathfrak{a}$ an ideal of A contained in the Jacobson radical of A and M a finitely generated A-module such that $M/\mathfrak{a}M$ is of finite length. Let $x_1, \dots, x_r$ be elements of $\mathfrak{a}$ and $\mathfrak{x}$ the ideal they generate.*

(a) We have $\dim_A(M/\mathfrak{x}M) \geq \dim_A(M) - r$.

(b) If $\dim_A(M/\mathfrak{x}M) = \dim_A(M) - r$, then $e_\mathfrak{a}(M/\mathfrak{x}M) \geq e_\mathfrak{a}(M)$.

(c) If $r < \dim_A(M)$ and for each i the element x_i is superficial for $M/(x_1M + \cdots + x_{i-1}M)$ relative to $\mathfrak{a}$, then

$$\dim_A(M/\mathfrak{x}M) = \dim_A(M) - 1, \quad e_\mathfrak{a}(M/\mathfrak{x}M) = e_\mathfrak{a}(M).$$

(d) *If* $r = \dim_A(M)$ *and for each* i *the element* x_i *is superficial for* $M/(x_1M + \cdots + x_{i-1}M)$ *relative to* $\mathfrak{a}$, *then*

$$e_{\mathfrak{a}}(M) = e_{\mathfrak{x}}(M) \leq \ell_A(M/\mathfrak{x}M) < +\infty.$$

Proof. The assertions in (a), (b), and (c) for $r = 1$ follows from Proposition 16.7.17, and the general case follows by induction. Now assume the hypothesis in (d) and put $\mathfrak{x}' = Ax_1 + \cdots + Ax_{r-1}$, $M' = M/\mathfrak{x}'M$; then $M/\mathfrak{x}M$ is identified with M'/x_rM'. By part (c), we have $\dim_A(M') = 1$ and $e_{\mathfrak{a}}(M) = e_{\mathfrak{a}}(M')$; Proposition 16.7.17 also implies that $M/\mathfrak{x}M$ has finite length and

$$e_{\mathfrak{a}}(M') = e_{x_rA}(M') \leq \ell_A(M'/\mathfrak{x}_rM') = \ell_A(M/\mathfrak{x}M).$$

On the other hand, since $x_r^nM' = \mathfrak{x}^nM'$ for each n, we have $e_{x_rA}(M') = e_{\mathfrak{x}}(M')$. By applying (b) to $x_1, \ldots, x_{r-1}$, we also obtain that $e_{\mathfrak{x}}(M') \geq e_{\mathfrak{x}}(M)$, so

$$e_{\mathfrak{x}}(M) \leq e_{\mathfrak{x}}(M') = e_{x_rA}(M') = e_{\mathfrak{a}}(M') = e_{\mathfrak{a}}(M).$$

Since $\mathfrak{x}$ is contained in $\mathfrak{a}$, this implies $e_{\mathfrak{x}}(M) = e_{\mathfrak{a}}(M)$ and completes the proof. □

Corollary 16.7.22. *Suppose that* A *is local, with residue field infinite, and put* $d = \dim_A(M)$. *Then there exists a sequence* $(x_1, \ldots, x_d)$ *of elements in* $\mathfrak{a}$ *such that, if* $\mathfrak{x}$ *is the ideal they generated, then*

$$e_{\mathfrak{a}}(M) = e_{\mathfrak{x}}(M) \leq \ell_A(M/\mathfrak{x}M) < +\infty$$

Proof. This follows from Theorem 16.7.21 and Example 16.7.20. □

Remark 16.7.4. In the situation of Corollary 16.7.22, we have

$$e_{\mathfrak{a}}(M) = e_{\mathfrak{x}}(M) \leq \ell_A(M/\mathfrak{x}M), \quad \ell_A(M/\mathfrak{a}M) \leq \ell_A(M/\mathfrak{x}M).$$

The three cases

$$e_{\mathfrak{a}}(M) < \ell_A(M/\mathfrak{a}M), \quad e_{\mathfrak{a}}(M) = \ell_A(M/\mathfrak{a}M), \quad e_{\mathfrak{a}}(M) > \ell_A(M/\mathfrak{a}M)$$

are all possible.

16.7.4 Exercise

Chapter 17

Complete Noetherian local rings

In this section, all rings are assumed to be commutative with unit. We denote by 1_A for the unit of a ring A. If $\mathfrak{p}$ a prime ideal of A, we denote by $\kappa(\mathfrak{p})$ the residue field of $A_{\mathfrak{p}}$. If A is local, $\mathfrak{m}_A$ will denote its maximal ideal and κ_A its residue field.

We say a ring homomorphism $\rho : A \to B$ is flat (resp. faithfully flat) if B is a flat A-module (resp. faithfully flat A-module). Recall that by Proposition 7.3.15, if A and B are local rings, ρ is faithfully flat if and only if it is local and flat.

17.1 Witt vectors and Witt rings

17.1.1 Witt polynomials

In this part, we fix a prime number p. For a positive integer n, we define the **n-th Witt polynomial** Φ_n to be

$$\Phi_n(X_0, \dots, X_n) = \sum_{i=0}^{n} p^i X_i^{p^{n-i}} = X_0^{p^n} + pX_1^{p^{n-1}} + \cdots + p^n X_n. \tag{1.1.1}$$

Clearly we have $\Phi_0 = X_0$ and the following recursive formulae

$$\Phi_{n+1}(X_0, \dots, X_{n+1}) = \Phi_n(X_0^p, \dots, X_n^p) + p^{n+1} X_{n+1}, \tag{1.1.2}$$

$$\Phi_{n+1}(X_0, \dots, X_{n+1}) = X_0^{p^{n+1}} + p\Phi_n(X_1, \dots, X_{n+1}). \tag{1.1.3}$$

If we assign X_i with weight p^i, the polynomial Φ_n is isobare with weight p^n.

Lemma 17.1.1. *Let A be a filtered ring with $(A_n)_{n\in\mathbb{Z}}$ its filtration. Let x, y be elements of A congruent mod A_m, then*

$$x^{p^n} \equiv y^{p^n} \mod A_{m+n}. \tag{1.1.4}$$

Proof. Let $P = \sum_{i=0}^{p-1} X^i Y^{p-1-i}$ in $\mathbb{Z}[X, Y]$. From the hypothesis on x and y, we have

$$P(x, y) \equiv P(x, x) \equiv px^{p-1} \mod A_m.$$

But we have $A_m + pA \subseteq A_1$, from which $P(x, y) \in A_1$. Finally, $x^p - y^p = (x - y)P(x, y)$ is contained in $A_m A_1 \subseteq A_{m+1}$, which complete the induction process. □

Proposition 17.1.2. *Let A be a filtered ring with $(A_n)_{n\in\mathbb{Z}}$ its filtration. Suppose that $A_0 = A$ and $p \cdot 1 \in A_1$. Let $a_0, \dots, a_n$ and $b_0, \dots, b_n$ be elements of A, and $m \geq 1$ be an integer. If $a_i \equiv b_i$ mod A_m for each i, then*

$$\Phi_i(a_0, \dots, a_i) \equiv \Phi_i(b_0, \dots, b_i) \mod A_{m+i} \quad \text{for } 0 \leq i \leq n. \tag{1.1.5}$$

Moreover, the converse holds if for each integer $k \geq 1$ and $x \in A$, the relation $px \in A_{k+1}$ implies $x \in A_k$.

Proof. We prove (1.1.5) by induction on n. The case $n = 0$ is immediate, so suppose $n \geq 1$. Apply (1.1.4) on a_i and b_i, we get

$$a_i^p \equiv b_i^p \mod A_{m+1} \quad \text{for } 0 \leq i \leq n-1, \tag{1.1.6}$$

also, by the induction hypothesis on $(a_0, \dots, a_{n-1})$ and $(b_0, \dots, b_{n-1})$,

$$\Phi_{n-1}(a_0^p, \dots, a_{n-1}^p) \equiv \Phi_{n-1}(b_0^p, \dots, b_{n-1}^p) \mod A_{m+n}. \tag{1.1.7}$$

Therefore, from (1.1.2) we conclude that

$$\Phi_n(a_0, \dots, a_n) - p^n a_n \equiv \Phi_n(b_0, \dots, b_n) - p^n b_n \mod A_{m+n}. \tag{1.1.8}$$

Now $a_n - b_n$ is contained in A_m, the element $p^n a_n - p^n b_n$ then belongs to A_{m+n} and this implies the congruence

$$\Phi_n(a_0, \dots, a_n) \equiv \Phi_n(b_0, \dots, b_n) \mod A_{m+n}.$$

Conversely, assume that for each integer $k \geq 1$ and $x \in A$, the relation $px \in A_{k+1}$ implies $x \in A_k$. We prove the inverse direction by induction on n. The case $n = 0$ is clear, and suppose that $n \geq 1$. Since $a_i \equiv b_i$ mod A_m for $0 \leq i \leq n-1$, by the induction hypothesis, we deduce the congruence (1.1.6), (1.1.7), and (1.1.8). But by hypothesis $\Phi_n(a_0, \dots, a_n) \equiv \Phi_n(b_0, \dots, b_n)$ mod A_{m+n}, so $p^n(a_n - b_n) \in A_{m+n}$. Since $px \in A_{k+1}$ implies $x \in A_k$, we conclude that $a_n \equiv b_n$ mod A_m, which completes the proof. □

Let A be a ring, and give $A^{\mathbb{N}}$ the structure of product ring. We define two maps f_A and v_A by the following formulae

$$f_A(\boldsymbol{a}) = (a_1, a_2, \dots), \quad v_A(\boldsymbol{a}) = (0, pa_0, pa_1, \dots).$$

where $\boldsymbol{a} = (a_n)_{n\in\mathbb{N}}$. For any positive integer m, let Φ_m be the map on $A^{\mathbb{N}}$ defined by $\boldsymbol{a} = (a_n)_{n\in\mathbb{N}} \mapsto \Phi_m(a_0, \dots, a_m)$. We denote by Φ_A the map $\boldsymbol{a} \mapsto (\Phi_n(\boldsymbol{a}))_{n\in\mathbb{N}}$ on $A^{\mathbb{N}}$.

Lemma 17.1.3. *Suppose that A is endowed with an endomorphism σ satisfying $\sigma(a) = a^p$ mod pA for any $a \in A$. Let $a_0, \dots, a_{n-1}$ be elemnts of A. Put $u_i = \Phi_i(a_0, \dots, a_i)$ for each i, and let u_n be an element of A. Then the following conditions are equivalent:*

(i) There exists $a_n \in A$ such that $u_n = \Phi_n(a_0, \dots, a_n)$.

(ii) We have $\sigma(u_{n-1}) \equiv u_n$ mod $p^n A$.

Proof. For $0 \leq i \leq n-1$, we have $\sigma(a_i) \equiv a_i^p \mod pA$. Applying Proposition 17.1.2 on the filtration $(p^n A)_{n\in\mathbb{N}}$ and $m = 1$, we have a congruence

$$\sigma(u_{n-1}) = \Phi_{n-1}(\sigma(a_0), \dots, \sigma(a_{n-1})) \equiv \Phi_{n-1}(a_0^p, \dots, a_0^p) \mod p^n A.$$

But, from formula (1.1.2), the relation $u_n = \Phi_n(a_0, \dots, a_n)$ is equivalent to

$$u_n = \Phi_{n-1}(a_0^p, \dots, a_{n-1}^p) + p^n a_n.$$

Thus the lemma is proved. □

Proposition 17.1.4. *Let A be a ring and f_A, v_A, and Φ_A be the maps defined above.*

(a) If p is not a divisor of zero in A, the map Φ_A is injective.

(b) If p is invertible in A, the map Φ_A is bijective.

(c) If σ is an endomorphism of A satisfying $\sigma(a) = a^p$ mod pA for any $a \in A$, the image of Φ_A is a subring of $A^{\mathbb{N}}$ invariant under f_A and v_A, which consists of elements $(u_n)_{n\in\mathbb{A}}$ such that $\sigma(u_n) \equiv u_{n+1}$ mod $p^{n+1}A$ for all $n \in \mathbb{N}$.

Proof. If $\boldsymbol{a} = (a_n)_{n\in\mathbb{N}}$ and $\boldsymbol{u} = (u_n)_{n\in\mathbb{N}}$ are elements of $A^{\mathbb{N}}$, the relation $\Phi_A(\boldsymbol{a}) = \boldsymbol{u}$ is equivalent, by formula (1.1.3), to

$$\begin{cases} u_0 = a_0, \\ u_n = \Phi_{n-1}(a_0^p, \dots, a_{n-1}^p) + p^n a_n \quad \text{for} \quad n \geq 1. \end{cases} \tag{1.1.9}$$

Let $\boldsymbol{u} = (u_n)_{n\in\mathbb{N}}$ be in $A^{\mathbb{N}}$. If p is not a zero divisor of A (resp. if p is invertible in A), there then exists at most (resp. exactly) one sequence $(a_n)_{n\in\mathbb{N}}$ satisfying (1.1.9), whence (a) and (b).

Now by Lemma 17.1.3, the image of Φ_A consists of elements $\boldsymbol{u} = (u_n)_{n\in\mathbb{N}}$ of $A^{\mathbb{N}}$ such that $\sigma(u_n) = u_{n+1}$ mod $p^{n+1}A$ for all $n \in \mathbb{N}$. Since σ is an endomorphism, it follows that this is a subring of $A^{\mathbb{N}}$ and invariant under l_A and v_A. □

Remark 17.1.1. Let $\boldsymbol{a} = (a_n)_{n\in\mathbb{N}}$ and $\boldsymbol{u} = (u_n)_{n\in\mathbb{N}}$ be elements of $A^{\mathbb{N}}$ such that $\Phi_A(\boldsymbol{a}) = \boldsymbol{u}$. Then by (1.1.9), we deduce the following assertions:

(a) If the u_n, for $0 \leq n \leq m$, is contained in a subring B of A and if, for any $x \in A$, the relation $px \in B$ implies $x \in B$, then a_n, for $0 \leq n \leq m$, are contained in B.

(b) If A is graded of type $\mathbb{N}$, p is not a zero divisor of A, and u_n is homogeneous of degree dp^n for $0 \leq n \leq m$ (where $d \in \mathbb{N}$), then a_n is homogeneous of degree dp^n for $0 \leq n \leq m$.

Now let A be the polynomial ring $\mathbb{Z}[\boldsymbol{X}, \boldsymbol{Y}]$ with indeterminates $\boldsymbol{X} = (X_n)_{n\in\mathbb{N}}$ and $\boldsymbol{Y} = (Y_n)_{n\in\mathbb{N}}$. Let θ be the endomorphism of A defined by $\theta(X_n) = X_n^p$ and $\theta(Y_n) = Y_n^p$ for $n \in \mathbb{N}$. Then p is not a divisor of zero in A and the set of $a \in A$ such that $\theta(a) = a^p$ mod pA is a subring of A containing X_n and Y_n, hence equal to A. By Proposition 17.1.4(a) and (c), there exist elements $\boldsymbol{S} = (S_n)_{n\in\mathbb{N}}$, $\boldsymbol{P} = (P_n)_{n\in\mathbb{N}}$, $\boldsymbol{I} = (I_n)_{n\in\mathbb{N}}$, and $\boldsymbol{F} = (F_n)_{n\in\mathbb{N}}$ in $A^{\mathbb{N}}$ characterized by

the equalities

$$\begin{cases} \Phi_A(\boldsymbol{S}) = \Phi_A(\boldsymbol{X}) + \Phi_A(\boldsymbol{Y}) \\ \Phi_A(\boldsymbol{P}) = \Phi_A(\boldsymbol{X})\Phi_A(\boldsymbol{Y}) \\ \Phi_A(\boldsymbol{I}) = -\Phi_A(\boldsymbol{X}) \\ \Phi_A(\boldsymbol{F}) = f_A(\Phi_A(\boldsymbol{X})). \end{cases} \tag{1.1.10}$$

The elements S_n, P_n, I_n, and F_n of A are then characterized by the following formulae (where $n \in \mathbb{N}$):

$$\Phi_n(S_0, \dots, S_n) = \Phi_n(X_0, \dots, X_n) + \Phi_n(Y_0, \dots, Y_n), \tag{1.1.11}$$

$$\Phi_n(P_0, \dots, P_n) = \Phi_n(X_0, \dots, X_n)\Phi_n(Y_0, \dots, Y_n), \tag{1.1.12}$$

$$\Phi_n(I_0, \dots, I_n) = -\Phi_n(X_0, \dots, X_n), \tag{1.1.13}$$

$$\Phi_n(F_0, \dots, F_n) = \Phi_{n+1}(X_0, \dots, X_{n+1}). \tag{1.1.14}$$

Formula (1.1.3) makes it possible in practice to determine the polynomials S_n, P_n, I_n and F_n step by step.

Example 17.1.5 (First terms of the polynomials S_n, P_n, I_n, and F_n).

(a) We have

$$S_0 = X_0 + Y_0, \quad S_1 = X_1 + Y_1 - \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} X_0 Y_0^{p-i}.$$

Furthermore, $S_n - X_n - Y_n$ is in the ring $\mathbb{Z}[X_0, \dots, X_{n-1}, Y_0, \dots, Y_{n-1}]$.

(b) We have

$$P_0 = X_0 Y_0, \quad P_1 = pX_1Y_1 + X_0^p Y_1 + X_1 Y_0^p.$$

(c) If $p \neq 2$, we have $I_n = -X_n$. If $p = 2$, then

$$I_0 = -X_0, \quad I_1 = -(X_0^2 + X_1), \quad I_2 = -X_0^4 - X_0^2 X_1 - X_1^2 - X_2.$$

(d) We have

$$F_0 = X_0^p + pX_1, \quad F_1 = X_1^p + pX_2 - \sum_{i=0}^{p-1} \binom{p}{i} p^{p-i-1} X_0^{pi} X_1^{p-i}.$$

Note that $\Phi_n(F_0, \dots, F_n) \equiv \Phi_n(X_0^p, \dots, X_n^p) \bmod p^{n+1}A$ for each $n \in \mathbb{N}$ since $F_n \equiv X_n^p \bmod pA$ for each $n \in \mathbb{N}$.

Remark 17.1.2. A subset $J \subseteq \mathbb{N}_+$ is called **divisor-stable** provided that $J \neq \varnothing$, and if $n \in J$, then all proper divisors of n are also in J. If J is a divisor-stable set, we let $\mathfrak{p}(J)$ denote the set of prime numbers contained in J. For any element j in J, define the polynomial φ_j of $\mathbb{Z}[(X_j)_{j\in J}]$ by the formula

$$\varphi_j = \sum_{d|j} d X_d^{j/d}.$$

Note that we have, for each integer $n \geq 0$, that

$$\varphi_{p^n} = \Phi_n(X_{p^0}, \dots, X_{p^n}).$$

For any ring A and any $n \in J$, we denote by φ_n the map from A^J to A given by $(a_j)_{j\in J} \mapsto \varphi_n((a_j)_{j\in J})$; we denote by φ_A, or simply φ, the map A^J to A defined by $\boldsymbol{a} = (a_j)_{j\in J} \mapsto (\varphi_n(\boldsymbol{a}))_{n\in J}$. Let $\mathcal{A} = \mathbb{Z}[(X_j)_{j\in J}, (Y_j)_{J\in J}]$ be the polynomial ring of indeterminates $\boldsymbol{X} = (X_j)_{j\in J}$ and $\boldsymbol{Y} = (Y_j)_{j\in J}$. We can show that there exists elements $\boldsymbol{s} = (s_j)_{j\in J}$, $\boldsymbol{p} = (p_j)_{j\in J}$ and $\boldsymbol{i} = (i_j)_{j\in J}$ characterized by the following equalities:

$$\begin{aligned}\varphi_{\mathcal{A}}(\boldsymbol{s}) &= \varphi_{\mathcal{A}}(\boldsymbol{X}) + \varphi_{\mathcal{A}}(\boldsymbol{Y})\\ \varphi_{\mathcal{A}}(\boldsymbol{p}) &= \varphi_{\mathcal{A}}(\boldsymbol{X})\varphi_{\mathcal{A}}(\boldsymbol{Y})\\ \varphi_{\mathcal{A}}(\boldsymbol{i}) &= -\varphi_{\mathcal{A}}(\boldsymbol{X}).\end{aligned}$$

In particular, this definition works, for example, if J is the set of integers $j \geq 1$.

17.1.2 The ring of Witt vectors

Let A be a ring. If $\boldsymbol{a} = (a_n)_{n\in\mathbb{N}}$ and $\boldsymbol{b} = (b_n)_{n\in\mathbb{N}}$ are elements of $A^{\mathbb{N}}$, we denote by $S_A(\boldsymbol{a}, \boldsymbol{b})$, or simply $S(\boldsymbol{a}, \boldsymbol{b})$, the sequence $(S_n(a_0, \dots, a_n, b_0, \dots, b_n))_{n\in\mathbb{N}}$. Simialrly, we denote by $P_A(\boldsymbol{a}, \boldsymbol{b})$ and $I_A(\boldsymbol{a})$ the resulting substitutions. By substituting X_n into a_n, Y_n into b_n, for each $n \in \mathbb{N}$, in the formulae (1.1.11), (1.1.12), and (1.1.13), we obtain the equalities

$$\Phi_A(S_A(\boldsymbol{a}, \boldsymbol{b})) = \Phi_A(\boldsymbol{a}) + \Phi_A(\boldsymbol{b}) \tag{1.2.1}$$

$$\Phi_A(P_A(\boldsymbol{a}, \boldsymbol{b})) = \Phi_A(\boldsymbol{a})\Phi_A(\boldsymbol{b}) \tag{1.2.2}$$

$$\Phi_A(I_A(\boldsymbol{a})) = -\Phi_A(\boldsymbol{a}). \tag{1.2.3}$$

We will denote by $W(A)$ the set $A^{\mathbb{N}}$ endowed with the laws of composition S_A and P_A.

Let $\rho : A \to B$ be a ring homomorphism. We denote $W(\rho)$ the map $\rho^{\mathbb{N}} : A^{\mathbb{N}} \to B^{\mathbb{N}}$ which sends an element $\boldsymbol{a} = (a_n)_{n\in\mathbb{N}}$ to $(\rho(a_n))_{n\in\mathbb{N}}$. From the definition, we have

$$W(\rho) \circ S_A = S_B \circ (W(\rho) \times W(\rho)) \tag{1.2.4}$$

$$W(\rho) \circ P_A = P_B \circ (W(\rho) \times W(\rho)) \tag{1.2.5}$$

$$W(\rho) \circ I_A = I_B \circ W(\rho) \tag{1.2.6}$$

$$W(\rho) \circ \Phi_A = \Phi_B \circ W(\rho) \tag{1.2.7}$$

Lemma 17.1.6. *Let A be a ring. Then there exists a surjective homomorphism $\rho : B \to A$, where B is a ring satisfying the following condition: p is not a divisor of zero in B, and there exists an endomorphism σ of B such that $\sigma(b) \equiv b^p$ mod pB for any $b \in B$.*

Proof. It suffices to take $B = \mathbb{Z}[(X_a)_{a\in A}]$, and let σ be the endomorphism on B defined by $\sigma(X_a) = X_a^p$ for any $a \in A$. The homomorphism $\rho : B \to A$ is defined to send X_a to a for any $a \in A$. □

Theorem 17.1.7. *Let A be a ring.*

(a) With the map S_A and P_A, the set $W(A)$ is a commutative ring. The addition identity is the sequence $\mathbf{0}_A$ with zero terms, and the multiplication identity is the sequence $\mathbf{1}_A$ of which all the terms are zero except that of index 0 which is equal to 1. The additive inverse of an element $\boldsymbol{a}$ in $W(A)$ is $I_A(\boldsymbol{a})$.

(b) *Let $\rho : A \to B$ be a homomorphism of rings. Then the induced map $W(\rho) : W(A) \to W(B)$ is a homomorphism of rings.*

(c) *The map Φ_A is a homomorphism from $W(A)$ to the product ring $A^{\mathbb{N}}$. In particular, for each $n \in \mathbb{N}$, the map $\Phi_n : \boldsymbol{a} \mapsto \Phi_n(a_0, \dots, a_n)$ is a homomorphism from $W(A)$ to A.*

Proof. Concerning the formulae (1.2.1), (1.2.2), (1.2.4), and (1.2.7), it suffices to prove (a). Let $\rho : B \to A$ be a ring homomorphism satisfying the conditions in Lemma 17.1.6. Let B' be the image of Φ_B in $B^{\mathbb{N}}$, which by Proposition 17.1.4 consists of elements $(b_n)_{n\in\mathbb{N}}$ such that $\sigma(b_n) \equiv b_{n+1} \bmod p^{n+1}B$ for all $n \in \mathbb{N}$. By Proposition 17.1.4, Φ_B induces a bijection between $W(B)$ and B'. In view of the formulas (1.2.1) to (1.2.3) and the relations $\Phi_n(\mathbf{0}_B) = 0$ and $\Phi_n(\mathbf{1}_B) = 1$, we get a ring structure on $W(B)$ by transporting structure, with addition identity $\mathbf{0}_B$, multiplication identity $\mathbf{1}_B$, and additive inverse $I_B(\boldsymbol{b})$.

The map $W(\rho) : W(B) \to W(A)$ is surjective (since ρ is surjective). By the fomulae (1.2.4) and (1.2.5), the equivalence relation R on $W(B)$ associated with the map $W(\phi)$ is compatible with the ring structure on $W(B)$. Thus $W(\rho)$ is a bijection from the quotient ring $W(B)/R$ to $W(A)$, compatible with addition and multiplication. Assertion (a) then follows by transporting structure. □

For a ring A, the ring $W(A)$ is called the **Witt ring** with coefficients in A. For $\boldsymbol{a}$ in $W(A)$ and $n \in \mathbb{N}$, the element $\Phi_n(\boldsymbol{a}) = \Phi_n(a_0, \dots, a_n)$ is called the **phantom components** of order n of $\boldsymbol{a}$.

Remark 17.1.3. Retain the notations in Remark 17.1.2. Let A be a ring. If $\boldsymbol{a}$ and $\boldsymbol{b}$ and elements of A^J and $\boldsymbol{r} = (r_j)_{j\in J}$ belongs to $\mathcal{A}^J$, we denote by $\boldsymbol{r}_A(\boldsymbol{a}, \boldsymbol{b})$ the element $(r_j(\boldsymbol{a}, \boldsymbol{b}))_{j\in J}$ of A^J. Let $U(A)$ be the set A^J endowed with the maps $\boldsymbol{s}_A$ and $\boldsymbol{p}_A$. WE can show that, with the addition $\boldsymbol{s}_A$ and multiplication $\boldsymbol{p}_A$, $U(A)$ is a commutative ring; we call it the **universal Witt ring** of A. The addition idnetity of $U(A)$ is the element with components all zero, and the multiplication identity is the element with components zero except 1_A at index 1; the additive inverse of $\boldsymbol{a}$ in $U(A)$ is $\boldsymbol{i}_A(\boldsymbol{a})$. The map φ_A is a homomorphism of $U(A)$ to the product ring A^J.

From now on, we use + and × to denote the addition and multiplication in the ring $W(A)$; for simplicity, we write $\mathbf{0}$ for $\mathbf{0}_A$ and $\mathbf{1}$ for $\mathbf{1}_A$. Let us introduce[1] two maps F_A and V_A on $W(A)$ by the formulae

$$F_A(\boldsymbol{a}) = (F_n(a_0, \dots, a_{n+1}))_{n\in\mathbb{N}}, \tag{1.2.8}$$

$$V_A(\boldsymbol{a}) = (0, a_0, a_1, \dots). \tag{1.2.9}$$

where $\boldsymbol{a} = (a_n)_{n\in\mathbb{N}}$. The map V_A is often called the **shift** operator. Note that by (1.1.14) we have the formula

$$\Phi_n(F_0(\boldsymbol{a}), \dots, F_n(\boldsymbol{a})) = \Phi_{n+1}(a_0, \dots, a_{n+1}).$$

We can also write it in the form

$$\Phi_A \circ F_A = f_A \circ \Phi_A. \tag{1.2.10}$$

[1]The letter F is the initial of the name of Frobenius, and the latter V is that of the German word *Verschiebung*, which means shift.

From the recursive formula (1.1.3), we can also prove that

$$\Phi_A \circ V_A = v_A \circ \Phi_A. \tag{1.2.11}$$

Let $\rho : A \to B$ be a ring homomorphism. It is clear that we have

$$W(\rho) \circ F_A = F_B \circ W(\rho), \tag{1.2.12}$$
$$W(\rho) \circ V_A = V_B \circ W(\rho). \tag{1.2.13}$$

Proposition 17.1.8. *Let A be a ring and $W(A)$ be the Witt ring with coefficients A.*

(a) The map F_A is an endomorphism of the ring $W(A)$, and V_A is an endomorphism of the additive group of $W(A)$.

(b) For $\boldsymbol{a} \in W(A)$, we have $F_A(V_A(\boldsymbol{a})) = p \cdot \boldsymbol{a}$.

(c) Let $\boldsymbol{a}$ and $\boldsymbol{b}$ be elements in $W(A)$. Then we have

$$V_A(\boldsymbol{a} \times F_A(\boldsymbol{b})) = V_A(\boldsymbol{a}) \times \boldsymbol{b}, \tag{1.2.14}$$
$$V_A(\boldsymbol{a}) \times V_A(\boldsymbol{b}) = p \cdot V_A(\boldsymbol{a} \times \boldsymbol{b}). \tag{1.2.15}$$

(d) Put $\boldsymbol{\mu} = V_A(\mathbf{1}) = (0, 1, 0, \dots)$. Then for $\boldsymbol{b}$ in $W(A)$ we have

$$V_A(F_A(\boldsymbol{b})) = \boldsymbol{\mu} \times \boldsymbol{b}. \tag{1.2.16}$$

(e) For any element $\boldsymbol{a}$ in $W(A)$, denote by $\boldsymbol{a}^p$ the p-th power of $\boldsymbol{a}$ in $W(A)$. Then

$$F_A(\boldsymbol{a}) \equiv \boldsymbol{a}^p \mod pW(A). \tag{1.2.17}$$

Proof. Let $\rho : B \to A$ be a ring homomorphism satisfying the conditions of Lemma 17.1.6. Then $W(\rho) : W(B) \to W(A)$ is a surjective ring homomorphism, and $\Phi_B : W(B) \to B^{\mathbb{N}}$ is an injective homomorphism of rings. Furthermore, $f_B : B^{\mathbb{N}} \to B^{\mathbb{N}}$ is a ring homomorphism. By the formulae (1.2.10) and (1.2.12), we have

$$\Phi_B \circ F_B = f_B \circ \Phi_B, \quad W(\rho) \circ F_B = F_A \circ W(\rho),$$

which proves the first assertion of (a). The second one can be proved similarly, using (1.2.11) and (1.2.13).

Let $\boldsymbol{a}$ be an element of $W(A)$, and choose a element $\boldsymbol{x}$ in $W(B)$ whose image under $W(\rho)$ is $\boldsymbol{a}$. Put $\xi = \Phi_B(\boldsymbol{x})$. By definition of f_B and v_B, we have $f_B(v_B(\xi)) = p \cdot \xi$. By formulae (1.2.10) and (1.2.11), the elements $F_B(V_B(\boldsymbol{x}))$ and $p \cdot \boldsymbol{x}$ of $W(B)$ then have the same image under the injective map Φ_B, and therefore are equal. The formula $F_A(V_A(\boldsymbol{a})) = p \cdot \boldsymbol{a}$ follows then from (1.2.12) and (1.2.13). This proves (b).

Reasoning analogously, we reduce the demonstration of formula (1.2.14) to the relation

$$v_B(\xi f_B(\eta)) = v_B(\xi)\eta$$

where ξ, η are in $B^{\mathbb{N}}$. This follows from the equalities

$$\xi f_B(\eta) = (\xi_0\eta_1, \xi_1\eta_2, \dots), \quad v_B(\xi)\eta = (0, p\xi_0\eta_1, p\xi_1\eta_2, \dots).$$

Taking into account (a) and (b), the formula (1.2.15) results from the formula (1.2.14), where we replace $\boldsymbol{b}$ by $V_A(\boldsymbol{b})$. Formula (1.2.16) is the particular case $\boldsymbol{a} = \mathbf{1}$ of formula (1.2.14).

Simialrly, we deduce the formula (1.2.17) from the relation

$$f_B(\xi) \equiv \xi^p \mod p\Phi_B(B^{\mathbb{N}})$$

where ξ^p denote the product of $B^{\mathbb{N}}$. By Proposition 17.1.4(c), this is equivalent to the fact that for all $n \geq 0$, we have

$$\sigma(\xi_{n+1} - \xi_n^p) \equiv \xi_{n+2} - \xi_{n+1}^p \mod p^{n+2}B.$$

But, for $n \geq 0$, we have $\sigma(\xi_n) \equiv \xi_{n+1} \bmod p^{n+1}B$, since $\xi = \Phi_B(\boldsymbol{x})$ (again by Proposition 17.1.4(c)); we then deduce from Lemma 17.1.1 that

$$\sigma(\xi_n)^p \equiv \xi_{n+1}^p \mod p^{n+2}B,$$

which completes the proof. □

17.1.3 Filtration and topology of the Witt ring

Lemma 17.1.9. *Let A be a ring and $m \geq 1$ an integer. Then*

$$\boldsymbol{a} = (a_0, \dots, a_{m-1}, 0, \dots) + (\underbrace{0, \dots, 0}_{m\text{-terms}}, a_m, a_{m+1}, \dots)$$

for any $\boldsymbol{a}$ in $W(A)$.

Proof. Let $\rho : B \to A$ be a ring homomorphism satisfying the conditions of Lemma 17.1.6. Then $W(\rho) : W(B) \to W(A)$ is a surjective ring homomorphism, and $\Phi_B : W(B) \to B^{\mathbb{N}}$ is an injective homomorphism of rings. It suffices to prove that

$$\Phi_n(\boldsymbol{b}) = \Phi_n(b_0, \dots, b_{m-1}, 0, \dots) + \Phi_n(0, \dots, 0, b_m, b_{m+1}, \dots) \tag{1.3.1}$$

for any $\boldsymbol{b}$ in $W(B)$ and $m \geq 1$. But we have

$$\Phi_n(b_0, \dots, b_{m-1}, 0, \dots) = \begin{cases} \Phi_n(b_0, \dots, b_n) & \text{if } 0 \leq n < m \\ \sum_{i=0}^{m-1} p^i b_i^{p^{n-i}} & \text{if } m \leq n \end{cases}$$

and

$$\Phi_n(0, b_m, b_{m+1}, \dots) = \begin{cases} 0 & \text{if } 0 \leq n < m \\ \sum_{i=m}^{m} p^i b_i^{p^{n-i}} & \text{if } m \leq n, \end{cases}$$

whence the formula (1.3.1). □

Let A be a ring. For each integer $m \geq 0$, we denote by $V_m(A)$ the set of Witt vectors $\boldsymbol{a} = (a_n)_{n\in\mathbb{N}}$ such that $a_n = 0$ for $0 \leq n < m$, which is also the m-fold image of V_A. From

Proposition 17.1.8 and induction on m, we have the formulae

$$V^m(\boldsymbol{a}+\boldsymbol{b}) = V^m(\boldsymbol{a}) + V^m(\boldsymbol{b}), \tag{1.3.2}$$

$$V^m(\boldsymbol{a}) \times \boldsymbol{b} = V^m(\boldsymbol{a} \times F^m(\boldsymbol{b})). \tag{1.3.3}$$

We set $V_m(A) = W(A)$ if $m < 0$. The sequence $(V_m(A))_{m\in\mathbb{Z}}$ is then a decreasing filtration of additive subgroups of $W(A)$, and is compatible with the ring structure of $W(A)$ if and only if the ring A has characteristic p.

In the following, we denote by $\mathcal{T}$ the topology on $W(A)$ associated with the filtration $(V_m(A))_{m\in\mathbb{Z}}$. As $V_m(A)$ is an ideal of $W(A)$ for all $m \in \mathbb{Z}$, the topology $\mathcal{T}$ is compatible with the ring structure of $W(A)$ (Example 3.3.8). Let $\boldsymbol{a} \in W(A)$; the sets $\boldsymbol{a} + V_m(A)$, for $m \in \mathbb{N}$, form a fundamental system of neighborhoods of $\boldsymbol{a}$ in $\mathcal{T}$. By Lemma 17.1.9, $\boldsymbol{a} + V_m(A)$ consists of Witt vectors $\boldsymbol{b}$ such that $a_i = b_i$ for $0 \leq i < m$. Consequently, $\mathcal{T}$ is none other than the topology product on $A^{\mathbb{N}}$ of the discrete topology on each of the factors, and $W(A)$ is therefore a separated and complete topological ring.

Let τ_A be the map of A to $W(A)$ that sends an element a of A to $(a, 0, 0, \dots)$. We have $\Phi_n(\tau(a)) = a^{p^n}$ for each $n \in \mathbb{N}$. For any ring homomorphism $\rho : B \to A$, it is clear that $W(\rho) \circ \tau_B = \tau_A \circ \rho$.

Proposition 17.1.10. *Let a, b be elements of A and $\boldsymbol{x} = (x_n)_{n\in\mathbb{N}}$ an element of $W(A)$.*

(a) We have the formulas

$$\tau(ab) = \tau(b) \times \tau(b), \tag{1.3.4}$$

$$\tau(a) \times \boldsymbol{x} = (a^{p^n} x_n)_{n\in\mathbb{N}}. \tag{1.3.5}$$

(b) The series $\sum_n V^n(\tau(x_n))$ converges in $W(A)$ to $\boldsymbol{x}$.

Proof. Let n be a positive integer. The polynomial $P_n(X_0, \dots, X_n, Y_0, \dots, Y_n)$ is isobare with weight p^n is we assign X_i with weight p^i. We then have

$$P_n(X_0, 0, \dots, 0, Y_0, \dots, Y_n) = X_0^{p^n} P_n(1, 0, \dots, 0, Y_0, \dots, Y_n).$$

Since $\mathbf{1} = (1, 0, 0, \dots)$ is a unit in the Witt ring with coefficients in $\mathbb{Z}[(X_n)_{n\in\mathbb{N}}, (Y_n)_{n\in\mathbb{N}}]$, we have

$$P_n(1, 0, \dots, 0, Y_0, \dots, Y_n) = Y_n.$$

By Substituting X_0 with a and Y_i with x_i, we deduce that

$$P_n(a, 0, \dots, 0, x_0, \dots, x_n) = a^{p^n} x_n.$$

By the definition of product in $W(A)$, this proves (1.3.5), and (1.3.4) is a special case of (1.3.5).

We now prove (b). By definition, $V^n(\tau(x_n))$ is the sequence of which all the components are zero, except that of index n which is equal to x_n. It follows from Lemma 17.1.9, by induction on m, which we have

$$\sum_{n=0}^{m} V^n(\tau(x_n)) = (x_0, \dots, x_m, 0, 0, \dots)$$

for each $m \geq 0$; we then deduce (b) by passing to limit in the topology $\mathcal{T}$ of $W(A)$, which is the product of the discrete topology on A. □

Now for each integer $n \geq 1$, let $W_n(A)$ be the quotient ring $W(A)/V_n(A)$. For any elements $a_0, \dots, a_{n-1}$ of A, we denote by $[a_0, \dots, a_{n-1}]$ or $[a_i]_{0 \leq i < n}$ the class modulo $V_n(A)$ of the element $(a_0, \dots, a_{n-1}, 0, 0, \dots)$ of $W(A)$. By Lemma 17.1.9, the map $(a_0, \dots, a_{n-1}) \mapsto [a_0, \dots, a_{n-1}]$ from A^n to $W_n(A)$ is bijective. For this reasong, we say that the elements of $W_n(A)$ are the Witt vectors of length n; similarly, one sometimes qualifies as Witt vectors of infinite length the elements of $W(A)$.

We denote by π_n the canonical homomorphism from $W(A)$ to $W_n(A)$. According to Lemma 17.1.9, for $\boldsymbol{a} = (a_n)_{n \in \mathbb{N}}$ in $W(A)$, we have

$$\pi_n(\boldsymbol{a}) = [a_0, \dots, a_{n-1}].$$

By the definition of the ring structure of $W(A)$, we have the following description of operations in $W_n(A)$:

$$\begin{aligned}
[a_0, \dots, a_{n-1}] + [b_0, \dots, b_{n-1}] &= [S_i(a_0, \dots, a_i; b_0, \dots, b_i)]_{0 \leq i < n} \\
[a_0, \dots, a_{n-1}] \times [b_0, \dots, b_{n-1}] &= [S_i(a_0, \dots, a_i; b_0, \dots, b_i)]_{0 \leq i < n} \\
-[a_0, \dots, a_{n-1}] &= [I_i(a_0, \dots, a_i)]_{0 \leq i < n}.
\end{aligned}$$

Moreover, the addition identity of $W_n(A)$ is $[0, \dots, 0]$ and the multiplication identity of $W(A)$ is $[1, 0, \dots, 0]$.

Let i be an integer such that $0 \leq i \leq n$. By passing to quotient, the homomorphism Φ_i from $W(A)$ to A defines a homomorphism from $W_n(A)$ to A, still denoted by Φ_i. It associates an Witt vector the element $\Phi_i(a_0, \dots, a_i)$ (called the phantom component of index i of $[a_0, \dots, a_{n-1}]$).

Let $\rho : A \to B$ be a ring homormorphism. By passing to quotient, the ring homomorphism $W(\rho)$ induces a homomorphism $W_n(\rho) : W_n(B) \to W_n(A)$. We have the following formula

$$W_n(\rho)[b_0, \dots, b_{n-1}] = [\rho(b_0), \dots, \rho(b_{n-1})] \tag{1.3.6}$$

for $[b_0, \dots, b_{n-1}]$ in $W_n(B)$.

Let m and n be integers such that $1 \leq n \leq m$. We have $V_n(A) \supset V_m(A)$, whence a canonical homomorphism $W_m(A) = W(A)/V_m(A)$ to $W_n(A) = W(A)/V_n(A)$, denoted by $\pi_{n,m}$. More precisely,

$$\pi_{n,m}[a_0, \dots, a_{m-1}] = [a_0, \dots, a_{n-1}] \tag{1.3.7}$$

for $[a_0, \dots, a_{m-1}]$ in $W_m(A)$. The family $(W_n(A), \pi_{n,m})$ is a inverse system of rings and the map $\pi : \boldsymbol{a} \mapsto (\pi_n(\boldsymbol{a}))_{n \geq 1}$ is a ring homomorphism from $W(A)$ to $\varprojlim W_n(A)$. Since $W(A)$ is separated and complete for the filtration $(V_n(A))_{n \in \mathbb{Z}}$, the canonical homomorphism π is an isomorphism of topological rings, where $W_n(A)$ has the discrete topology for each $n \geq 1$.

Henceforth, the homomorphisms π_n and $\pi_{n,m}$ will be called the projection from $W(A)$ to $W_n(A)$ and $W_m(A)$ to $W_n(A)$, respectively.

Example 17.1.11.

(a) The homomorphism $\Phi_0 : W_1(A) \to A$ is an isomorphism.

(b) Explicitly, the operations on $W_2(A)$ are given by

$$[a_0, a_1] + [b_0, b_1] = [a_0 + b_0, a_1 + b_1 - \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} a_0^i b_0^{p-i}],$$
$$[a_0, a_1] \times [b_0, b_1] = [a_0 b_0, a_0^p b_1 + a_1 b_0^p + p a_1 b_1].$$

where $[a_0, a_1]$ and $[b_0, b_1]$ are in $W_2(A)$. The phantom componenet of $[a_0, a_1]$ is a_0 and $a_0^p + p a_1$.

(c) Let $n \geq 1$ be an integer. If $a_0, \ldots, a_{n-1}$ and $b_0, \ldots, b_{n-1}$ are integers such that $a_i \equiv b_i \bmod p$ for each i, then (Proposition 17.1.2)

$$\Phi_{n-1}(a_0, \ldots, a_{n-1}) \equiv \Phi_{n-1}(b_0, \ldots, b_{n-1}) \mod p^n.$$

Therefore, by passing to quotient, Φ_{n-1} defines a homomorphism $\varphi_n : W_n(\mathbb{Z}/p\mathbb{Z}) \to \mathbb{Z}/p^n\mathbb{Z}$. The image of φ_n is a subgroup of $\mathbb{Z}/p^n\mathbb{Z}$ containing 1, hence the whole $\mathbb{Z}/p^n\mathbb{Z}$. Since $\mathbb{Z}/p^n\mathbb{Z}$ and $W_n(\mathbb{Z}/p\mathbb{Z})$ are both finite sets, φ_n is an isomorphism.

Let m and n be integers such that $1 \leq n \leq m$. There exists a ring homomorphism $\alpha_{n,m} : \mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$; moreover, the diagram

$$\begin{tikzcd} \mathbb{Z}/p^m\mathbb{Z} \arrow[r, "\alpha_{n,m}"] \arrow[d] & \mathbb{Z}/p^n\mathbb{Z} \arrow[d] \\ W_m(\mathbb{Z}/p\mathbb{Z}) \arrow[r, "\pi_{n,m}"] & W_n(\mathbb{Z}/p\mathbb{Z}) \end{tikzcd}$$

is commutative. This then gives a map $\varphi = \varprojlim \varphi_n$ and an isomorphism of topological rings $W(\mathbb{Z}/p\mathbb{Z}) = \varprojlim W_n(\mathbb{Z}/p\mathbb{Z})$ and $Z_{\mathfrak{p}} = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$.

Let $m, n \geq 1$ be integers. By construction, we have an exact sequence of additive groups

$$0 \longrightarrow W(A) \xrightarrow{V^m} W(A) \xrightarrow{\pi_m} W_m(A) \longrightarrow 0 \tag{1.3.8}$$

By passing to quotient, the endomorphism V^n of the additive group of $W(A)$ defines a homomorphism V_m^n on the additive group $W_m(A)$ to $W_{m+n}(A)$. In other words, we have a commutative diagram

$$\begin{tikzcd} W(A) \arrow[r, "V^n"] \arrow[d, "\pi_n"] & W(A) \arrow[d, "\pi_{n+m}"] \\ W_m(A) \arrow[r, "V_m^n"] & W_{n+m}(A) \end{tikzcd}$$

Moreover, from (1.3.8) we deduce the following exact sequence

$$0 \longrightarrow W_m(A) \xrightarrow{V_m^n} W_{m+n}(A) \xrightarrow{\pi_{n,n+m}} W_n(A) \longrightarrow 0 \tag{1.3.9}$$

and for $[a_0, \ldots, a_{m-1}]$ in $W_m(A)$,

$$V_m^n[a_0, \ldots, a_{m-1}] = [\underbrace{0, \ldots, 0}_{n \text{ terms}}, a_0, \ldots, a_{m-1}] \tag{1.3.10}$$

From Eq. (1.2.16)(c), we have $FV^{m+1}(\boldsymbol{a}) = p \cdot V^m(\boldsymbol{a})$ for $\boldsymbol{a}$ in $W(A)$ and therefore $F(V_{m+1}(A)) \subseteq V_m(A)$. By induction on n, we then deduce that F^n maps $V_{n+m}(A)$ to $V_m(A)$, and therefore defines, by passing to quotient, a homomorphism $F^n_m : W_{n+m}(A) \to W_m(A)$. By construction, we have the following exact sequence

$$\begin{tikzcd} W(A) \arrow[r, "F^n"] \arrow[d, "\pi_{n+m}"] & W(A) \arrow[d, "\pi_m"] \\ W_{n+m}(A) \arrow[r, "F^n_m"] & W_m(A) \end{tikzcd}$$

Recall the polynomial F_i in $\mathbb{Z}[X_0, \dots, X_{i+1}]$ for each $i \geq 0$. The homomorphism F^1_m of $W_{m+1}(A)$ to $W_m(A)$ has the following explicit expression

$$F^1_m[a_0, \dots, a_m] = [F_i(a_0, \dots, a_{i+1})]_{0 \leq i < m}. \tag{1.3.11}$$

Let $\boldsymbol{a}, \boldsymbol{a}' \in W_m(A)$ and $\boldsymbol{b} \in W_{m+1}(A)$. The following formulae then follows from Eq. (1.2.16):

$$\begin{aligned} F^1_m(V^1_m(\boldsymbol{a})) &= p \cdot \boldsymbol{a} \\ V^1_m(\boldsymbol{a} \times F^1_m(\boldsymbol{b})) &= V^1_m(\boldsymbol{a}) \times \boldsymbol{b} \\ V^1_m(\boldsymbol{a}) \times V^1_m(\boldsymbol{a}') &= p \cdot V^1_m(\boldsymbol{a} \times \boldsymbol{a}') \\ V^1_m(F^1_m(\boldsymbol{b})) &= \boldsymbol{\mu}_{m+1} \times \boldsymbol{b} \end{aligned}$$

where $\boldsymbol{\mu}_{m+1} = [0, 1, 0 \dots, 0]$.

17.1.4 The Witt ring with characteristic p

Proposition 17.1.12. *Let A be a ring with characteristic p. Then for $\boldsymbol{a}, \boldsymbol{b}$ in $W(A)$ and positive integers m, n, we have*

$$F(\boldsymbol{a}) = (a_n^p)_{n \in \mathbb{N}} \tag{1.4.1}$$

$$p \cdot \boldsymbol{a} = VF(\boldsymbol{a}) = FV(\boldsymbol{a}) = (0, a_0^p, a_1^p, \dots) \tag{1.4.2}$$

$$V^m(\boldsymbol{a}) \times V^n(\boldsymbol{b}) = V^{m+n}(F^n(\boldsymbol{a}) \times F^m(\boldsymbol{b})). \tag{1.4.3}$$

Proof. The formula (1.4.1) follows from Example 17.1.5(d). We immediately deduce from this the equality

$$VF(\boldsymbol{a}) = FV(\boldsymbol{a}) = (0, a_0^p, a_1^p, \dots)$$

and the equality $p \cdot \boldsymbol{a} = FV(\boldsymbol{a})$ is already proved in Proposition 17.1.8(b), whence (1.4.2). Now recall that by (1.3.3), we have

$$V^m(\boldsymbol{a}) \times V^n(\boldsymbol{b}) = V^m(\boldsymbol{a} \times F^m(V^n(\boldsymbol{b}))).$$

By (1.3.2), we also deduce that

$$V^n(F^m(\boldsymbol{b})) \times \boldsymbol{a} = V^n(F^m(\boldsymbol{b}) \times F^n(\boldsymbol{a})).$$

Fomula (1.4.3) then follows from these two equalities and the relation $F^m \circ V^n = V^n \circ F^m$, which

comes from (1.4.1). □

Corollary 17.1.13. *Let m and n be positive integers, then*

$$V_m(A) \times V_n(A) \subseteq V_{m+n}(A).$$

Proof. This follows from (1.4.3), since $V_m(A)$ is the image of V^m. □

Remark 17.1.4. Let A be a ring with characteristic p. By Proposition 17.1.12, we have the formulae

$$F_m^n[a_0, \dots, a_{n+m-1}] = [a_0^{p^n}, \dots, a_{m-1}^{p^n}], \quad p^n \cdot [a_0, \dots, a_{n+m-1}] = [\underbrace{0, \dots, 0}_{n \text{ terms}}, a_0^{p^n}, \dots, a_{m-1}^{p^n}]$$

for any Witt vector $[a_0, \dots, a_{n+m-1}]$ of length $n + m$.

Proposition 17.1.14. *Let A be a ring.*

(a) For each integer $k \geq 1$, we have $V_1(A)^k = p^{k-1} \cdot V_1(A)$.

(b) Suppose that A is a ring with characteristic p. Then the $V_1(A)$-adic topology and the p-adic topology coincide on $W(A)$, and is finer than the topology $\mathcal{T}$. The ring $W(A)$ is separated and complete for the p-adic topology.

Proof. We prove (a) by induction on k. The case $k = 1$ is evident, so suppose $k \geq 2$. By the induction hypothesis, we have $V_1(A)^{k-1} = p^{k-2} \cdot V_1(A)$ and Concequently $V_1(A)^k = p^{k-2} \cdot V_1(A)^2$. But by Eq. (1.2.15)(d), $V_1(A)^2 = p \cdot V_1(A)$, so (a) follows.

Suppose now that A has characteristic p. Then by (1.4.2),

$$pW(A) = VF(W(A)) \subseteq V_1(A)$$

combine this with (a), we deduce by induction that $p^k \cdot W(A) \subseteq V_1(A)^k \subseteq p^{k-1} \cdot W(A)$, and by Corollary 17.1.13 the inclusion $V_1(A)^k \subseteq V_k(A)$, for each $k \geq 1$. The first assertion in (b) then follow.

Let $k \geq 1$ be an integer. By (1.4.2), the ideal $p^k \cdot W(A)$ of $W(A)$ is the set of elements $\boldsymbol{a} = (a_n)_{n \in \mathbb{N}}$ of $W(A)$ such that $a_n = 0$ for $n < k$ and $a_n \in A^{p^k}$ for $n \geq k$. It is therefore closed in the topology $\mathcal{T}$. Since $W(A)$ is separated and complete for the topology $\mathcal{T}$ and that the ideals $p^k \cdot W(A)$ of $W(A)$, for $k \geq 1$, form a base of neighborhoods of $\mathbf{0}$ in $W(A)$ for the p-adic topology, the ring $W(A)$ is separated and complete for the p-adic topology (Proposition 3.2.19). □

Proposition 17.1.15. *Let A be a perfect ring of characteristic p.*

(a) For any element $\boldsymbol{a} = (a_n)_{n \in \mathbb{N}}$ in $W(A)$, the series $\sum_n p^n \tau(a_n^{p^{-n}})$ converges in $W(A)$ to $\boldsymbol{a}$.

(b) In $W(A)$, the $V_1(A)$-adic topology, the p-adic topology, and the topology $\mathcal{T}$ coincide. Moreover precisely, we have $V_n(A) = p^n W(A) = V_1(A)^n$ for each integer $n \geq 0$. In particular, Φ_0 defines an isomorphism of $W(A)/pW(A)$ to A.

Proof. By definition, the map $a \mapsto a^p$ is an automorphism of A. Proposition 17.1.12 then show that F is an automorphism of $W(A)$, and for $n \in \mathbb{N}$, we have

$$p^n \cdot W(A) = V^n F^n(W(A)) = V^n(W(A)) = V_n(A).$$

In particular, $V_1(A)^n = (pW(A))^n = p^n \cdot W(A)$. Assertion (b) then follows. By Proposition 17.1.12, we have

$$p^n \cdot \tau(a_n^{p^{-n}}) = V^n F^n \tau(a_n^{p^{-n}}) = V^n \tau(a_n)$$

so (a) follows from Proposition 17.1.10. □

Proposition 17.1.16. *Let A be a field with characteristic p. Then $W(A)$ is a local integral domain, separated and complete, with maximal ideal $V_1(A)$ and residue field isomorphic to A. If A is perfect, the ring $W(A)$ is a DVR, and its maximal ideal is $pW(A)$.*

Proof. The homomorphism Φ_0 defines an isomomorphic of $W(A)/V_1(A)$ to A. The ideal $V_1(A)$ of $W(A)$ is therefore maximal. The ring $W(A)$ is separated and complete for the $V_1(A)$-topology (Proposition 17.1.14), so is local with maximal ideal $V_1(A)$ by Proposition 11.3.26.

Let $\boldsymbol{a}$ and $\boldsymbol{b}$ be two nonzero elements in $W(A)$. There exists integers $n, m \geq 0$ and elements $\tilde{\boldsymbol{a}} = (\tilde{a}_n)_{n\in\mathbb{N}}$ and $\tilde{\boldsymbol{b}} = (\tilde{b}_n)_{n\in\mathbb{N}}$ of $W(A)$ such that $\boldsymbol{a} = V^m(\tilde{\boldsymbol{a}})$, $\boldsymbol{b} = V^n(\tilde{\boldsymbol{b}})$ and the eleemnts $\tilde{a}_0$, $\tilde{b}_0$ are nonzero. Then the $m+n$-th component of $\boldsymbol{a} \times \boldsymbol{b}$ is equal to the 0-th component of $F^n(\tilde{\boldsymbol{a}}) \times F^m(\tilde{\boldsymbol{b}})$ (formula (1.4.3)), which is $\tilde{a}^{p^n}\tilde{b}^{p^m}$ (formula (1.4.1) and Example 17.1.5). Therefore $\boldsymbol{a} \times \boldsymbol{b}$ is nonzero and $W(A)$ is integral.

If the field A is perfect, the maximal ideal $V_1(a)$ of $W(A)$ is equal to $pW(A)$ by Proposition 17.1.15(b) and therefore $W(A)$ is a DVR by Proposition 14.2.16(c). □

17.2 Cohen rings

In this part, we fix a prime integer p.

17.2.1 p-rings

Let C be a ring. We say C is a ***p*-ring** if the ideal pC of C is maximal and if C is separated and complete for the pC-adic topology.

If $p1_C$ is nilpotent in C and the ideal pC is maximal, then C is a p-ring and the pC-adic topology is discrete. In particular, every field with characteristic p is a p-ring.

Proposition 17.2.1. *Let C be a p-ring.*

(a) The ring C is local with maximal ideal pC.

(b) Suppose that $p1_C$ is nilpotent and let d be the smallest positive integer such that $p^d 1_C = 0$. Then the ideals of C are of the form p^iC and $p^iC \neq p^jC$ if i, j are distinct integers such that $0 \leq i, j \leq d$. The C-module C has length d.

(c) Suppose that $p1_C$ is not nilpotent. Then C is a DVR whose residue field is of characteristic p, and the fraction field of characteristic 0. The ideals p^nC, where $n \in \mathbb{N}$, are distinct; they are the nonzero ideals of C. The C-module C has infinite length.

Proof. Assertion (a) follows from Proposition 11.3.26. By hypothesis we have $\bigcap_{n\geq 0} p^nC = \{0\}$. Let $x \neq 0$ be in C; there exists an integer $n \geq 0$ such that $x \in p^nC$, $x \notin p^{n+1}C$. Write $x = p^n y$ where $y \in C$, then $y \notin pC$, so it is invertible.

Suppose that $p1_C$ is not nilpotent. If x_1 and x_1 are two nonzero elements in C, there exist integers $n_1, n_2 \geq 0$ and invertible elements y_1, y_2 of C such that $x_1 = p^{n_1}y_1$, $x_2 = p^{n_2}y_2$. We

then have $x_1x_2 = p^{n_1+n_2}y_1y_2 \neq 0$, so C is integral. Since C is a local ring, not a field, and the maximal ideal $\mathfrak{m}_C = pC$ is principal, we conclude that C is a DVR (Proposition 14.2.16). The nonzero ideals of C are then of the form p^nC, and are all distinct. In particular, the ring C is not Artinian, so the C-module C has infinite length. The residue field C/pC of C clearly has characteristic p. Let q be the characteristic of the fraction field of C. We have $p1_C \neq 0$, so $q \neq p$. But if $q \neq 0$, we have $q1_C \neq 0$ and C/pC then has characteristic $q \neq p$, which is absurd. This proves (c).

Suppose that $p1_C$ is nilpotent and let d be the smallest positive integer such that $p^d1_C = 0$. We have a sequence of ideals

$$C \supseteq pC \supseteq \cdots \supseteq p^{d-1}C \supseteq p^dC = \{0\}. \tag{2.1.1}$$

If i is an integer such that $0 \leq i < d$ and $p^iC = p^{i+1}C$, then

$$p^{d-i-1}p^iC = p^{d-i-1}p^{i+1}C = p^dC = \{0\}$$

contradicting the hypothesis $p^{d-1}1_C \neq 0$. Therefore the ideals in the sequence above are all distinct. Let $\mathfrak{a}$ be an ideal of C and i the smallest integer such that $\mathfrak{a} \supseteq p^iC$. Let $x \neq 0$ be in $\mathfrak{a}$; we can write $x = p^mu$ where $m \geq 0$ and u is invertible. Then $p^m1_C \in \mathfrak{a}$, whence $p^mC \subseteq \mathfrak{a}$ and $m \geq i$. This shows $x \in p^iC$, so $\mathfrak{a} = p^iC$. We now conclude that (2.1.1) is a Jordan-Hölder sequence for the C-module C, so C has length d. □

Corollary 17.2.2. *If the p-ring C is integral, it is a DVR, or a field with characteristic p.*

Proof. Suppose that C is integral. If $p1_C$ is nilpotent, then $p1_C = 0$, and $\{0\}$ is a maximal ideal of C, whence C is a field with characteristic p. Otherwise, $p1_C$ is not nilpotent and C is a DVR by Proposition 17.2.1. □

Corollary 17.2.3. *Let C be a p-ring and $\mathfrak{a}$ a proper ideal of C. Then $C/\mathfrak{a}$ is a p-ring.*

Proof. We may suppose that $\mathfrak{a} \neq \{0\}$. Then there exists an integer $i \geq 1$ such that $\mathfrak{a} = p^iC$. The idela $pC/\mathfrak{a}$ of $C/\mathfrak{a}$ is maximal and we have $p^i1_{C/\mathfrak{a}} = 0$, so $C/\mathfrak{a}$ is a p-ring. □

Let C be a p-ring. The length of C, denoted by $l(C)$, is the supremum in $\overline{\mathbb{R}}$, of the set of integers $n \geq 1$ such that $p^{n-1}1_C \neq 0$. By Proposition 17.2.1, $l(C)$ is finite and equal to the length of the C-module C, or is $+\infty$, in which case the C-module C has infinite length.

Example 17.2.4 (Example of p-rings).

(a) For each integer $n \geq 1$, the ring $\mathbb{Z}/p^n\mathbb{Z}$ is a p-ring of length n. The ring $\mathbb{Z}_p$ of p-adic integers is a p-ring of length infinite.

(b) Let K be a perfect field of characteristic p. By Proposition 17.1.16, the Witt ring $W(K)$ is a p-ring of infinite length. The map $(a_n)_{n\in\mathbb{N}} \mapsto a_0$ induces by passing to quotient an isomorphism of $W(K)/pW(K)$ to the field K. For each integer $n \geq 1$, the ring

$$W_n(K) = W(K)/p^nW(K)$$

is a p-ring of length n. Note that $W(\mathbb{F}_p) = \mathbb{Z}_p$, so this generalize the example in (a).

Proposition 17.2.5. *Let C_1 and C_2 be p-rings and $\rho : C_1 \to C_2$ a ring homomorphism. Let $\bar{\rho}$ be the homomorphism of $\kappa_{C_1} = C_1/pC_1$ to $\kappa_{C_2} = C_2/pC_2$ induced by ρ on the residue field.*

(a) We have $l(C_1) \geq l(C_2)$, and ρ is injective if and only if $l(C_1) = l(C_2)$.

(b) For ρ to be surjective, it is necessary and sufficient that $\bar{\rho}$ being an isomorphism.

(c) For ρ to be an isomorphism, it is necessary and sufficient that $\bar{\rho}$ being an isomorphism and we have $l(C_1) = l(C_2)$.

Proof. Let $n \geq$ be an integer. We have $\rho(p^{n-1}1_{C_1}) = p^{n-1}1_{C_2}$, so the relation $p^{n-1}1_{C_2} \neq 0$ implies $p^{n-1}1_{C_1} \neq 0$ and they are equivalent if ρ is injective. We then have $l(C_2) \leq l(C_1)$ where the equality holds if ρ is injective. If ρ is not injective, there exists an integer $i < i(C_1)$ such that the kernel of ρ is the ideal p^iC_1 of C_1; we have $p^i1_{C_2} = 0$, so $l(C_2) \leq i$. This proves (a). Since κ_{C_1} and κ_{C_2} are fields, the homomorphism $\bar{\rho}$ is injective. If ρ is surjective, so is $\bar{\rho}$ and hence it is an isomorphism. Conversely, assume that $\bar{\rho}$ is surjective. Then for each integer $n \geq 0$, the map $\bar{\rho}_n : p^nC_1/p^{n+1}C_1 \to p^nC_2/p^{n+1}C_2$ induced by ρ is surjective. Since C is complete for the pC_1-adic topology, ρ is then surjective by Corollary 11.3.31. This proves (b). Finally, (a) and (b) imply (c). □

Proposition 17.2.6. *Let $(C_n, \pi_{n,m})$ be a inverse system of rings indexed by $\mathbb{N}$. Suppose that C_n is a p-ring for each $n \in \mathbb{N}$ and the homomorphism $\pi_{n,m}$ are surjective. Then $C = \varprojlim C_n$ is a p-ring, and for each $n \in \mathbb{N}$, the canonical homomorphism $\pi_n : C \to C_n$ is surjective and induces an isomorphism of κ_C to κ_{C_n}.*

Proof. Since the maps $\pi_{n,m}$ are surjective, π_n is surjective (Proposition 11.3.6). Let d_n be the length of C_n. By Proposition 17.2.5(a), the sequence d_n in $\mathbb{N} \cup \{+\infty\}$ is increasing; if it is stationary, there exists an integer n_0 such that $\pi_{n,m}$ is an isomorphism of C_m to C_n for $m \geq n \geq N_0$, hence C is isomorphic to C_{n_0}, a p-ring.

It then suffices to consider the case where d_n are all finite, and (d_n) tends to infinity. Let us endow the ring C with the trivial filtration. For each $n \in \mathbb{N}$, let I_n be the kernel of π_n, and put $I_n = C$ for $n < 0$. Endow C with the filtration $(I_n)_{n\in\mathbb{N}}$. It is then separated and complete, for the topology $\mathcal{T}$ defined bby the filtration is the inverse limit topology of the discrete topologis over C_n. Let $k \geq 1$ be an integer. We have $p^kC \subseteq \varprojlim_n (p^kC_n)$. Conversely, if $x = (x_n)_{n\in\mathbb{N}} \in \varprojlim_n (p^kC_n)$ and if we set $X_n = \{y \in C : \pi_n(p^ky) = x_n\}$, the sequence $(X_n)_{n\in\mathbb{N}}$ is a decreasing sequence of nonempty closed affine subsets of C. Since C/I_n is an Artinian C-module, the intersection of X_n is nonempty (**??**); for every $z \in \bigcap_{n\in\mathbb{N}} X_n$, we have $p^kz = x$. We have therefore proved that $p^kC = \varprojlim_n (p^kC_n)$ for each integer $k \geq 1$. In particular, the ideal p^kC of C is closed for the topology $\mathcal{T}$. For C, the p-adic topology is finer than the topology $\mathcal{T}$ since we have $p^{d_n}C \subseteq I_n$. It then follows from Proposition 3.2.19 that C is separated and complete for the pC-adic topology. In addition we have $pC = \varprojlim pC_n = \pi_0^{-1}(pC_0)$ and therefore the surjective homomorphism of C/pC to C_0/pC_0 induced by π_0 is an isomorphism. This shows that pC is maximal and therefore C is a p-ring. The final assertion follows from Proposition 17.2.5(b). □

Now let A be a separated and complete local ring, with residue field of characteristic p. A Cohen subring of A is defined to be a subring C of A that is a p-ring and such that $A = \mathfrak{m}_A + C$ (i.e., $A/\mathfrak{m}_A = C/(\mathfrak{m}_A \cap C)$). In this case, the ideal $\mathfrak{m}_A \cap C$ is maximal in C, hence equal to pC. The canonical map $\kappa_C = C/pC$ to $\kappa_A = A/\mathfrak{m}_A$ is then an isomorphism.

Example 17.2.7. Let C be a p-ring. The formal series ring $A = C[\![X_1, \dots, X_n]\!]$ is then Noetherian, local, separated and complete, with maximal ideal generated by $(p, T_1, \dots, T_n)$. It is immediate that C is a Cohen subring of A. This applies in particular if C is equal to $\mathbb{Z}_p$, to $\mathbb{Z}/p^n\mathbb{Z}$, or a field with characteristic p.

Theorem 17.2.8. *Let A be a seaprated and complete local ring, with residue field k of characteristic p. Let $\pi : A \to k$ be the canonical map, and S a subset of A such that π induces a bijection of S to a p-basis for k.*

(a) There exists a unique Cohen subring C of A containing S.

(b) The subring C is closed in A, and the pC-adic topology of C is induced by the $\mathfrak{m}_A$-adic topology of A.

(c) Every closed subring B of A, containing S, and such that $A = B + \mathfrak{m}_A$, contains C.

Proof. We divide the proof into several parts. First, we assume that $\mathfrak{m}_A$ is nilpotent. Let n be a positive integer such that $\mathfrak{m}_A^{n+1} = \{0\}$. If Φ_n is the n-th Witt polynomial, the map $\rho : [a_0, \dots, a_n] \mapsto \Phi_n(a_0, \dots, a_n)$ is a homomorphism from $W_{n+1}(A)$ to A. Let B_n be the image of ρ_n and C_n the subring of A generated by $B_n \cup S$. We note that $pA \subseteq \mathfrak{m}_A$ and B_n consists of elements of the form $a_0^{p^n} + pa_1^{p^{n-1}} + \cdots + p^n a_n$, where $a_0, \dots, a_n \in A$. Concequently, we have $\pi(B_n) = k^{p^n}$, and $\pi(C_n) = k^{p^n}[\pi(S)]$. Since $\pi(S)$ is a p-basis for k, we have $k = k^{p^n}[\pi(S)]$ (**??**), whence $\pi(C_n) = k$, and $C_n + \mathfrak{m}_A = A$.

Let B be a subring of A containing S. We claim that, for B to contain C_n, it is necessary and sufficient that $A = B + \mathfrak{m}_A$. First, if B contains C_n, then

$$B + \mathfrak{m}_A \supseteq C_n + \mathfrak{m}_A = A$$

so $B + \mathfrak{m}_A = A$. Conversely, suppose that $B + \mathfrak{m}_A = A$. Let $a_0, \dots, a_n$ be elements of A; there exists by hypothesis elements $b_0, \dots, b_0$ of B such that $a_i \equiv b_i \bmod \mathfrak{m}_A$ for each i. By Proposition 17.1.2 and the hypothesis $\mathfrak{m}_A^{n+1} = 0$, we then have $\Phi_n(a_0, \dots, a_n) = \Phi_n(b_0, \dots, b_n) \in B$, whence $B_n \subseteq B$. Since C_n is the ring generated by $B_n \cup S$, we have $C_n \subseteq B$.

Let $\mathcal{S}$ be the set of subrings B of A containing S and such that $B + \mathfrak{m}_A = A$. There exists by the above claim a smallest element C in $\mathcal{S}$ (take the smallest integer n such that $\mathfrak{m}_A^{n+1} = \{0\}$, then C_n is the desired subring), and we have $C_n = C$ for any integer $n \geq 0$ such that $\mathfrak{m}_A^{n+1} = \{0\}$. We have $C + \mathfrak{m}_A = A$ by construction and $p1_C$ is nilpotent; clearly $pC \subseteq C \cap \mathfrak{m}_A$. We now prove that $C \cap \mathfrak{m}_A \subseteq pC$. Choose an integer $n \geq 1$ such that $\mathfrak{m}_A^n = \{0\}$, so $C = C_n = C_{n-1}$. Let Λ be the subset of $\mathbb{N}^{\oplus S}$ formed by elements $(\alpha_s)_{s \in S}$ with finite support such that $0 \leq \alpha_s < p^n$ for each $s \in S$. Since B_n contains $s^{p^n} = \Phi_n(s, 0, \dots, 0)$ for each $s \in S$, the monomials $z_\alpha = \prod_{s \in S} s^{\alpha_s}$, for $\alpha \in \Lambda$, generate the C_n as a B_n-module. Moreover, by the formula

$$\Phi_n(a_0, \dots, a_n) = a_0^{p^n} + p\Phi_{n-1}(a_1, \dots, a_n),$$

any element of B_n is of the form $a^{p^n} + pb$ where $a \in A$ and $b \in B_{n-1}$. Therefore any element of $C = C_n$ is of the form

$$x = \sum_{\alpha \in \Lambda} c_\alpha^{p^n} z_\alpha + py \tag{2.1.2}$$

where $c_\alpha \in A$ for $\alpha \in \Lambda$, and $y \in C_{n-1} = C$. If x is in $C \cap \mathfrak{m}_A$, we have $\pi(x) = 0$ whence $\sum_{\alpha\in\Lambda} \pi(c_\alpha)^{p^n}\pi(z_\alpha) = 0$. Since $\pi(S)$ is a p-basis for k, $\pi(c_\alpha) = 0$ for all $\alpha \in \Lambda$ (**??**). We then have $c_\alpha \in \mathfrak{m}_A$, whence $c_\alpha^n = 0$ and a fortiori $c_\alpha^{p^n} = 0$. By (2.1.2), we then get $x = py$, whence $C \cap \mathfrak{m}_A \subseteq pC$. With this, it is now clear that C is a Cohen subring of A. We have $p^n C = \mathfrak{m}_A^n = \{0\}$ for n large enough and assertion (b) is then trivial. Assertion (c) follows from the construction of C.

We now turn to the general case. For each integer $n \geq 0$, let A_n be the local ring $A/\mathfrak{m}_A^{n+1}$, $\mathfrak{m}_n = \mathfrak{m}_A/\mathfrak{m}_A n + 1$, and $\pi_n : A \to A_n$ the canonical homomorphism. By the previous case, there exists a unique Cohen subring C_n in A_n containing $\pi_n(S)$. For $0 \leq n \leq m$, we denote by $\pi_{n,m}$ the canonical map from A_m to A_n. By Corollary 17.2.3, $\pi_{n,m}(C_m)$ is a p-ring; we have $\pi_{n,m}(C_m) + \mathfrak{m}_n = A_n$, so $\pi_{n,m}(C_m)$ is equal to the Cohen subring C_n of A_n. By Proposition 17.2.6, the subring $\varprojlim C_n$ of $\varprojlim A_n$ is a p-ring. Put $C = \bigcap_{n\in\mathbb{N}} \pi_n^{-1}(C_n)$. Then C is the preimage of $\varprojlim C_n$ under the isomorphism $a \mapsto (\pi_n(a))_{n\in\mathbb{N}}$ of A to $\varprojlim A_n$, whence a closed subring of A, and a p-ring. We have $\pi_n(C) = C_n$ for each $n \in \mathbb{N}$ (Proposition 17.2.6) and in particular $\pi_0(C) = A_0$, which means $\pi(C) = k$. Therefore C is a Cohen subring of A.

For each integer $n \geq 0$, let $J_n = C \cap \mathfrak{m}_A^n$. Since the local ring A is separated, we have $\bigcap_{n\in\mathbb{N}} J_n = \{0\}$, and by the structure of ideals of p-rings, every ideal of C is of the form $p^i C$ and contains some J_n. Conversely, J_n contains $p^n C$. Therefore the pC-adic topology is induced by the $\mathfrak{m}_A$-topology on A. This proves (b). Now let B be a closed subring of A containing S and such that $B + \mathfrak{m}_A = A$. Since B is closed, we have $B = \bigcap_{n\in\mathbb{N}} \pi_n^{-1}(\pi_n(B))$. We have $\pi_n(B) \supset \pi_n(S)$ and $\pi_n(B) + \mathfrak{m}_n = A_n$, whence $\pi_n(B) \supseteq C_n$ and therefore $B \supseteq C$. This proves (c) and completes the proof. □

Remark 17.2.1. Suppose that $p1_A$ is not nilpotent (in particular if A is an integral domain with fraction field of characteristic 0). Then C is a DVR with fraction field of characteristic 0.

17.2.2 Existence and uniqueness of p-rings

Proposition 17.2.9. *Let C_1 and C_2 be p-rings such that $l(C) \geq l(C_2)$, π_1 (resp. π_2) the canonical homomorphism of C_1 (resp. C_2) to κ_{C_1} (resp. κ_{C_2}). Let $(x_\lambda)_{\lambda\in\Lambda}$ (resp. $(y_\lambda)_{\lambda\in\Lambda}$) be a family of elements of C_1 (resp. C_2) whose image under π_1 (resp. π_2) is a p-basis of κ_{C_1} (resp. κ_{C_2}). Let η be an isomorphism of κ_{C_1} to κ_{C_2} such that $\eta(\pi_1(x_\lambda)) = \pi_2(y_\lambda)$ for every $\lambda \in \Lambda$. There then exists a unique homomorphism $\rho : C_1 \to C_2$ such that $\eta \circ \pi_1 = \pi_2 \circ \rho$ and $\rho(x_\lambda) = y_\lambda$ for every $\lambda \in \Lambda$. It is surjective, and an isomorphism if $l(C_1) = l(C_2)$.*

Proof. Let A be the subring of $C_1 \times C_2$ formed by pairs (x, y) such that $\eta(\pi_1(x)) = \pi_2(y)$. The map $(x, y) \mapsto \pi_1(x)$ is a surjective homomorphism of A to κ_C. Its kernel $\mathfrak{m}$, equal to $pC_1 \times pC_2$, is then a maximal ideal of A. The subspace A of $C_1 \times C_2$ is closed, hence complete, and the topology induced on A from $C_1 \times C_2$ is the $\mathfrak{m}$-adic topology. Thus A is a separated and complete local ring with maximal ideal $\mathfrak{m}$. For each $\lambda \in \Lambda$, we have $(x_\lambda, y_\lambda) \in A$ by hypothesis; if ξ_λ is the calss of (x_λ, y_λ) modulo $\mathfrak{m}$, the family $(\xi_\lambda)_{\lambda\in\Lambda}$ is a p-basis of $A/\mathfrak{m}$. By Theorem 17.2.8, there exists a unique Cohen subring $\tilde{C}$ of A containing (x_λ, y_λ) for each $\lambda \in \Lambda$. By definition, we have $l(\tilde{C}) = l(C_1) \geq l(C_2)$. The restriction to $\tilde{C}$ of the projection of $C_1 \times C_2$ to C_1 is a homomorphism $h_1 : \tilde{C} \to C_1$ which induces an isomorphism of $\kappa_{\tilde{C}}$ to κ_{C_1}. By Proposition 17.2.5(c), h_1 is an isomorphism of $\tilde{C}$ to C_1. We also see that the restriction h_2 to $\tilde{C}$ of the projection from $C_1 \times C_2$ to C_2 is a surjective homomorphism. Therefore, $\tilde{C}$ is the graph of a surjective homomorphism

$\rho = h_2 \circ h_1^{-1}$ of C_1 to C_2, and we have $\eta \circ \pi_1 = \pi_2 \circ \rho$, $\rho(x_\lambda) = y_\lambda$ for $\lambda \in \Lambda$. Moreover, if $l(C_1) = l(C_2)$, ρ is an isomorphism.

Let ρ_1 be a homomorphism of C_1 to C_2 such that $\eta \circ \pi_1 = \pi_2 \circ \rho$, $\rho(x_\lambda) = y_\lambda$ for $\lambda \in \Lambda$, and let $\tilde{C}'$ be the graph of ρ_1. It is immediate that $\tilde{C}'$ is a Cohen subring of A, containing (x_λ, y_λ) for $\lambda \in \Lambda$, whence $\tilde{C}' = \tilde{C}$ and $\rho_1 = \rho$. □

Proposition 17.2.10. *Let k be a field of characteristic p, and let $n \geq 1$ an integer, or $+\infty$. Then there exists a p-ring of length n with residue field isomorphic to k.*

Proof. The ring $W(k)$ of Witt vectors with coefficients in k is an integral seaprated and complete local ring, with residue field isomorphic to k (Proposition 17.1.16), and we have $p \cdot 1_{W(k)} \neq 0$. Let C be a Cohen subring of $W(k)$ (Theorem 17.2.8). Then C is a p-ring of length $+\infty$ with residue field isomorphic to k, and, if $n \geq 1$ is an integer, the quotient C/p^nC is a p-ring of length n with residue field isomomorphic to k. □

Remark 17.2.2. Let $n \geq 1$ be an integer and S a p-basis of k. We can show that the subring $W_n(k)$ generated by $W_n(k^{p^n})$ and the elements $[\xi, 0, \ldots, 0]$ (where $\xi \in S$), is a p-ring of length n with residue field isomorphic to k.

Corollary 17.2.11. *Let C be a p-ring of finite length n. Then there exists a p-ring $\tilde{C}$ of infinite length such that C is isomomorphic to $\tilde{C}/p^n\tilde{C}$.*

Proof. By Proposition 17.2.10, there exists a p-ring $\tilde{C}$ of infinite length such that $\kappa_{\tilde{C}}$ is isomorphic to κ_C. Then $\tilde{C}/p^n\tilde{C} = \tilde{C}_n$ is a p-ring of length n, and $\kappa_{\tilde{C}_n}$ is isomomorphic to $\kappa_{\tilde{C}}$, hence to κ_C. By Proposition 17.2.9, the ring C and $\tilde{C}_n$ is isomorphic. □

Proposition 17.2.12. *Let C be a p-ring, with residue field k prefect. Suppose that C has finite length n (resp. infinite length). There exists a unique isomorphism $\rho_C : W_n(k) \to C$ (resp. $\rho_C : W(k) \to C$) which induces by passing to quotient the identity map on k.*

Proof. Since $W_n(k)$ (resp. $W(k)$) is a p-ring with residue field k and length n (infinite), and $\varnothing$ is a p-basis for k, Proposition 17.2.9 then implies the claim. □

17.2.3 Multiplicative representatives

Theorem 17.2.13. *Let A be a separated and complete local ring, k the residue field, and $\pi : A \to k$ the canonical map. Suppose that k is perfect with characteristic p.*

(a) There exists a unique homomorphism $\rho : W(k) \to A$ such that $\pi(\rho(\boldsymbol{a})) = a_0$ for each $\boldsymbol{a} = (a_n)_{n\in\mathbb{N}}$ in $W(k)$.

(b) The homomorphism ρ is continuous if we endow $W(k)$ with the $pW(k)$-adic topology, and its image is the unique Cohen subring of A.

Proof. By Theorem 17.2.8, there exists a unique Cohen subring C of A. Let $\rho : W(k) \to A$ be a ring homomorphism such that $\pi(\rho(\boldsymbol{a})) = a_0$ for $\boldsymbol{a} = (a_n)_{n\in\mathbb{N}}$ in $W(k)$; is is immediate that the image of ρ is a Cohen subring of A, hence equal to C. The existence and uniqueness of ρ then follows from Proposition 17.2.12. The pC-adic topology on C is induced by the $\mathfrak{m}_A$-adic topology (Theorem 17.2.8(b)), so ρ is continuous. □

Proposition 17.2.14. *Retain the hypothesis and notations in Therorem 17.2.13. There exist a multiplicative subset S of A such that π induces a bijection of S to k. For an element $a \in A$ to belong to S, it is necessary and sufficient that for each $n \in \mathbb{N}$, there exists an element a_n in A such that $a = a_n^{p^n}$. The set S consists of elements of the form $\rho(x, 0, 0, \dots,)$.*

Proof. Let S be a multiplicative subset of A such that π induces a bijection of S to k. Let T be the set of elements of A which are p^n-th powers for every $n \in \mathbb{N}$. Let $a \in S$ and $n \in \mathbb{N}$; since k is perfect, there exists x_n in k such that $x_n^{p^n} = \pi(\boldsymbol{a})$. But $\pi(S) = k$, so there exists $a_n \in S$ such that $x_n = \pi(a_n)$. Then we have $\pi(a_n^{p^n}) = \pi(a)$ whence $a_n^{p^n} = a$ since π is injective on S. This shows $S \subseteq T$. Conversely, we show that the restriction of π on T is injective, which then proves that $S = T$: let a and b be elements of T such that $\pi(a) = \pi(b)$. Let $n \in \mathbb{N}$; there exists two elements a_n and b_n of A such that $a = a_n^{p^n}$, $b = b_n^{p^n}$. Then $\pi(a_n)^{p^n} = \pi(b_n)^{p^n}$, hence $\pi(a_n) = \pi(b_n)$. This means $a_n \equiv b_n \bmod \mathfrak{m}_A$, so $a_n^{p^n} \equiv b_n^{p^n} \bmod \mathfrak{m}_A^{n+1}$ (Lemma 17.1.1). But then $a \equiv b \bmod \mathfrak{m}_A^{n+1}$. Since n is arbitrary and A is separated, we conclude that $a = b$.

In the notations of Therorem 17.2.13, let $\varphi = \rho \circ \tau_k$, which means

$$\varphi(x) = \rho(x, 0, 0, \dots)$$

for $x \in k$. Since τ_k is multiplicative (Proposition 17.1.10), so is φ and it is clear that $\pi \circ \varphi$ is the identity map on k. The image of φ then satisfies the requirements. □

The elements of S are often called the **multiplicative (or Teichmüller) representatives** of A. Recall that by Proposition 17.1.15, we have

$$\boldsymbol{a} = \sum_{n=0}^{\infty} p^n \tau_k(a_n^{p^{-n}})$$

for $\boldsymbol{a} = (a_n)_{n \in \mathbb{N}}$ in $W(k)$. Therefore

$$\rho(\boldsymbol{a}) = \sum_{n=0}^{\infty} p^n \varphi(a_n^{p^{-n}})$$

because ρ is continuous. By this formula, the unique Cohen subring of A consists of elements of the form $\sum_{n=0}^{\infty} p^n s_n$ where $s_n \in S$ for each $n \in \mathbb{N}$.

Example 17.2.15 (Example of multiplicative representatives).

(a) Let k be a perfect field of characteristic p. The multiplicative representatives of the ring $W(k)$ is the Witt vectors $\tau(x) = (x, 0, 0, \dots)$ for $x \in k$.

(b) Let A be an integral separated and complete local ring. We suppose that the residue field k of A is finite, with $q = p^f$ elements, hence perfect with characteristic p. We have $x^q = x$ for each $x \in k$, hence $s^q = s$ for each multiplicative representative. It follows that the set of multiplicative representatives consists of 0 and the $q-1$-th roots of the unity in the field of fractions of A. If the field of fractions of A is locally compact, the existence of the multiplicative representatives follows also from **??**.

In particular, consider the case $A = \mathbb{Z}_p$. Then the multiplicative representatives are 0 and the $(p-1)$-th roots of unity in the field Q_p.

17.2.4 Structure of Noetherian complete local rings

We now use the results in this part to give a structural theorem for Noetherian complete local rings (such rings are separated by Corollary 11.4.16). Let A and C be Noetherian complete local rings and $\rho : C \to A$ a ring homomorphism which induces an isomorphism residue fields. Let $(p_1, \dots, p_m)$ be a sequence generating the maximal ideal $\mathfrak{m}_C$ of C, and let $(t_1, \dots, t_n)$ be a sequence of elements of A. Let S denote the sequence $(\rho(p_1), \dots, \rho(p_m), t_1, \dots, t_n)$.

Lemma 17.2.16. *Let $B = C[\![T_1, \dots, T_n]\!]$ and $\eta : B \to A$ be the unique homomorphism extending ρ that sends T_i to t_i for each i.*

(a) For η to be surjective, it is necessary and suffcient that S generates the ideal $\mathfrak{m}_A$ of A, or its class modulo $\mathfrak{m}_A^2$ generates $\mathfrak{m}_A/\mathfrak{m}_A^2$ as a vector space over κ_A.

(b) For η to make A a finite B-algebra, it is necessary and sufficient that S generates a defining ideal of the $\mathfrak{m}_A$-adic topology on A.

Proof. Let $\mathfrak{n}$ be the ideal of B generated by $T_1, \dots, T_n$. Any homomorphism η of B to A extending ρ and such that $\eta(T_i) = t_i$ maps $\mathfrak{n}$ to $\mathfrak{m}_A$, hence is continuous when B is endowed with the $\mathfrak{n}$-adic topology. The existence and uniqueness of η then follows from **??**.

The ring $B = C[\![T_1, \dots, T_n]\!]$ is a Noetherian complete local ring, and $\mathfrak{m}_B$ is generated by $p_1, \dots, p_m, T_1, \dots, T_n$. We then have $\eta(\mathfrak{m}_B) \subseteq \mathfrak{m}_A$ and η is defines a homomorphism $\mathrm{gr}(\eta) : \mathrm{gr}(B) \to \mathrm{gr}(A)$. But the ring $\mathrm{gr}(A)$ is generated by $A/\mathfrak{m}_A = \kappa_A$ and $\mathfrak{m}_A/\mathfrak{m}_A$, $\mathrm{gr}(\eta)$ induces an isomorphism of $\kappa_B = \kappa_C$ to κ_A, and the classes modulo $\mathfrak{m}_B^2$ of the elements $p_1, \dots, p_m, T_1, \dots, T_n$ generate $\mathfrak{m}_B/\mathfrak{m}_B^2$ as a κ_B-vector space; moreover η is surjective if and only if $\mathrm{gr}(\eta)$ is surjective (Corollary 11.3.31). These prove (a).

The ideal $\mathfrak{a}$ of A generated by S is equal to $\eta(\mathfrak{m}_B)A$. Since $\mathfrak{m}_A$ contains $\eta(\mathfrak{m}_B)$, A is a Zariski ring for the $\mathfrak{a}$-adic topology. The ring $A/\mathfrak{a}$ is Artinian if and only if its length as an A-module is finite. But as any simple module of A is killed by $\mathfrak{m}_A$ and, by hypothesis, $A/\mathfrak{m}_A$ and $B/\mathfrak{m}_B$ are isomorphic, this happens exactly when the dimension of the vector space $A/\mathfrak{a}$ over $B/\mathfrak{m}_B$ is finite. By Corollary 12.2.21, we see $\mathfrak{a}$ is a defining ideal of A if and only if the dimension of $A/\mathfrak{a}$ over $B/\mathfrak{m}_B$ is finite. This is indeed the case if A is a finite B-algebra. Conversely, suppose then $\mathfrak{a}$ is a defining ideal of A. The $\mathfrak{m}_B$-adic topology on the B-module A then coincides with the $\mathfrak{m}_A$-adic topology on A, hence is separated. Since $A/\mathfrak{a}$ is a finitely generated $B/\mathfrak{m}_B$-module, A is a finitely generated B-module (Corollary 11.3.34). This proves (c). □

Lemma 17.2.17. *Suppose that C is regular and $(p_1, \dots, p_m)$ is a system of parameters for C.*

(a) If the sequence S is secant for A, the homomorphism $\eta : B \to A$ is injective.

(b) For η to be inejctive and make A a finite B-algebra, it is necessary and sufficient that S is a maximal secant sequence for A. In this case A has dimension $m + n$.

Proof. For the sequence S to be maximal secant for A, it is necessary and sufficient that it generates a defining ideal of A, and in that case A has dimension $m + n$ (Theorem 16.3.12 and Proposition 16.3.14). By Lemma 17.2.16(b), this is equivalent to that A is a finite B-algebra, and has dimension $m + n$. Now C is a Noetherian integral domain with dimension m, so $B = C[\![T_1, \dots, T_n]\!]$ is a Noetherian integral domain with dimension $m + n$. If A is a finite B-algebra, let $\mathfrak{a}$ be the kernel of η, then $\dim(A) = \dim(B/\mathfrak{a})$. Since B is a Noetherian integral

domain with finite dimension, we have $\dim(B/\mathfrak{a}) < \dim(B)$ if $\mathfrak{a} \neq \{0\}$. Thus, if A is a finite B algebra, η is injective if and only if A has dimension $m+n$. This proves (b).

Suppose that S is secant for A. We may add elements $t_{n+1}, \dots, t_{n+r}$ of $\mathfrak{m}_A$ to form a maximal secant sequence. By the argument above, there exists an injective homomorphism $\tilde{\eta}$ from $C[\![T_1, \dots, T_n, T_{n+1}, \dots, T_{n+r}]\!] = B[\![T_{n+1}, \dots, T_{n+r}]\!]$ which extends η and sends T_{n+j} to t_{n+j} for $1 \leq j \leq r$. Hence η is injective. This proves (a). □

Theorem 17.2.18 (Cohen Structure Theorem). *Let A be a Noetherian complete local ring with residue field k of characteristic p. Let C be a p-ring of infinite length, whose residue field is isomorphic to k.*

(a) If n is the dimension of $\mathfrak{m}_A/(\mathfrak{m}_A^2 + pA)$ over k, there exists an ideal $\mathfrak{a}$ of $C[\![T_1, \dots, T_n]\!]$ such that A is isomorphic to $C[\![T_1, \dots, T_n]\!]/\mathfrak{a}$.

(b) Let d be the dimension of A. Suppose that $p1_A$ is not a divisor of zero in A. Then there exists a subring B of A isomorphic to $C[\![T_1, \dots, T_{d-1}]\!]$ such that A is a finite B-algebra.

Proof. Let $\tilde{C}$ be a Cohen subring of A. Since C has infnite length, there exists a homomorphism of C to $\tilde{C}$. Concequently, there exists a local homomorphism $\rho : C \to A$. Choose elements $t_1, \dots, t_n$ of $\mathfrak{m}_A$ whose classes form a basis for $\mathfrak{m}_A/(\mathfrak{m}_A^2 + pA)$ over k. We have $\rho(p1_C) = p1_A$, and Lemma 17.2.16(b) proves the existence of a surjective homomorphism of $C[\![T_1, \dots, T_m]\!]$ to A, which sends T_i to t_i for each i. This proves (a).

Suppose now that $p1_A$ is not a divisor of zero in A, hence secant for A. There exists by Proposition 16.5.9 elements $t_1, \dots, t_{d-1}$ of $\mathfrak{m}_A$ such that $(p1_A, t_1, \dots, t_{d-1})$ is a maximal secant sequence for A. The Noetherian local ring C is regular (it is a DVR), and $p1_C$ is a system of parameters of C. Assertion (b) now follows from Lemma 17.2.17(b). □

17.2.5 Coefficient fields

Let A be a ring. Recall that the characteristic of A is defined if A contains a subfield. It is equal to 0 if and only if A contains a subfield isomorphic to $\mathbb{Q}$, and equal to a prime number p if and only if $p1_A = 0$. If the characteristic of A is defined and $\rho : A \to B$ is a nonzero ring homomorphism, then the characteristic of B is defined and equal to A.

Now let A be a local ring with maximal ideal $\mathfrak{m}$ and residue field k. We distinguish two cases.

(a) Suppose that k has characteristic 0. Then A contains a field and the characteristic of A is 0. In fact, the canonical homomorphism of $\mathbb{Z}$ to A is injective since the canonical map of $\mathbb{Z}$ to k factors through it, and for any nonzero integer n, $n1_A$ is invertible in A since it is not contained in the maximal ideal $\mathfrak{m}$.

(b) Suppose that k has characteristic $p \neq 0$. Then A contains a field if and only if $p1_A = 0$ (since such a field must have characteristic p), and in this case A has characteristic p.

Now assume that A is an integral domain with fraction field K. We now the field K also has a characteristic, which is equal to that of A (if the characteristic of A is defined). Then A contains a subfield if and only if the characteristic of K and k are equal. In this case, we say A is a local ring with **equal characteristic**. We also note that, if the characteristic of k and K are unequal,

then k must have characteristic $p \neq 0$ with K characteristic 0. In this case we say A is a local ring with **unequal characteristic**.

Proposition 17.2.19. *Let k_0 be a field, A a k_0-algebra and a separated and complete local ring, k a sub-k_0-extension of κ_A which has a separable transcendental basis $(\xi)_{\lambda\in\Lambda}$ over k_0. For any $\lambda \in \Lambda$, let x_λ be a representative of ξ_λ in A. Then there exists a unique subfield K of A, containing k_0 and the elements x_λ, such that the canonical homomorphism $\pi : A \to \kappa_A$ induces an isomorphism of K to k.*

Proof. Let φ be the k_0-homomorphism of the polynomial ring $k_0[(X_\lambda)_{\lambda\in\Lambda}]$ to A which sends X_λ to x_λ for each λ. Let u be a nonzero element in $k_0[(X_\lambda)_{\lambda\in\Lambda}]$; we have $\pi(\varphi(u)) \neq 0$ since the family $(\xi)_\lambda$ is algebraically independent over k_0 in κ_A, so $\varphi(u)$ is invertible in A. It follows that φ extens to a homomorphism ψ of the field $k_1 = k_0((X_\lambda)_{\lambda\in\Lambda})$ to A. Then A is a k_1- algebra, κ_A is an extension of k_1 and k a subextension of κ_A which is algebraic and separable over k_1. It suffices to prove that there exists a unique subfield K of A containing $\psi(k_1)$ and such that $\pi(K) = k$.

Let $\mathcal{S}$ be the set of subfield K of A, containing $\psi(k_1)$ and such that $\pi(K) \subseteq k$; this is inductive with respect to the inclusion relation. Let K be a maximal element in $\mathcal{S}$; we consider k as an extension (algebraic and separable) of K. Let $\xi \in k$ and $P \in K[X]$ its minimal polynomial over k. Since ξ is a simple root of P, the Hensel lemma (Corollary 11.5.17) then shows the existence of an element $x \in A$ such that $\pi(x) = \xi$ and $P(x) = 0$. The subfield $K(x)$ of A then belongs to $\mathcal{S}$, so $x \in K$ by the maximality of K. This shows $\xi \in \pi(K)$, so $\pi(K) = k$.

We now show the uniqueness of K. Let K and K' be subfields of A containing $\psi(k_1)$ and such that $\pi(K) = \pi(K') = k$. Let $\xi \in k$, and let $x \in K$, $x' \in K'$ be elements such that $\pi(x) = \pi(x') = \xi$. If $P \in k_1[X]$ is the minimal polynomial of ξ over k_1, then ξ is a simple root of P, and we have $P(x) = P(x') = 0$. By Hensel lemma we then have $x = x'$, so $K = K'$. □

Remark 17.2.3. The previous proof applies more generally to the case where we only assume that A is a Henselian local ring. The uniqueness proof uses the assumption that the local ring A is separate, but not that it is complete.

Let A be a local ring. A **representative field** of A is defined to be a subfield K of A such that the canonical homomorphism of A to κ_A induces an isomorphism of K to κ_A (in other words, $A = K + \mathfrak{m}_A$). It is clear that such a field exists only when the characteristic of A is defined. This condition is also sufficient when A is separated and complete. More precisely, we have the following theorem:

Theorem 17.2.20. *Let A be a seperated and complete local ring of equal characteristic p.*

(a) Suppose $p = 0$ and let $(x_\lambda)_{\lambda\in\Lambda}$ be a family of elements of A whose class modulo $\mathfrak{m}_A$ forms a transcendental basis for κ_A over $\mathbb{Q}$. Then there exists a unique representative field of A containing the elements x_λ.

(b) Suppose $p \neq 0$ and let $(x_\lambda)_{\lambda\in\Lambda}$ be a family of elements of A whose class modulo $\mathfrak{m}_A$ forms a p-basis for κ_A. Then there exists a unique representative field of A containing the elements x_λ, which is a Cohen subring of A.

Proof. Suppose that $p = 0$, so A is a $\mathbb{Q}$-algebra. Since any transcendental basis for κ_A over $\mathbb{Q}$ is separable, the assertion in (a) follows from Proposition 17.2.19 applied to $k_0 = \mathbb{Q}$, $k = \kappa_A$.

Now suppose that $p \neq 0$. Then we have $p1_A = 0$, and any Cohen subring C of A satisfies $pC = 0$. Therefore, the notations of representative field and Cohen subring coincide on A. Assertion (b) therefore follows from Theorem 17.2.8. □

Corollary 17.2.21. *Let A be a separated and complete local ring, whose residue field is an algebraic extension of $\mathbb{Q}$. Then there exists a unique representative field of A.*

Proof. In fact, the ring A is of characteristic 0, and the empty set is a transcendental basis for κ_A over $\mathbb{Q}$. □

Corollary 17.2.22. *Let A be a separated and complete local ring, with residue field of characteristic $p \neq 0$. Suppose that the residue field κ_A is perfect. Then there exists a unique representative field of A, which coincide with the multiplicative representatives.*

Proof. This follows from Theorem 17.2.20(b) and Proposition 17.2.14. □

Theorem 17.2.23. *Let A be a Noetherian complete local ring with dimension d. Let K be a representative field of A, and m the dimension of $\mathfrak{m}_A/\mathfrak{m}_A^2$ over K.*

(a) There exists an ideal $\mathfrak{a}$ of $K[\![T_1, \dots, T_m]\!]$ such that A is isomorphic to $K[\![T_1, \dots, T_m]\!]/\mathfrak{a}$.

(b) There exists a sub-K-algebra B of A, isomorphic to $K[\![T_1, \dots, T_d]\!]$, such that A is a finite B-algebra.

(c) If A is regular then there exists an isomorphism of A to $K[\![T_1, \dots, T_d]\!]$.

Proof. Let $t_1, \dots, t_m$ be elements of $\mathfrak{m}_A$ whose classes in $\mathfrak{m}_A$ form a basis for $\mathfrak{m}_A/\mathfrak{m}_A^2$. By Lemma 17.2.16, there exists a surjective K-homomorphism of $K[\![T_1, \dots, T_m]\!]$ to A, sending T_i to t_i. This proves (a). Similarly, (b) follows from Lemma 17.2.17, and the existence of a maximal secant sequence for A. Finally, assertion (c) follows from Corollary 16.5.8. □

17.3 Integral closure of complete local rings

17.3.1 Japanese rings

Let A be a Noetherian integral domain. It is called an **N-1 ring** if the integral closure of A in its fraction field K is a finite A-algebra. It is called an **N-2 ring** (or **Japanese**) if the integral closure of A in any finite extension of K is a finite A-algebra. In other words, A is Japanese if it satisfies the following condition: any integral A-algebra B integral over A, contained in a finite type extension of the field of fractions K of A, is a finite A-algebra. Indeed, the field of fractions L of B is an algebraic extension of K, so is of finite degree over K. The A-algebra B is contained in the integral closure of A in L, and is therefore finite if the latter is finite.

We note that Japanese rings are stable under localization. That is, if A is a Noetherian integral Japanese ring and S a multiplicative subset of A non containing 0, then the fraction ring $S^{-1}A$ is Japanese. This follows from the observation that the integral closure of $S^{-1}A$ is the localization of that of A, and hence is finite over A if A is Japanese.

Example 17.3.1. We recall that, by Theorem 13.3.5, any integral k-algebra of finite type, where k is a field, is a Japanese ring. Note that this is true for the coordinate ring of an algebraic variety.

Proposition 17.3.2. *Let A be a Noetherian integral domain, with fraction field K. Suppose that for any finite purely inseparable extension L of K, the integral closure of A in L is a finite A-algebra. Then A is Japanese.*

Proof. Let E be a finite extension of K. Let N be the normal closure of E over K and L the invariant field of $\mathrm{Aut}_K(N)$. Then L is the purely inseparable closure of K in N and the extension L/N is separable (Proposition 9.1.89). The integral closure B of A in L is then by hypothesis a finite A-algebra; the integral closure C of B in E is a finite B-algebra by Corollary 13.1.50, which contains the integral closure of A in E. Since A is Noetherian, this completes the proof. □

Corollary 17.3.3. *Suppose that K is perfect (for example of characteristic 0). Then A is Japanese if and only if it is integrally closed.*

Proposition 17.3.4. *Let B be a Noetherian integral domain and A a Noetherian subring of B, such that B is a finite A-algebra. For A to be Japanese, it is necessary and sufficient that B is Japanese.*

Proof. Let K (resp. L) be the fraction field of A (resp. B). Suppose that A is Japanese, and let E be a finite extension of L. Let C be the integral closure of B in E. By Proposition 13.1.6, C is also the integral closure of A in E, hence is a finite A-algebra (since E is a finite extension of K and A is Japanese). A fortiori, C is a finite B-algebra, this proves B is Japanese.

Conversely, suppose that B is Japanese and let N be a finite extension of K. Let D be the integral closure of A in N. Let E be the composed extension of L and N (over K); since B is Japanese, the integral closure D' of B in E is a finite B-algebra, hence a finite A-algebra; the A-module D is a sub-module of D', so is finite over A. This shows A is Japanese. □

Theorem 17.3.5 (Tate). *Let A be an integrally closed Noetherian ring, a an element of A. Suppose that the ideal aA is prime, the ring A/aA is Japanese and A is complete for the aA-adic topology. Then the ring A is Japanese.*

Proof. Let K be the fraction field of A. The assertion is trivial if K has characteristic 0. We may therefore assume that K has characteristic $p > 0$. Also, suppose that $a \neq 0$. Let L be a finite purely inseparable extension of K and $q = p^e$ a power of p such that $L \subseteq K^{1/q}$. By extending our field, we may assume that $a = x^q$ for some $x \in L$. It then suffices to prove that the integral closure B of A is a finite A-algebra.

We claim that xB is the unique ideal of B lying over aA (such an ideal exists by going up theorem). In fact, let $\mathfrak{P}$ be such an ideal. We have $x^q = a \in \mathfrak{P}$, hence $xB \subseteq \mathfrak{P}$ since $\mathfrak{P}$ is prime. Conversely, let y be an element of $\mathfrak{P}$; the element y^q of K is integral over A, hence belongs to A (recall that A is integrally closed). Since $\mathfrak{P} \cap A = aA$, there exist $b \in A$ such that $y^q = ab = x^q b$. Then the lement y/x of L is integral over A, hence contained in B; this means $y \in xB$, hence $\mathfrak{P} = xB$.

Recall that the ring B_{xB} is the integral closure of A_{aA} in L. By Proposition 14.2.16, A_{aA} is a DVR; we then deduce from the Krull-Akizuki theorem that B_{xB} is Noetherian (the ring $\kappa(xB)$ is a finite extension of $\kappa(aA)$). The ring B/xB is integral over the Japanese ring A/aA and its fraction field is a finite extension of that of A. Concequently, B/xB is a finitely generated (A/aA)-module. For each integer $i \geq 0$, this is isomorphic to the module $x^iB/x^{i+1}B$; so the (A/aA)-module B/aB possesses a composition sequence of length q with quotients finitely generated (A/aA)-modules, hence is also finitely generated over (A/aA).

Endow the ring A with the aA-adic topology and B the aB-adic topology. Then A is complete by hypothesis; since B_{xB} is a Noetherian integral domain, the aB_{xB}-adic filtration on B_{xB} is separated (Krull intersection theorem); therefore we have $\bigcap_n a^n B \subseteq \bigcap_n a^n B_{xB} = \{0\}$, and the aB-adic filtration on B is separated. The $\mathrm{gr}_{aA}(A)$-module $\mathrm{gr}_{aB}(B)$ is generated by $\mathrm{gr}_0(B)$, hence is finitely generated. It then follows from Corollary 11.3.34 that B is a finitely generated A-module, which completes the proof. □

Corollary 17.3.6. *Let R be a Noetherian integral domain and n an integer. If R is Japanese, so is the ring $R[\![T_1, \dots, T_n]\!]$.*

Proof. Argue by induction, we may assume that $n = 1$. Let S be the integral closure of R. If R is Japanese, S is a finite R-algebra, hence a Japanese ring (Proposition 17.3.4). The ring $S[\![T]\!]$ is Noetherian and integrally closed, so by applying Theorem 17.3.5 on $A = S[\![T]\!]$ and $a = T$, we deduce that $S[\![T]\!]$ is Japanese. Thus $R[\![T]\!]$ is Japanese (Proposition 17.3.4). □

Theorem 17.3.7 (Nagata). *Every Noetherian integral complete local ring is Japanese.*

Proof. By Theorem 17.2.20, there exist an integer $n \geq 0$, a ring R that is a field of a DVR whose fraction field has characteristic 0, and a subring B of A, isomorphic to $R[\![T_1, \dots, T_n]\!]$, such that A is a finite B-algebra. Since R is Japanese, we see B is Japanese, hence so is A. □

A Noetherian semi-local ring A is called **analytically unramified** if its completion $\widehat{A}$ is reduced. A prime ideal $\mathfrak{p}$ of A is said to be **analytically unramified** if $\widehat{A}/\widehat{\mathfrak{p}} = \widehat{A/\mathfrak{p}}$ is reduced. Theorem 17.3.7 then imply the following important result:

Corollary 17.3.8. *Let A be a semi-local Noetherian ring which is analytically unramified. Then the integral closure $\overline{A}$ of A in the total fraction ring $Q(A)$ is a finite A-algebra.*

Proof. Suppose first that A is local and complete, with $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ the minimal prime ideals of A. For each $i = 1, \dots, n$, let K_i be the fraction field of $A/\mathfrak{p}_i$ and $\overline{A}_i$ the integral closure of $A/\mathfrak{p}_i$ in K_i. Since A is reduced, $Q(A)$ is the product of the K_i and $\overline{A}$ is the product of $\overline{A}_i$ (Corollary 13.1.23). Since the local ring $A/\mathfrak{p}_i$ is integral and complete, it is Japanese (Theorem 17.3.7), so $\overline{A}_i$ is a finite A_i-algebra, and therefore $\overline{A}$ is finite over A. If A is semi-local and complete, it is isomorphic to a finite product of complete local rings (Corollary 11.3.28), and we conclude the claim by the previous case.

In the general case, note that the completion $\widehat{A}$ of A is semi-local, complete, Noetherian and faithfully flat (A is a Zariski ring). Let S be the set of elements of A that are not zero divisors; we have $Q(A) = S^{-1}A$. Since $\widehat{A}$ is flat over A, the elements of S are not zero divisors in $\widehat{A}$, and $S^{-1}\widehat{A}$ is identified with a subring of $Q(\widehat{A})$. Moreover, the ring $\overline{A} \otimes_A \widehat{A}$ is identified as a subring of $Q(A) \otimes_A \widehat{A}$, hence a subring T integral over $\widehat{A}$. The preceding arguments then apply and show that $\overline{A} \otimes_A \widehat{A}$ is a finitely generated $\widehat{A}$-module. Therefore, $\overline{A}$ is a finitely generated A-module (Proposition 7.3.17). □

Recall that an algebra E over a field K is called separable if the ring $L \otimes_K E$ is reduced for any extension L of K. The following proposition generalizes Theorem 17.3.7.

Proposition 17.3.9. *Let A be a semi-local Noetherian integral ring, K its fraction field. If the K-algebra $K \otimes_A \widehat{A}$ is separable, the ring A is Japanese.*

Proof. Let L be a finite extension of K and B the integral closure of A in L. Let F be a finite subset of B such that $L = K[F]$ (Theorem 13.1.48); let C be the A-algebra generated by F. Then L is the fraction field of C, the ring B is the integral closure of C, and it suffices to prove that B is a finite C-algebra. But C is a Noetherian semi-local ring, with completion identified with $C \otimes_A \widehat{A}$, which is a subring of the reduced ring $L \otimes_A \widehat{A} = L \otimes_K (K \otimes_A \widehat{A})$ and therefore reduced. The proposition then follows from Corollary 17.3.8. □

Finally, before considering Nagata ring, we prove some lemmas which will be used latter.

Lemma 17.3.10. *Let A be a Noetherian semi-local ring and B a finite A-algebra. Then B is Noetherian and semi-local; let $\mathfrak{m}_1, \dots, \mathfrak{m}_n$ be its maximal ideals. The canonical homomorphism of B to $\prod_{i=1}^n \widehat{B}_{\mathfrak{m}_i}$ then extends to an isomorphism of $\widehat{A} \otimes_A B$ to $\prod_{i=1}^n \widehat{B}_{\mathfrak{m}_i}$.*

Proof. By Corollary 12.2.22, the ring B is semi-local and $\mathfrak{m}_A B$ is a defining ideal. By Theorem 11.4.17(b), the ring $\widehat{A} \otimes_A B$ is the completion of B for the topology defined by its Jacobson radical. Then we can apply Corollary 11.3.28. □

Lemma 17.3.11. *Let A be a Noetherian ring and M an A-module. The canonical map of M into $\prod_{\mathfrak{p} \in \mathrm{Ass}(M)} M_{\mathfrak{p}}$ is injective.*

Proof. Let m be a nonzero element in M; then $\mathrm{Ann}(m)$ is contained in a prime ideal $\mathfrak{p}$ in $\mathrm{Ass}(M)$ (Proposition 12.1.3), and the image of m in $M_{\mathfrak{p}}$ is thus nonzero. □

Lemma 17.3.12. *Let A be a Noetherian local ring and $\mathfrak{p}$ a prime ideal of A. Assume that $A_{\mathfrak{p}}$ is a DVR and $\mathfrak{p}$ is analytically unramified, then for any associated prime $\hat{\mathfrak{q}}$ of $\widehat{A}/\mathfrak{p}\widehat{A}$, the local ring $\widehat{A}_{\hat{\mathfrak{q}}}$ is a DVR.*

Proof. Let π be a uniformizer for $A_{\mathfrak{p}}$. Since $\mathfrak{p}$ is analytically unramified, the associated primes of $\widehat{A}/\mathfrak{p}\widehat{A}$ are exactly the minimal primes of $\widehat{A}$ over $\mathfrak{p}\widehat{A}$, and in particular there is no embedded associated primel. Also, since $\widehat{A}/\mathfrak{p}\widehat{A} = \widehat{A/\mathfrak{p}}$ is reduced, we have $\{0\} = \bigcap \hat{\mathfrak{q}}/\mathfrak{p}\widehat{A}$ in $\widehat{A}/\mathfrak{p}\widehat{A}$, where $\hat{\mathfrak{q}}$ runs through minimal primes over $\mathfrak{p}\widehat{A}$. Therefore in $\widehat{A}$ we have

$$\mathfrak{p}\widehat{A} = \bigcap_{\hat{\mathfrak{q}} \in \mathrm{Ass}(\widehat{A}/\mathfrak{p}\widehat{A})} \hat{\mathfrak{q}}$$

which is then the unique primary decomposition of $\mathfrak{p}\widehat{A}$ in $\widehat{A}$. By Proposition 12.2.10, the $\hat{\mathfrak{q}}$-primary component of this decomposition is given by the saturation of $\mathfrak{p}\widehat{A}$ with respect to $\hat{\mathfrak{q}}$ (which is equal to $\hat{\mathfrak{q}}$), so in particular, we have

$$\hat{\mathfrak{q}}\widehat{A}_{\hat{\mathfrak{q}}} = \mathfrak{p}\widehat{A}_{\hat{\mathfrak{q}}} = \pi\widehat{A}_{\hat{\mathfrak{q}}}.$$

Since π is $\widehat{A}$-regular by the flatness of $\widehat{A}$ over A, the local ring $\widehat{A}_{\hat{\mathfrak{q}}}$ is regular of dimension 1, hence a DVR. □

Lemma 17.3.13. *Let A be a Noetherian semi-local integral domain with maximal ideal $\mathfrak{m}$. Let x be a nonzero element in $\mathfrak{m}$ such that*

(a) A/xA has no embedded primes;

(b) for each associated prime $\mathfrak{p}$ of A/xA, the local ring $A_{\mathfrak{p}}$ is regular and $\mathfrak{p}$ is analytically unramified.

Then A is analytically unramified.

Proof. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ be the associated primes of A/xA. Since A/xA has no embedded primes, we see that each $\mathfrak{p}_i$ has height 1, and is a minimal prime over xA. For each i, let $\hat{\mathfrak{q}}_{i,1}, \dots, \hat{\mathfrak{q}}_{i,n_i}$ be the associated primeds of the $\widehat{A}$-module $\widehat{A}/\mathfrak{p}_i\widehat{A}$. By Lemma 17.3.12 we see that $\widehat{A}_{\hat{\mathfrak{q}}_{i,j}}$ is a DVR for each i, j. Also, since $\widehat{A}$ is flat over A, by Proposition 12.2.26 we have

$$\mathrm{Ass}_{\widehat{A}}(\widehat{A}/x\widehat{A}) = \bigcup_{\mathfrak{p}\in\mathrm{Ass}_A(A/xA)} \mathrm{Ass}_{\widehat{A}}(\widehat{A}/\mathfrak{p}\widehat{A}) = \{\hat{\mathfrak{q}}_{i,j}\}.$$

Let y be a nonzero nilpotent in $\widehat{A}$. Then since $\widehat{A}_{\hat{\mathfrak{q}}_{i,j}}$ is integral for each i, j, the element y is mapped to zero in $\widehat{A}_{\hat{\mathfrak{q}}_{i,j}}$. By Lemma 17.3.11, the canonical image of y in $\widehat{A}/x\widehat{A}$ is then zero, which means $y = xy'$ for some $y' \in \widehat{A}$. But since the homothety with ratio x is injective on A, it is also injective on $\widehat{A}$, which implies $y' \in \widehat{A}$ is also a nonzero nilpotent element. Repeating this process, we conclude that $y \in \bigcap_n x^n\widehat{A} = \{0\}$ (Corollary 11.4.16), which shows $\widehat{A}$ is reduced and A is therefore analytically unramified. □

17.3.2 Nagata rings

A Noetherian ring is called Nagata if for any prime ideal $\mathfrak{p}$ of A, the Noetherian integral domain $A/\mathfrak{p}$ is Japanese. In this part, we give some of the properties of Nagata rings, and a criterion of Noetherian semi-local rings to be Nagata.

Example 17.3.14 (Example of Nagata rings).

(a) Any algebra of finite type over a field is a Nagata ring.

(b) Any Noetherian complete local ring is a Nagata ring by Theorem 17.3.7.

(c) The ring $\mathbb{Z}$ is a Nagata ring since any quotient $\mathbb{Z}/p\mathbb{Z}$ is a perfect field (hence Japanese).

(d) We will see that any algebra of finite type over a Nagata ring is Nagata.

Proposition 17.3.15. *Let A be a Nagata ring.*

(a) Any finite A-algebra is a Nagata ring.

(b) For any multiplicative subset S of A, the ring $S^{-1}A$ is a Nagata ring.

Proof. Let B be a finite A-algebra and $\rho : A \to B$ the homomorphism. For each prime ideal $\mathfrak{P}$ of B, the ring $B/\mathfrak{P}$ is a finite algebra of the Japanese ring $A/\mathfrak{p}^c$, hence is Japanese.

Let S be a multiplicative subset of A and $\mathfrak{q}$ a prime ideal of $S^{-1}A$; then there exist a prime ideal $\mathfrak{p}$ of A such that $\mathfrak{q} = S^{-1}\mathfrak{p}$. The ring $S^{-1}A/\mathfrak{q}$ is a fraction ring of the Japanese ring $A/\mathfrak{p}$, hence is Japanese. □

Theorem 17.3.16 (Nagata). *Let A be a Noetherian semi-local integral domain. If A is a Nagata ring then it is analytically unramified.*

Proof. We use induction on $\dim(A)$. Let B be the integral closure of A in its fraction field K. Then B is finite over A, hence $\dim(A) = \dim(B)$ and for any $\mathfrak{P} \in \mathrm{Spec}(B)$, the domain $B/\mathfrak{P}$ is finite over $A/\mathfrak{p}$ (where $\mathfrak{p} = \mathfrak{P} \cap A$), which is assumed to be Japanese. Thus $B/\mathfrak{P}$ is Japanese and B is therefore a Nagata ring. Moreover, the defining ideal of B is given by the extension of that

of A, which implies $\widehat{B} = B \otimes_A \widehat{A}$; since $\widehat{A}$ is a flat A-module, we can then identify $\widehat{A}$ as a subring of $\widehat{B}$. Thus we can replace A by its integral closure and assume that A is integrally closed. In this case, for any nonzero element $x \in A$, the A-module A/xA has no embedded primes by Proposition 15.1.29. If $\mathfrak{p} \in \mathrm{Ass}(A/xA)$, then $A/\mathfrak{p}$ is a Nagata domain and $\dim(A/\mathfrak{p}) < \dim(A)$, hence $\mathfrak{p}$ is analytically unramified by the induction hypothesis. Moreover, $A_\mathfrak{p}$ is a DVR because $\mathrm{ht}(\mathfrak{p}) = 1$ (Theorem 15.1.28 and Proposition 15.1.29). So the conditions of Lemma 17.3.13 are satisfied, and A is analytically unramified. □

Theorem 17.3.17 (Zariski-Nagata). *Let A be a Noetherian semi-local ring. The following conditions are equivalent:*

(i) A is a Nagata ring;

(ii) for any prime ideal $\mathfrak{p}$ of A, the $\kappa(\mathfrak{p})$-algebra $\kappa(\mathfrak{p}) \otimes_A \widehat{A}$ is separable;

(iii) for any reduced A-algebra R, the ring $R \otimes_A \widehat{A}$ is reduced.

Proof. We first demonstrate the equivalence of (ii) and (iii). The implication (iii)⇒(ii) is trivial; suppose conversely that A satisfies (ii). Then for any A-algebra K that is a field, the ring $K \otimes_A \widehat{A}$ is reduced since it is isomorphic to $K \otimes_{\kappa(\mathfrak{p})} \kappa(\mathfrak{p}) \otimes_A \widehat{A}$. Now let C be a reduced A-algebra of finite type, then the ring C, being Noetherian, is isomorphic to a subring of a finite product $K_1 \times \cdots \times K_n$ of fields (Proposition 12.2.24). Since $\widehat{A}$ is flat over A, the ring $C \otimes_A \widehat{A}$ is isomorphic to a subring of the reduced ring $\prod_i (K_i \otimes_A \widehat{A})$, hence is reduced. Finally, since any reduced A-algebra R is the union of a family of finite type A-algebras (C_α), we see $R \otimes_A \widehat{A}$ is reduced (it is the inductive limit of the family $(C_\alpha \otimes_A \widehat{A})$).

We now show that (ii)⇔(i). Let $\mathfrak{p}$ be a prime ideal of A. The fraction field K of $A/\mathfrak{p}$ is then identified with $\kappa(\mathfrak{p})$, and the K-algebra $K \otimes_{A/\mathfrak{p}} \widehat{A/\mathfrak{p}}$ is identified with $\kappa(\mathfrak{p}) \otimes_{A/\mathfrak{p}} \widehat{A}/\mathfrak{p}\widehat{A}$, hence to $\kappa(\mathfrak{p}) \otimes_A \widehat{A}$. If $\kappa(\mathfrak{p}) \otimes_A \widehat{A}$ is a separable $\kappa(\mathfrak{p})$-algebra, then $A/\mathfrak{p}$ is Japanese by Proposition 17.3.9.

Conversely, we prove (i)⇒(ii). Let A be a semi-local Noetherian Nagata ring, let $\mathfrak{p}$ be an ideal of A, and L a finite extension of $\kappa(\mathfrak{p})$. It suffices to show that the ring $L \otimes_A \widehat{A}$ is reduced. Let B by the integral closure of $A/\mathfrak{p}$ in L; since $A/\mathfrak{p}$ is Japanese, B is a finite A-algebra hence a semi-local Nagata ring (Proposition 17.3.15). Let $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ be the maximal ideal of B; the ring $L \otimes_A \widehat{A}$ is identified with a fraction ring of $B \otimes_A \widehat{A}$, and with that of a product of complete local rings $\widehat{B}_{\mathfrak{m}_i}$ (Lemma 17.3.10). It then suffices to prove that, for any maximal ideal $\mathfrak{m}$ of B, the ring $\widehat{B}_\mathfrak{m}$ is reduced (Corollary 10.2.38). But the ring $B_\mathfrak{m}$ is a Noetherian local ring that is Nagata (Proposition 17.3.15), so by Theorem 17.3.16 it is analytically unramified, which is what we want. □

Corollary 17.3.18 (Chevally). *Let A be a reduced algebra of finite type over a field, and $\mathfrak{p}$ a prime ideal of A. Then the local ring $A_\mathfrak{p}$ is analytically unramified.*

Proof. Since A is reduced, the local ring $A_\mathfrak{p}$ is reduced. The ring A is Nagata, hence $A_\mathfrak{p}$ is also Nagata, and Theorem 17.3.16 implies the claim. □

Corollary 17.3.19. *Let k be a field of characteristic 0 and A a Noetherian local k-algebra. Then A is a Nagata ring if and only if every prime ideal $\mathfrak{p}$ of A is analytically unramified.*

Proof. In fact, since the residue field $\kappa(\mathfrak{p})$ has characteristic 0, the $\kappa(\mathfrak{p})$-algebra $\kappa(\mathfrak{p}) \otimes_A \widehat{A} = \kappa(\mathfrak{p}) \otimes_{A/\mathfrak{p}} \widehat{A/\mathfrak{p}}$ is separable if and only if it is reduced, which shows that the stated condition is

sufficient (Theorem 17.3.17, not that $\kappa(\mathfrak{p}) \otimes_{A/\mathfrak{p}} \widehat{A/\mathfrak{p}}$ is a localization of $\widehat{A/\mathfrak{p}}$). It is also necessary by take $R = A/\mathfrak{p}$ in Theorem 17.3.17(iii). □

A Noetherian ring A is called **universally Japanese** if any integral A-algebra B of finite type over A is Japanese. It is clear that such a ring is Nagata, since $A/\mathfrak{p}$ is a finite type A-algebra for any prime ideal $\mathfrak{p}$ of A. We now prove the reverse direction, which is not at all obvious. For this, we first establish some lemmas.

Lemma 17.3.20. *Let A be a Noetherian integral domain and put $X = \mathrm{Spec}(A)$. Suppoe that there exist nonzero element f in A such that A_f is integrally closed, then the set*

$$\mathrm{Nor}(X) = \{\mathfrak{p} \in \mathrm{Spec}(A) : A_{\mathfrak{p}} \textit{ is integrally closed}\}$$

is open in X.

Proof. If $f \notin \mathfrak{p}$ for some $\mathfrak{p} \in X$, then $A_{\mathfrak{p}}$ is a localization of A_f, hence integrally closed. This shows $D(f) \subseteq \mathrm{Nor}(X)$. Now we put

$$E = \{\mathfrak{p} \in \mathrm{Ass}_A(A/fA) : \text{either } \mathrm{ht}(\mathfrak{p}) = 1 \text{ and } A_{\mathfrak{p}} \text{ is not regular, or } \mathrm{ht}(\mathfrak{p}) > 1\}.$$

Since $\mathrm{Ass}_A(A/fA)$ is finite, it is clear that E is a finite subset of X. On the other hand, by Serre's criterion for normality, if $\mathfrak{p} \notin \mathrm{Nor}(X)$ then there exist a prime $\mathfrak{q} \subseteq \mathfrak{p}$ such that either $\mathrm{ht}(\mathfrak{q}) \geq 2$ and $\mathrm{depth}(A_{\mathfrak{q}}) < 2$, or $\mathrm{ht}(\mathfrak{q}) = 1$ and $A_{\mathfrak{q}}$ is not regular. This in particular also means that $A_{\mathfrak{q}}$ is not integrally closed, and hence $f \in \mathfrak{q}$. In both cases we see $\mathfrak{q}$ is an associated prime of A/fA. It then follows that $\mathrm{Nor}(X) = X \setminus \bigcup_{\mathfrak{p} \in E} V(\mathfrak{p})$, so $\mathrm{Nor}(X)$ is open in X. □

Lemma 17.3.21. *Let A be a Noetherian domain with quotient field K. Then A is N-1 if and only if the following conditions hold:*

(a) there exists a nonzero element $f \in A$ such that A_f is integrally closed;

(b) $A_{\mathfrak{m}}$ is N-1 for each maximal ideal $\mathfrak{m}$ of A.

Proof. First assume that A is N-1. Let $\overline{A}$ be the integral closure of A in its fraction field K. By assumption we can find $x_1, \ldots, x_n$ in $\overline{A}$ which generate it as an A-module. Since $\overline{A} \subseteq K$, we may further assume that $x_i = a_i/b$ for $a_i, b \in A$. Then $A_f \cong \overline{A}_f$, where the latter is the integral closure of the former. This shows A_f is integrally closed, hence (a) holds. It is clear that (b) follos, since the integral closure of $A_{\mathfrak{m}}$ is just $\overline{A}_{\mathfrak{m}}$.

Conversely, assume (a), (b) for A and let K be the fraction field of A. For a subring B of K that is finite over A, we set $X = \mathrm{Spec}(A)$, $Y = \mathrm{Spec}(B)$. Note that $A_f = B_f$ since A_f is integrally closed, so by Lemma 17.3.20 the set $\mathrm{Nor}(Y)$ is open in Y. Since the canonical map $\overline{X} \to X$ is closed (Proposition 13.1.82), the image of the complement of $\mathrm{Nor}(Y)$ is then closed in X, we denote it by Z_B for such a ring B.

Pick a maximal ideal $\mathfrak{m}$ of A and let $A_{\mathfrak{m}} \subseteq \overline{A}_{\mathfrak{m}}$ be the integral closure of the local ring in K. By assumption, this is a finite ring extension, so we can find finitely many elements $x_1, \ldots, x_n$ in $\overline{A}$ such that $\overline{A}_{\mathfrak{m}}$ is generated by $x_1, \ldots, x_n$ over $A_{\mathfrak{m}}$. Let $B(\mathfrak{m}) = A[x_1, \ldots, x_n] \subseteq K$, then $B(\mathfrak{m})$ is finite over A, hence is Noetherian. Let $\mathfrak{M}$ be any prime ideal of $B(\mathfrak{m})$ lying over $\mathfrak{m}$, then

$$B(\mathfrak{m})_{\mathfrak{M}} \supset B(\mathfrak{m})_{\mathfrak{m}} \supset B(\mathfrak{m}),$$

and $B(\mathfrak{m})_{\mathfrak{m}} = \overline{A}_{\mathfrak{m}}$ is integrally closed. Thus $B(\mathfrak{m})_{\mathfrak{M}}$ is a localization of the integrally closed ring $\overline{A}_{\mathfrak{m}}$, so is integrally closed. This shows $\mathfrak{m} \notin Z_{B(\mathfrak{m})}$, so the intersection $\bigcap_{\mathfrak{m}\in\mathrm{Max}(A)} Z_{B(\mathfrak{m})}$ contains no closed point, and is therefore empty (since it is a closed subset of X). As X is quasi-compact, we can choose maximal ideals $\mathfrak{m}_1, \dots, \mathfrak{m}_r$ such that $\bigcap_i Z_{B(\mathfrak{m}_i)} = \varnothing$. Put $B_i = B(\mathfrak{m}_i)$ and let C be the ring generated by all of these; it is finite over A. We claim that $Z_C = \varnothing$, in other words, $C_{\mathfrak{Q}}$ is integrally closed for any $\mathfrak{Q} \in \mathrm{Spec}(C)$. In fact, the contraction of any prime $\mathfrak{Q}$ of C into A is not contained in some Z_{B_i}, so it lies over a prime $\mathfrak{P}_i$ of B_i such that $(B_i)_{\mathfrak{P}_i}$ is integrally closed. This implies $C_{\mathfrak{Q}} = (B_i)_{\mathfrak{P}_i}$ is integrally closed too, so C is integrally closed (Proposition 13.1.41). In other words, C is the integral closure of A in K, so A is N-1. □

Theorem 17.3.22 (Nagata). *Let A be a Noetherian ring. The following are equivalent:*

(i) A is a Nagata ring;

(ii) any finite type A-algebra B is Nagata;

(iii) A is universally Japanese.

Proof. It is clear that a Noetherian universally Japanese ring is universally Nagata (i.e., condition (ii) holds). Let A be a Noetherian Nagata ring. We will show that any finite type A-algebra B is Nagata. Note that the canonical image of A in B is also a Nagata ring, so we may assume that A is a subring of B. Then $B = A[x_1, \dots, x_n]$ with $x_i \in B$, and by induction it suffices to consider the case $B = A[x]$.

Let $\mathfrak{P}$ be a prime ideal of B and $\mathfrak{p} = \mathfrak{P}^c$. Then $B/\mathfrak{P} = (A/\mathfrak{p})[\bar{x}]$, where $A/\mathfrak{p}$ is a Nagata domain (Proposition 17.3.15), and we must show that $B/\mathfrak{P}$ is Japanese. We are then reduced to prove the following assertion:

(A1) If A is a Noetherian Nagata domain and $B = A[x]$ is an integral domain generated by a single x over A, then B is Japanese.

Let K be the fraction field of A and $\overline{A}$ the integral closure of A in K. Let $\overline{B}$ be the subring of the fraction field of B generated by $\overline{A}$ and B. As $\overline{A}$ is finite over A (by the Nagata property, since A is an integral domain), $\overline{B}$ is finite over B. Since B is Noetherian, it then suffices to prove that $\overline{B}$ is Japanese (Proposition 17.3.4). Hence we can add the integrally closed assumption in (A1):

(A2) If A is an integrally closed Noetherian Nagata domain and $B = A[x]$ is an integral domain generated by a single x over A, then B is Japanese.

In this case, let L be the fraction field of B. We first note that, if x is transcendental over A, then $B = A[x]$ is isomorphic to the polynomial ring $A[X]$, hence is integrally closed. Thus if L has characteristic 0, we are done (Corollary 17.3.3). Suppose otherwise L has characteristic $p > 0$, and take a finite purely inseparable extension E of $L = K(x)$. Let $q = p^e$ be a power of p such that $E \subseteq L^{1/q}$. Then there exists a finite purely inseparable extension K' of K such that $E \subseteq K'(x^{1/q})$. If $\overline{A}$ (resp. $\overline{B}$) is the integral closure of A in K' (resp. of B in L), then $\overline{A}[x^{1/q}]$ is normal and we have $B = A[x] \subseteq \overline{B} \subseteq \overline{A}[x^{1/q}]$. Since $\overline{A}[x^{1/q}]$ is finite over B, we conclude that $\overline{B}$ is finite over B.

Now assume that x is algebraic over A, so that L/K is a finite extension. Let E be a finite extension of L (hence finite over K) and $\overline{A}$ be the integral closure of A in E. Then the integral closure $\overline{B}$ of B in E is equal to the integral closure of $\overline{A}[x]$ in E. Also the fraction field of $\overline{A}$

is E and $\overline{A}$ is a finite A-algebra (A is Japanese). This implies that $\overline{A}$ is a Nagata ring (Proposition 17.3.15). To show that $\overline{B}$ is finite over B is the same as showing that $\overline{B}$ is finite over $\overline{A}[x]$, so by replacing A by $\overline{A}$ and B by $\overline{B}[x]$, we are reduced to prove the following statement:

(A3) If A is an integrally closed Noetherian Nagata domain with fraction field K and x is an element of K, the ring $B = A[x]$ is N-1.

We now proceed with proving (A3). Since $x \in K$, we can write $x = a/b$ where $a, b \in A$. Then $B_a = B[1/a] = A[1/a]$ is integrally closed since it is a localization of A. By Lemma 17.3.21, it then suffices to prove that $B_{\mathfrak{M}}$ is N-1 for any maximal ideal $\mathfrak{M}$ of B. Now pick such a maximal ideal and set $\mathfrak{m} = \mathfrak{M} \cap A$. The residue field extension $\kappa(\mathfrak{m})/\kappa(\mathfrak{M})$ is finite and generated by the image of x. Hence there exists a monic polynomial $f(X) \in A[X]$ with $f(x) \in \mathfrak{M}$. Let E/K be a finite extension of fields such that $f(X)$ splits completely in $E[X]$. Let $\overline{A}$ be the integral closure of A in E, and $\overline{B} \subseteq E$ be the subring generated by $\overline{A}$ and x. As A is a Nagata ring, we see $\overline{A}$ is finite over A and hence Nagata (Proposition 17.3.15). Moreover, $\overline{B}$ is finite over B. If for every maximal ideal $\overline{\mathfrak{M}}$ of $\overline{B}$ the local ring $\overline{B}_{\overline{\mathfrak{M}}}$ is N-1, then $\overline{B}_{\overline{\mathfrak{M}}}$ is N-1 by Lemma 17.3.21, which in turn implies that $B_{\mathfrak{M}}$ is N-1 (by a proof similar to that of Proposition 17.3.4). Thus, after replacing A by $\overline{A}$ and B by $\overline{B}$, and $\mathfrak{M}$ by any of the maximal ideals $\overline{\mathfrak{M}}$ lying over $\mathfrak{M}$, we reach the situation where the polynomial $f(X)$ above split completely: $f(X) \prod_{i=1}^{d}(X - a_i)$ with $a_i \in A$. Since $f(x) \in \mathfrak{M}$ we see that $x - a_i \in \mathfrak{M}$ for some i. Finally, after replacing x by $x - a_i$ we may assume that $x \in \mathfrak{M}$.

We will show that Lemma 17.3.13 applies to the local ring $B_{\mathfrak{M}}$ and the element x. This will imply that $B_{\mathfrak{M}}$ is analytically unramified, whence it is N-1 by Corollary 17.3.8. Let Q be the kenrel of the canonical map $A[X] \to B$, where X is mapped to x. Then by Exercise 16.2.4, the ideal Q is generated by all linear forms $aX - b$, where $ax = b$ in K. Therefore, we see that

$$B/xB = A[X]/(x, \mathfrak{a}) = A/I$$

where I is the constant term of the elements in Q, or in other words $I = xA \cap A$. Now note that A is a Noetherian integrally closed domain and I is divisorial, so by Proposition 15.1.21, if $\operatorname{div}(xA \cap A) = \sum_i n_i P_i$ with $\mathfrak{p}_i$ the corresponding prime of P_i, then

$$I = xA \cap A = \bigcap_i \mathfrak{p}_i^{(n_i)}$$

is the unique reduced primary decomposition of I and the $\mathfrak{p}_i$ are isolated primes of I. This shows $A/I = B/xB$ has no embedded primes, so does $B_{\mathfrak{M}}$, in view of Proposition 12.1.11.

Now let $\mathcal{P} \in \operatorname{Spec}(B_{\mathfrak{M}})$ be an associated prime of $B_{\mathcal{P}}/xB_{\mathfrak{M}}$. Then $\mathfrak{p} = \mathcal{P} \cap A$ is an associated prime of $A/(xB_{\mathfrak{M}} \cap A) = A/I$ and $\operatorname{ht}(\mathfrak{p}) = 1$ by Proposition 15.1.29, so $(B_{\mathfrak{M}})_{\mathcal{P}} = A_{\mathfrak{p}}$ is a DVR (Theorem 15.1.28), hence regular. Finally, $B_{\mathfrak{M}}/\mathcal{P}$ is a localization of $B/(\mathcal{P} \cap B)$ (which is isomorphic to $A/\mathfrak{p}$ since $x \in \mathfrak{p}$), so $B_{\mathfrak{M}}/\mathcal{P}$ is a Noetherian Nagata local domain, hence analytically unramified. Thus the conditions in Lemma 17.3.13 are verified and our proof is completed. □

Chapter 18

Depth

18.1 Homological definition of depth

Let A be a ring, $\mathfrak{a}$ an ideal of A, and M an A-module. We define the **depth of M relative to** $\mathfrak{a}$, denoted by $\operatorname{depth}_A(\mathfrak{a}, M)$ or $\operatorname{depth}(\mathfrak{a}, M)$, to be the infimum in $\mathbb{N} \cup \{+\infty\}$ of the set of integers i such that $\operatorname{Ext}^i_A(A/\mathfrak{a}, M)$ is nonzero. If A is a local ring, we simply call the **depth of M** and we denote $\operatorname{depth}_A(M)$ or $\operatorname{depth}(M)$ the depth of M relative to the maximum ideal $\mathfrak{m}_A$ of A; the depth of the local ring A is defined to be the depth of the A-module A.

Unwinding the definition, we see that, if $\operatorname{depth}_A(\mathfrak{a}, M) = +\infty$, we have $\operatorname{Ext}^i_A(A/\mathfrak{a}, M) = 0$ for all i; if $\operatorname{depth}_A(\mathfrak{a}, M) = r < +\infty$, then $\operatorname{Ext}^i_A(A/\mathfrak{a}, M) = 0$ for $i < r$ and $\operatorname{Ext}^r_A(A/\mathfrak{a}, M) \neq 0$.

Remark 18.1.1.

(a) Let M be a fnitely generated A-module and such that $M = \mathfrak{a}M$, which means $\operatorname{supp}(M) \cap V(\mathfrak{a}) = \varnothing$ (Corollary 10.4.38). In this case, $\operatorname{depth}_A(\mathfrak{a}, M)$ is equal to $+\infty$: in fact, the ideal $\operatorname{Ann}(M) + \mathfrak{a}$ is equal to A (since $V(\operatorname{Ann}(M) + \mathfrak{a}) = \varnothing$) and is contained in the annihilator of $\operatorname{Ext}^i_A(A/\mathfrak{a}, M)$ for each i. We will see conversely that, if $\mathfrak{a}$ is a finitely generated ideal, then $\operatorname{depth}_A(\mathfrak{a}, M) = +\infty$ implies $M = \mathfrak{a}M$.

(b) For $\operatorname{depth}_A(\mathfrak{a}, M)$ to be zero, it is necessary and sufficient that $\operatorname{Hom}_A(A/\mathfrak{a}, M)$ is zero, which is to say that M has a nonzero element killed by $\mathfrak{a}$. This in particular implies that $\operatorname{Ass}(M) \cap V(\mathfrak{a}) \neq \varnothing$ (Proposition 12.1.3). If A is Noetherian and the A-module M is finitely generated, the following conditions are equivalent (Corollary 12.1.19):

  (i) $\operatorname{depth}_A(\mathfrak{a}, M) = 0$;

  (ii) for any $x \in \mathfrak{a}$, the homothety x_M is not injective;

  (iii) we have $\operatorname{Ass}(M) \cap V(\mathfrak{a}) \neq \varnothing$.

(c) By (b), for a local ring to have zero depth. it is necessary and sufficient that there exist a nonzero element x of A such tha $\mathfrak{t}\mathfrak{m}_A x = 0$. If A is not a field, such an element is then not invertible, hence belongs to $\mathfrak{m}_A$ and satisfies $x^2 = 0$. Therefore, any reduced local ring of dimension ≥ 1 has depth ≥ 1.

(d) Let $(M_i)_{i \in I}$ be a family of A-module. By **??**, we have $\operatorname{depth}(\mathfrak{a}, \prod_{i \in I} M_i) = \inf_{i \in I} \operatorname{depth}(\mathfrak{a}, M_i)$.

Proposition 18.1.1. *Let A be a ring, $\mathfrak{a}$ an ideal of A, and let*

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

be an exact sequence of A-modules. Then there are exactly three cases:

(i) $\operatorname{depth}(\mathfrak{a}, M) = \operatorname{depth}(\mathfrak{a}, M') \leq \operatorname{depth}(\mathfrak{a}, M'')$*;*

(ii) $\operatorname{depth}(\mathfrak{a}, M) = \operatorname{depth}(\mathfrak{a}, M'') \leq \operatorname{depth}(\mathfrak{a}, M')$*;*

(iii) $\operatorname{depth}(\mathfrak{a}, M'') = \operatorname{depth}(\mathfrak{a}, M') - 1 < \operatorname{depth}(\mathfrak{a}, M'')$*;*

Proof. Consider the long exact sequence associated with this short exact sequence:

$$0 \to \operatorname{Ext}^0_A(A/\mathfrak{a}, M') \to \operatorname{Ext}^0_A(A/\mathfrak{a}, M) \to \operatorname{Ext}^0_A(A/\mathfrak{a}, M'') \to \operatorname{Ext}^1_A(A/\mathfrak{a}, M') \to \cdots$$

We may exclude the case $\operatorname{depth}(\mathfrak{a}, M') = \operatorname{depth}(\mathfrak{a}, M) = \operatorname{depth}(\mathfrak{a}, M') = +\infty$. There then exists in this sequence a first non-zero module, and the next module is thus nonzero. The three cases then correspond to which module is the first to be nonzero. □

Proposition 18.1.2. *Let A be a ring, $\mathfrak{a}$ an ideal of A, M an A-module and N an A-module killed by a power of $\mathfrak{a}$. Then $\operatorname{Ext}^i_A(N, M) = 0$ for any integer $i < \operatorname{depth}_A(\mathfrak{a}, M)$.*

Proof. □

Chapter 19

Sheaves and cohomology of sheaves

19.1 Sheaves of sets

In this section, X always denotes a topological space.

19.1.1 Presheaves and sheaves

Definition 19.1.1. *A **presheaf** $\mathscr{F}$ on a topological space X is the following data.*

- *To each open set $U \subseteq X$, we have a set $\mathscr{F}(U)$.*
- *For each inclusion $U \subseteq V$ of open sets, we have a **restriction map** $\mathrm{res}_U^V : \mathscr{F}(V) \to \mathscr{F}(U)$.*

The data is required to satisfy the following two conditions.

- *The map res_U^U is the identity: $\mathrm{res}_U^U = \mathbf{1}_{\mathscr{F}(U)}$.*
- *If $U \subseteq V \subseteq W$ are inclusions of open sets, then the restriction maps commute,*

$$\begin{tikzcd}
\mathscr{F}(W) \arrow[rr, "\mathrm{res}_U^W"] \arrow[dr, "\mathrm{res}_V^W"'] & & \mathscr{F}(U) \\
& \mathscr{F}(V) \arrow[ur, "\mathrm{res}_U^V"'] &
\end{tikzcd}$$

Definition 19.1.2. *A **morphism of presheaves** $\varphi : \mathscr{F} \to \mathscr{G}$ is a family of maps $\varphi(U) : \mathscr{F}(U) \to \mathscr{G}(U)$ for all open subsets $U \subseteq X$ behaving well with respect to restriction: if $U \hookrightarrow V$ then*

$$\begin{tikzcd}
\mathscr{F}(U) \arrow[r, "\varphi(U)"] \arrow[d, "\mathrm{res}_V^U"'] & \mathscr{G}(U) \arrow[d, "\mathrm{res}_V^U"] \\
\mathscr{F}(V) \arrow[r, "\varphi(V)"] & \mathscr{G}(V)
\end{tikzcd} \tag{1.1.1}$$

commutes. Composition of morphisms φ and ψ of presheaves is defined in the obvious way: $(\varphi \circ \psi)_U := \varphi_U \circ \psi_U$. We obtain the category $\mathbf{PSh}(X)$ of presheaves on X.

If $U \subseteq V$ are open subset of X and $s \in \mathscr{F}(V)$, we will usually write $s|_U$ instead of $\mathrm{res}_U^V(s)$. The elements of $\mathscr{F}(U)$ are called **sections of $\mathscr{F}$ over U**. By convention, if the U is omitted, it is implicitly taken to be X: sections of $\mathscr{F}$ means sections of $\mathscr{F}$ over X. These are also called **global sections**. Very often we will also write $\Gamma(U, \mathscr{F})$ instead of $\mathscr{F}(U)$.

Remark 19.1.1. Given any topological space X, we have a category of open sets $\mathcal{T}_X$, where the objects are the open sets and the morphisms are set inclusions. A presheaf is a contravariant funtor from this category to **Set**:

$$\mathscr{F} : (\mathcal{T}_X)^{op} \to \mathbf{Set}$$

and a morphism of presheaves is a natural transforml of presheaves. With this observation, for any category C we can define a **presheaf $\mathscr{F}$ with values in C** to be a contravariant funtor $(\mathcal{T}_X)^{op} \to C$. A morphism $\mathscr{F} \to \mathscr{G}$ of presheaves with values in C is then simply a morphism of functors.

Example 19.1.3 (presheaf of functions). Let E be a set. For each open subset U of X, let $\mathrm{Map}_E(U)$ be the set of all maps $U \to E$. For an open subset $V \subseteq U$ we define $\mathrm{res}^U_V : \mathrm{Map}_E(U) \to \mathrm{Map}_E(V)$ as the usual restriction of maps. Then Map_E is a presheaf on X.

More generally, a family $\mathscr{F}$ of subsets $\mathscr{F}(U) \subseteq \mathrm{Map}_E(U)$, where U runs through the open subsets of X, is called a **presheaf of E-valued functions on X**, if it is stable under restriction, i.e., for all open sets $V \subseteq U$ and all $f \in \mathscr{F}(U)$ one has $f|_V \in \mathscr{F}(V)$. Then $\mathscr{F}$ together with the restriction maps is a presheaf of sets.

If E is a group (respectively an R-module for some ring R, respectively an A-algebra for some commutative ring A), then $\mathscr{F}$ is a presheaf of groups (respective of R-modules, respective of A-algebras).

Example 19.1.4 (Examples of presheaf of functions).

(a) Let Y be a topological space. For open subset $U \subseteq X$, define

$$C(U, Y) := \{f : U \to Y \mid f \text{ is continuous}\}.$$

Then $C(-, Y)$ is a presheaf of Y-valued functions on X. If $Y = \mathbb{R}$, then $C(-, Y)$ a presheaf of $\mathbb{R}$-algebras.

(b) Let V be a finite-dimensional R-vector spaces and let X be an open subspace of V. Let $0 \leq n \leq \infty$. For an open subset U of X, define

$$C^n(U) := \{f : U \to W, f \text{ is a } C^n\text{-map}\}.$$

Then C^n is a presheaf of functions on X. It is a presheaf of $\mathbb{R}$-algebras.

Definition 19.1.5. *A presheaf is a **sheaf** if it satisfies two more axioms.*

- ***Identity axiom**. If $\{U_i\}_{i\in I}$ is an open cover of U, and $s_1, s_2 \in \mathscr{F}(U)$, and $s_1|_{U_i} = s_2|_{U_i}$ for all i, then $s_1 = s_2$.*
- ***Gluability axiom**. If $\{U_i\}_{i\in I}$ is an open cover of U, then given $s_i \in \mathscr{F}(U_i)$ for all i, such that*

$$s_i|_{U_i\cap U_j} = s_j|_{U_i\cap U_j}$$

for all i and j, then there is some $s \in \mathscr{F}(U)$ such that $s|_{U_i} = s_i$ for all i.

*A **morphism of sheaves** is a morphism of presheaves, and we obtain the category of sheaves on the topological space X, which we denote by* $\mathbf{Shv}(X)$.

Remark 19.1.2. If $\mathscr{F}$ is a sheaf on X, then by using the covering of the empty set $U = \varnothing$ with empty index set $I = \varnothing$, we see $\mathscr{F}(\varnothing)$ is a set consisting of one element. In general, if $U, V \subseteq X$ are disjoint open subsets, then

$$\mathscr{F}(U \cup V) = \mathscr{F}(U) \times \mathscr{F}(V).$$

Example 19.1.6 (Sheaf of E-valued functions). Let E be a set and let $\mathscr{F}$ be a presheaf of E-valued functions on X. Then $\mathscr{F}$ is a sheaf if and only if the following condition holds:

> For every open subset U of X, for every open covering $\{U_i\}_{i\in I}$ of U and for every map $f : U \to E$ such that $f|_{U_i} \in \mathscr{F}(U_i)$ for all i, one has $f \in \mathscr{F}(U)$.

In particular, the presheaves $C(-, Y)$ and C^n are in fact sheaves.

Example 19.1.7 (Constant sheaf). The presheaf of constant functions with values in some set is in general not a sheaf: if U_1 and U_2 are disjoint non-empty open subsets and if $f_1 : U_1 \to E$ and $f_2 : U_2 \to E$ are constant maps that take different values, then there does not exist a constant map f on $U = U_1 \cup U_2$ whose restriction to U_i is f_i for $i = 1, 2$.

If one takes instead the sheaf of locally constant functions with values in some set E, then this is a sheaf. This comes from the simple observation: endow E with the discrete topology, then locally constant maps are exactly continuous maps from U to E. This is called the **constant sheaf associated to E**. We denote this sheaf E_X.

19.1.2 Stalks of presheaves and sheaves

Let X be a topological space, $\mathscr{F}$ be a presheaf on X, and let $x \in X$ be a point. The **stalk** of $\mathscr{F}$ in x is defined by the direct limit

$$\mathscr{F}_x := \varinjlim_{U \ni x} \mathscr{F}(U).$$

More concretely, one has

$$\mathscr{F}_x = \{(U, s) : U \text{ is an open neighborhood of } x \text{ and } s \in \mathscr{F}(U)\}/\sim .$$

where two pairs $(U_1, s_1) \sim (U_2, s_2)$ are equivalent if there exists an open neighborhood V of x with $V \subseteq U_1 \cap U_2$ such that $s_1|_V = s_2|_V$. Then for each open neighborhood U of x we have a canonical map

$$\mathscr{F}(U) \mapsto \mathscr{F}_x, \quad s \mapsto s_x,$$

which sends $s \in \mathscr{F}(U)$ to the class of (U, s) in $\mathscr{F}_x$. We call s_x the **germ** of s in x.

Remark 19.1.3. If $\mathscr{F}$ is a presheaf on X with values in $\mathcal{C}$, where $\mathcal{C}$ is any category in which filtered colimits exist, then the stalk $\mathscr{F}_x$ is an object in $\mathcal{C}$ and we obtain a functor $\mathscr{F} \to \mathscr{F}_x$ from the category of presheaves on X with values in $\mathcal{C}$ to the category $\mathcal{C}$.

Example 19.1.8 (Stalk of the sheaf of continuous functions). Let X be a topological space, let C_X be the sheaf of continuous $\mathbb{R}$-valued functions on X, and let $x \in X$. Then

$$C_{X,x} = \{(U, f) : x \in U \subseteq X \text{ open}, f : U \to \mathbb{R} \text{ is continuous}\}/\sim,$$

where $(U, f) \sim (V, g)$ if there exists $x \in W \subseteq U \cap V$ open such that $f|_W = g|_W$. In particular we see that for $x \in V \subseteq U$ open and $f : U \to \mathbb{R}$ continuous one has $(U, f) \sim (V, f|_V)$. As C_X is a sheaf of $\mathbb{R}$-algebras, $C_{X,x}$ is an $\mathbb{R}$-algebra.

If the germ $s \in C_{X,x}$ of a continuous function at x is represented by (U, f), then $s(x) := f(x) \in \mathbb{R}$ is independent of the choice of the representative (U, f). We obtain an $\mathbb{R}$-algebra homomorphism

$$\mathrm{ev}_x : C_{X,x} \to \mathbb{R}, \quad s \mapsto s(x),$$

which is surjective because $C_{X,x}$ contains in particular the germs of all constant functions. Let $\mathfrak{m}_x = \ker \mathrm{ev}_x = \{s \in C_{X,x} : s(x) = 0\}$. Then $\mathfrak{m}_x$ is a maximal ideal because $C_{X,x}/\mathfrak{m}_x \cong \mathbb{R}$ is a field. Let $s \in C_{X,x} \setminus \mathfrak{m}_x$ be represented by (U, f). Then $f(x) \neq 0$. By shrinking U we may assume that $f(y) \neq 0$ for all $y \in Y$ because f is continuous. Hence $1/f$ exists and s is a unit in $C_{X,x}$. Therefore the complement of $\mathfrak{m}_x$ consists of units of $C_{X,x}$. This shows that $C_{X,x}$ is a local ring with maximal ideal $\mathfrak{m}_x$. The same argument shows that for every open subspace X of a finite-dimensional $\mathbb{R}$-vector space the stalk $C^n_{X,x}$ is a local ring with residue field $\mathbb{R}$.

Now let $\varphi : \mathscr{F} \to \mathscr{G}$ be a morphism of presheaves on X, we then have an induced map $\varphi_x : \mathscr{F}_x \to \mathscr{G}_x$ defined by

$$\varphi_x := \varinjlim_{U \ni x} \varphi_U,$$

which sends the equivalence class of (U, f) in $\mathscr{F}_x$ to the class of $(U, \varphi_U(f))$ in $\mathscr{G}_x$. This defines a functor $\mathscr{F} \mapsto \mathscr{F}_x$ from the category of presheaves on X to the category of sets such that for every open neighborhood U of X one has a commutative diagram

$$\begin{tikzcd} \mathscr{F}(U) \arrow[r, "f \mapsto f_x"] \arrow[d, "\varphi_U"'] & \mathscr{F}_x \arrow[d, "\varphi_x"] \\ \mathscr{G}(U) \arrow[r, "g \mapsto g_x"] & \mathscr{G}_x \end{tikzcd} \tag{1.2.1}$$

Now we introduct a construction frequently apprears in the theory of sheaves. The **Godement construction**

$$\mathrm{God} : \mathbf{Psh}(X) \to \mathbf{Shv}(X)$$

is the functor given by sending a presheaf $\mathscr{F} \in \mathbf{PSh}(X)$ to the sheaf $\mathrm{God}(\mathscr{F})$ defined by sending an open set U to

$$\mathrm{God}(\mathscr{F})(U) := \prod_{x \in U} \mathscr{F}_x,$$

with the restriction morphisms given by product projections (it is easy to see this defines a sheaf on X). The assignment of God on morphisms is given by sending a morphism of presheaves $\phi : \mathscr{F} \to \mathscr{G}$ to the morphism

$$\mathrm{God}(\phi)_U : \prod_{x \in U} \mathscr{F}_x \to \prod_{x \in U} \mathscr{G}_x.$$

Proposition 19.1.9. *Let $\mathscr{F}$ be a sheaf of sets. For every open $U \subseteq X$ the map*

$$\mathscr{F}(U) \to \prod_{x \in U} \mathscr{F}_x, \quad s \mapsto (s_x)_{x \in U}.$$

identifies $\mathscr{F}(U)$ with the elements $(s_x)_{x\in U}$ with the property

> *For any $x \in U$ there exists a open subset V containing x and a section $s \in \mathscr{F}(V)$ such that for all $y \in V$ we have $s_y = (V, s)$ in $\mathscr{F}_y$.*

If an element (s_x) satisfies the condition above, we say it ***consists of compatible germs****. Thus the Godement construction identifies $\mathscr{F}$ as a subsheaf of* $\mathrm{God}(\mathscr{F})$.

Proof. Let $s, t \in \mathscr{F}(U)$ such that $s_x = t_x$ for all $x \in U$. Then for all $x \in U$ there exists an open neighborhood $V_x \subseteq U$ of x such that $s|_{V_x} = t|_{V_x}$. Clearly, $U = \bigcup_{x\in U} V_x$ and therefore $s = t$ by identity axiom.

Clearly any section s of $\mathscr{F}$ over U gives a choice of compatible germs for U. Conversely, if $(s_x)_{x\in U}$ consists of compatible germs, that is, there is an open cover $\{U_i\}$ of U, and sections $s_i \in \mathscr{F}(U_i)$, such that $(s_x)_{x\in U_i}$ is given by (U_i, s_i). Then by gluability there is a section $\sigma \in \mathscr{F}(U)$ such that $\sigma|_{U_i} = s_i$, and it is clear from the condition that $\sigma_x = s_x$. □

The importance of stalks is contained in the following result, which says a morphism between sheaves is determined by its value on stalks.

Proposition 19.1.10. *Let X be a topological space, $\mathscr{F}$ and $\mathscr{G}$ presheaves on X, and let $\varphi, \psi : \mathscr{F} \to \mathscr{G}$ be two morphisms of presheaves.*

(a) If $\mathscr{F}$ is a sheaf, the induced maps on stalks $\varphi_x : \mathscr{F}_x \to \mathscr{G}_x$ are injective for all $x \in X$ if and only of $\varphi_U : \mathscr{F}(U) \to \mathscr{G}(U)$ is injective for all open subsets $U \subseteq X$.

(b) If $\mathscr{F}$ and $\mathscr{G}$ are both sheaves, the maps $\varphi_x : \mathscr{F}_x \to \mathscr{G}_x$ are bijective for all $x \in X$ if and only of $\varphi_U : \mathscr{F}(U) \to \mathscr{G}(U)$ is injective for all open subsets $U \subseteq X$.

(c) If $\mathscr{F}$ and $\mathscr{G}$ are both sheaves, the morphism φ and ψ are equal if and only of $\varphi_x = \psi_x$ for all $x \in X$.

Proof. First we show that taking stalks preserves injectivity and surjectivity. Assume that φ_U is injective for all U. Let $s_0, t_0 \in \mathscr{F}_x$ such that $\varphi_x(s_0) = \varphi_x(t_0)$. Let s_0 be represented by (s, U) and t_0 by (t, V). By shrinking U and V we may assume $U = V$. From diagram (1.2.1), we see

$$\varphi_U(s)_x = \varphi_x(s_0) = \varphi_x(t_0) = \varphi_U(t)_x,$$

so there exists an open neighborhood $W \subseteq U$ containing such that

$$\varphi_W(s|_W) = (\varphi_U(s))|_W = (\varphi_U(t))|_W = \varphi_W(t|_W).$$

As φ_W is injective, we find $s|_W = t|_W$ and hence $s_0 = s_x = t_x = t_0$. Thus φ_x is injective. If on the other hand φ_U is surjective for all $U \subseteq X$, let t_0 be any elememt in $\mathscr{G}_x$, which is represented by (t, U). Then there is a $s \in \mathscr{F}(U)$ such that $\varphi_U(s) = t$, and (1.2.1) implies

$$\varphi_x(s_x) = \big(\varphi_U(s)\big)_x = t_x.$$

so φ_x is surjective.

For (a), assume that $\mathscr{F}$ is a sheaf, and consider the commutative diagram

$$\begin{tikzcd} \mathscr{F}(U) \arrow[r] \arrow[d, "\varphi_U"] & \prod_{x\in U} \mathscr{F}_x \arrow[d, "\prod_{x\in U}\varphi_x"] \\ \mathscr{G}(U) \arrow[r] & \prod_{x\in U} \mathscr{G}_x \end{tikzcd}$$

By Proposition 19.1.9 the map $\mathscr{F}(U) \to \prod_{x\in U} \mathscr{F}_x$ is injective, thus if φ_x are all injective, so is φ_U. Assertion (c) can also be derived from this diagram.

Then we prove (b). Assume φ_x are bijective, we show that φ_U is surjective. Let $t \in \mathscr{G}(U)$. For any $x \in U$, since φ_x is surjective, there exist $s_x \in \mathscr{F}_x$ such that $\varphi_x(s_x) = t_x$. Let s_x be represented by a section $s(x)$ on a neighborhood V_x of x. Then by (1.2.1),

$$\big(\varphi_{V_x}(s(x))\big)_x = \varphi_x(s_x) = (t|_{V_x})_x.$$

By shrinking V_x we may assume that $\varphi_{V_x}(s(x)) = t|_{V_x}$.

Now U is covered by such open sets V_x, and on each V_x we have a section $s(x) \in \mathscr{F}(V_x)$. For two distinct points $x, y \in U$, $s(x)|_{V_x\cap V_y}$ and $s(y)|_{V_x\cap V_y}$ are both sent to $t|_{V_x\cap V_y}$ by φ, so by the injectivity of φ we just proved, $s(x)|_{V_x\cap V_y} = s(y)|_{V_x\cap V_y}$. Therefore, the gulability axiom produces a section $s \in \mathscr{F}(U)$ such that $s|_{V_x} = s(x)$, and from diagram (1.1.1) and the construction, we have

$$\big(\varphi_U(s)\big)|_{V_x} = \varphi_{V_x}(s|_{V_x}) = \varphi_{V_x}(s(x)) = t|_{V_x},$$

so the identity axiom implies $\varphi_U(s) = t$. □

Definition 19.1.11. *Let $\mathscr{F}$ be a sheaf of abelian groups on a topological space X, $U \subseteq X$ open and $s \in \mathscr{F}(U)$ a section. The **support** of s is defined by*

$$\operatorname{supp}(s) = \{x \in U : s_x \neq 0\}.$$

*The **support** of $\mathscr{F}$ is defined to be*

$$\operatorname{supp}(\mathscr{F}) = \{x \in X : \mathscr{F}_x \neq 0\}.$$

Proposition 19.1.12. *Let $\mathscr{F}$ be a sheaf of abelian groups on a topological space, $U \subseteq X$ open, and $s \in \mathscr{F}(U)$ a section. Then* $\operatorname{supp}(s)$ *is closed in U.*

Proof. For $x \in U \setminus \operatorname{supp}(s)$ we have $s_x = 0$, so there exists an open subset $V \subseteq U$ with $s|_V = 0$. This implies $s_y = 0$ for every $y \in V$ and therefore $V \subseteq U \setminus \operatorname{supp}(s)$. Hence $U \setminus \operatorname{supp}(s)$ is open. □

Example 19.1.13. Let X be a topological space. Let C_X be the sheaf of continuous $\mathbb{R}$-valued functions on X. Let $U \subseteq X$ be open and $s \in C_X(U)$ a continuous function $U \to \mathbb{R}$. In the proof of Proposition 19.1.12 we have just seen that $U \setminus \operatorname{supp}(s)$ is the interior of $\{x \in U : s(x) = 0\}$. Therefore we have

$$\operatorname{supp}(s) = \overline{\{x \in U : s(x) \neq 0\}}$$

which coincides with usual definition of the support of a continuous function.

19.1.3 Sheafification

In this part, we give a functorial way to attach to a presheaf a sheaf. This can be seen as the left adjoint of the forgetful functor from $\mathbf{Shv}(X)$ to $\mathbf{Psh}(X)$.

Definition 19.1.14 (Universal property of sheafification). *If $\mathscr{F}$ is a presheaf on X, then a morphism of presheaves $\iota_{\mathscr{F}} : \mathscr{F} \to \mathscr{F}^{\#}$ on X is called a* ***sheafification*** *of $\mathscr{F}$ if $\mathscr{F}^{\#}$ is a sheaf, and for any sheaf $\mathscr{G}$, and any presheaf morphism $\varphi : \mathscr{F} \to \mathscr{G}$, there exists a unique morphism of sheaves $\tilde{\varphi} : \mathscr{F}^{\#} \to \mathscr{G}$ making the diagram*

$$\begin{tikzcd} \mathscr{F} \arrow[r, "\iota_{\mathscr{F}}"] \arrow[dr, "\varphi"'] & \mathscr{F}^{\#} \arrow[d, "\tilde{\varphi}"] \\ & \mathscr{G} \end{tikzcd}$$

commute.

As a universal construction, the sheafification functor $\mathscr{F} \to \mathscr{F}^{\#}$ is left-adjoint to the forgetful functor from sheaves on X to presheaves on X: there is a canonical isomorphism

$$\mathrm{Mor}_{\mathbf{Shv}(X)}(\mathscr{F}^{\#}, \mathscr{G}) \cong \mathrm{Mor}_{\mathbf{Psh}(X)}(\mathscr{F}, \mathscr{G})$$

for any presheaf $\mathscr{F}$ and sheaf $\mathscr{G}$.

In Proposition 19.1.9 we see that if $\mathscr{F}$ is a sheaf, then $\mathscr{F}(U)$ can be identified as elements in $\prod_{x \in U} \mathscr{F}_x$ consists of compatible germs. This turns out to be a appropriate way to define the sheafification.

Proposition 19.1.15. *Let $\mathscr{F}$ be a presheaf on a topological space X. Then there exists a sheafification $\iota_{\mathscr{F}} : \mathscr{F} \to \mathscr{F}^{\#}$ such that the following properties hold:*

(a) For all $x \in X$ the map on stalks $\iota_{\mathscr{F},x} : \mathscr{F}_x \to \mathscr{F}^{\#}_x$ is bijective.

(b) For every presheaf $\mathscr{G}$ on X and every morphism of presheaves $\varphi : \mathscr{F} \to \mathscr{G}$ there exists a unique morphism $\tilde{\varphi} : \mathscr{F}^{\#} \to \mathscr{G}^{\#}$ making the diagram commutes:

$$\begin{tikzcd} \mathscr{F} \arrow[r, "\iota_{\mathscr{F}}"] \arrow[d, "\varphi"'] & \mathscr{F}^{\#} \arrow[d, "\tilde{\varphi}"] \\ \mathscr{G} \arrow[r, "\iota_{\mathscr{G}}"] & \mathscr{G}^{\#} \end{tikzcd} \tag{1.3.1}$$

In particular, $\mathscr{F} \to \mathscr{F}^{\#}$ is a functor from the category of presheaves on X to the category of sheaves on X. The sheafification $\iota_{\mathscr{F}} : \mathscr{F} \to \mathscr{F}^{\#}$ is unique up to isomorphism.

Proof. Suppose $\mathscr{F}$ is a presheaf. Define $\mathscr{F}^{\#}$ by declearing $\mathscr{F}^{\#}(U)$ as the set of compatible germs of the presheaf $\mathscr{F}$ over U. Explicitly:

$$\begin{aligned} \mathscr{F}^{\#}(U) &= \{(s_x)_{x \in U} \in \prod_{x \in U} \mathscr{F}_x : (s_x)_{x \in U} \text{ consists of compatible germs}\} \\ &= \{(s_x)_{x \in U} \in \prod_{x \in U} \mathscr{F}_x : \forall x \in U, \exists V \subseteq U \text{ and } \tilde{s} \in \mathscr{F}(V) \text{ s.t. } \tilde{s}_y = s_x \text{ for all } y \in V\}. \end{aligned}$$

For $U \subseteq V$ the restriction map $\mathscr{F}^{\#}(V) \to \mathscr{F}^{\#}(U)$ is induced by the natural projection. With this,

for any covering $U = \bigcup_i U_i$ and sections $(s_x)_{x\in U_i}$ in $\mathscr{F}^\#$, the condition

$$\big((s_x)_{x\in U_i}\big)|_{U_i\cap U_j} = \big((s_x)_{x\in U_j}\big)|_{U_i\cap U_j}$$

implies that $(s_x)_{x\in U_i}$ and $(s_x)_{x\in U_j}$ have common germs on their common domains. Thus we can construct a unique section $(s_x)_{x\in U}$ by just gathering their germs. It is clear that such a section $(s_x)_{x\in U}$ has compatible germs, hence belongs to $\mathscr{F}^\#$. This shows $\mathscr{F}^\#$ is a sheaf. For $U \subseteq X$ open, we define $\iota_{\mathscr{F},U} : \mathscr{F}(U) \to \mathscr{F}^\#(U)$ by $s \mapsto (s_x)_{x\in U}$. The definition of $\mathscr{F}^\#$ shows that, for $x \in X$, $\mathscr{F}^\#_x = \mathscr{F}_x$ and that $\iota_{\mathscr{F},x}$ is the identity.

Now let $\mathscr{G}$ be a presheaf on X and let $\varphi : \mathscr{F} \to \mathscr{G}$ be a morphism. Sending $(s_x)_{x\in U}$ to $\big(\varphi_x(s_x)\big)_{x\in U}$ defines a morphism $\mathscr{F}^\# \to \mathscr{G}^\#$. By Proposition 19.1.10(c) this is the unique morphism making the diagram (1.3.1) commutative.

If we assume in addition that $\mathscr{G}$ is a sheaf, then the morphism of sheaves $\iota_{\mathscr{G}}$, which is bijective on stalks, is an isomorphism by Proposition 19.1.10(b). Composing the morphism $\mathscr{F}^\# \to \mathscr{G}^\#$ with $\iota_{\mathscr{G}}^{-1}$, we obtain the morphism $\tilde{\varphi} : \mathscr{F}^\# \to \mathscr{G}$. Finally, the uniqueness of $\iota_{\mathscr{F}} : \mathscr{F} \to \mathscr{F}^\#$ is a formal consequence of universal property. □

Proposition 19.1.16. *The sheafification of an injection (resp. surjection) of presheaves of sets is an injection (resp. surjection).*

Proof. This follows from the fact that sheafification does not change the stalk. □

From Proposition 19.1.10, we get the following characterization of the sheafification.

Proposition 19.1.17. *Let $\mathscr{F}$ be a presheaf and $\mathscr{G}$ be a sheaf. Then $\mathscr{G}$ is isomorphic to the sheafification of $\mathscr{F}$ if and only and if there exists a morphism $\iota : \mathscr{F} \to \mathscr{G}$ such that ι_x is bijective for all $x \in X$.*

Proof. One direction is trivial, assume the converse. Then there is a $\tilde{\iota} : \mathscr{F}^\# \to \mathscr{G}$ such that the following diagram commutes

$$\begin{tikzcd} \mathscr{F}^\# \arrow[r, "\tilde{\iota}"] & \mathscr{G} \\ \mathscr{F} \arrow[u] \arrow[ur, "\iota"'] & \end{tikzcd}$$

By Proposition 19.1.10 $\tilde{\iota}$ induced isomorphisms on stalks, hence is an isomorphism $\mathscr{F}^\# \cong \mathscr{G}$. □

Example 19.1.18. Let E be a set and let $\mathscr{F}$ be a presheaf of functions with values in E. Then its sheafification is given by

$$\mathscr{F}^\#(U) = \{f : U \to E \mid \exists \text{ open covering } (U_i)_i \text{ of } U \text{ such that } f|_{U_i} \in \mathscr{F}(U_i) \text{ for all } i\}.$$

Indeed, this is a sheaf by Example 19.1.6 and the inclusions $\mathscr{F}(U) \hookrightarrow \mathscr{F}^\#(U)$ for U open define a morphism of presheaves $\mathscr{F} \to \mathscr{F}^\#$ that is bijective on stalks. Hence we can apply Proposition 19.1.17.

Example 19.1.19. From the previous example, let's consider the constant presheaves. Let E_X be the sheaf of locally constant functions with values in E:

$$E_X = \{f : U \to E \mid \forall x \in U, \exists V \ni x \text{ open s.t. } f \text{ is constant on } V\}$$

then by Proposition 19.1.17, E_X is the sheafification of the presheaf of constant functions with values in E.

Example 19.1.20 (Open subset as a sheaf). Let $U \subseteq X$ be an open subset, then we can define a presheaf $\mathscr{U}$

$$\mathscr{U}(V) = \begin{cases} \{i_V\} & \text{if } V \subseteq U \\ \varnothing & \text{otherwise} \end{cases}$$

where $i_V : V \hookrightarrow U$ is the inclusion map. Let $\mathscr{U}^\#$ be its sheafification.

Let $\mathscr{F}$ be a sheaf and $s \in \mathscr{F}(U)$, then we can define a morphism φ_s by setting $\varphi_{s,U}(\mathbf{1}_U) = s$ and others by restriction. Then we get a map

$$\mathscr{F}(U) \to \mathrm{Mor}_{\mathbf{Psh}(X)}(\mathscr{U}, \mathscr{F})$$

which can be shown is an isomorphism. Together with the adjointness of sheafification, we get isomorphisms

$$\mathscr{F}(U) \cong \mathrm{Mor}_{\mathbf{Psh}(X)}(\mathscr{U}, \mathscr{F}) \cong \mathrm{Mor}_{\mathbf{Shv}(X)}(\mathscr{U}^\#, \mathscr{F}).$$

19.1.4 Direct and inverse images of sheaves

In this part $f : X \to Y$ denotes a continuous map of topological spaces. We will now see how to use f in order to attach to a sheaf on X a sheaf on Y (direct image) and to a sheaf on Y a sheaf an X (inverse image).

Definition 19.1.21 (Direct image of a presheaf). *Let $f : X \to Y$ be a continuous map. Let $\mathscr{F}$ be a presheaf on X. We define a presheaf $f_*\mathscr{F}$ on Y by (for $V \subseteq Y$ open)*

$$(f_*\mathscr{F})(V) = \mathscr{F}\left(f^{-1}(V)\right)$$

*the restriction maps given by the restriction maps for $\mathscr{F}$. Then $f_*\mathscr{F}$ is called the **direct image** of $\mathscr{F}$ under f or the **pushforward presheaf** of $\mathscr{F}$ by f. Whenever $\varphi : \mathscr{F}_1 \to \mathscr{F}_2$ is a morphism of presheaves, the family of maps $f_*(\varphi)_V := \varphi_{f^{-1}(V)}$ for $V \subseteq Y$ open is a morphism $f_*(\varphi) : f_*\mathscr{F}_1 \to f_*\mathscr{F}_2$. We thus obtain a functor f_* from the category of presheaves on X to the category of presheaves on Y.*

Proposition 19.1.22. *Let $f : X \to Y$ be a continuous map*

(a) If $\mathscr{F}$ is a sheaf on X, then $f_*\mathscr{F}$ is a sheaf on Y. Therefore f_* also defines a functor $f_* : \mathbf{Shv}(Y) \to \mathbf{Shv}(X)$.

(b) If $g : Y \to Z$ is a second continuous map, then $(g \circ f)_* = g_* \circ f_*$.

Proof. This first statement immediately follows from the fact that if $V = \bigcup V_i$ is an open covering in Y, then $f^{-1}(V) = \bigcup_i f^{-1}(V_i)$ is an open covering in X. The second claim is a computation:

$$(g \circ f)_*\mathscr{F}(W) = \mathscr{F}\left((g \circ f)^{-1}(W)\right) = \mathscr{F}\left(f^{-1} \circ g^{-1}(W)\right) = g_*\mathscr{F}\left(f^{-1}(W)\right) = g_* \circ f_*\mathscr{F}(W).$$

where $W \subseteq Y$ is open. □

We now define the inverse image of a sheaf. Let $\mathscr{G}$ be a presheaf of sets on Y. The **pullback presheaf** $f^p\mathscr{G}$ of a given presheaf $\mathscr{G}$ is defined as the left adjoint of the pushforward f_* on

presheaves. In other words, it should be a presheaf $f^p\mathscr{G}$ on X such that

$$\mathrm{Mor}_{\mathbf{Psh}(X)}(f^p\mathscr{G}, \mathscr{F}) \cong \mathrm{Mor}_{\mathbf{Psh}(X)}(\mathscr{G}, f_*\mathscr{F})$$

It turns out that this actually exists.

Proposition 19.1.23 (Inverse image of a presheaf). *Let $f : X \to Y$ be a continuous map and let $\mathscr{G}$ be a presheaf on Y. There exists a functor $f^p : \mathbf{Psh}(Y) \to \mathbf{Psh}(X)$ which is left adjoint to f_*. For a presheaf $\mathscr{G}$ it is determined by*

$$f^p\mathscr{G}(U) = \varinjlim_{\substack{V \supseteq f(U) \\ V \subseteq Y \text{ open}}} \mathscr{G}(V).$$

the restriction maps being induced by the restriction maps of $\mathscr{G}$.

Proof. The colimit is over the partially ordered set consisting of open subset $V \subseteq Y$ which contain $f(U)$ with ordering by reverse inclusion. This is a directed partially ordered set, and if $U_1 \subseteq U_2$, then every open neighbourhood of $f(U_2)$ is an open neighbourhood of $f(U_1)$. Hence the system defining $f^p\mathscr{G}(U_2)$ is a subsystem of the one defining $f^p\mathscr{G}(U_1)$ and we obtain a restriction map. Note that the construction of the colimit is clearly functorial in $\mathscr{G}$, and similarly for the restriction mappings. Hence we have defined f^p as a functor. Now we turn to the proof of the adjointness. For this, we need to define the unit map and the counit map, as follows.

- There exists a canonical map $\mathscr{G}(V) \to f^p\mathscr{G}\big(f^{-1}(V)\big)$ for any open subset $V \subseteq Y$, because the system of open neighbourhoods of $f\big(f^{-1}(V)\big)$ contains the element V:

$$\rho_{\mathscr{G},V} : \mathscr{G}(V) \longrightarrow f^p\mathscr{G}(f^{-1}(V)) = \varinjlim_{U \supseteq f(f^{-1}(V))} \mathscr{G}(U)$$

  This is compatible with restriction mappings, so there is a canonical map $\rho_{\mathscr{G}} : \mathscr{G} \to f_*f^p\mathscr{G}$.

- There exists a canonical map $f^pf_*\mathscr{F}(U) \to \mathscr{F}(U)$ for any open subset $U \subseteq X$:

$$\sigma_{\mathscr{F},U} : f^pf_*\mathscr{F}(U) = \varinjlim_{V \supseteq f(U)} \mathscr{F}(f^{-1}(V)) \longrightarrow \mathscr{F}(U)$$

  where the map is given by the restriction of $\mathscr{F}(f^{-1}(V))$ to $\mathscr{F}(U)$. One easily verifies that the maps are compatible with restriction maps and thus there is a canonical map $\sigma_{\mathscr{F}} : f^pf_*\mathscr{F} \to \mathscr{F}$.

The maps we get are illustrated in the following diagram:

$$\begin{tikzcd}
X \arrow[d, "f"] & & & \\
Y & & f^p\mathscr{G} \arrow[r, "\psi"'] \arrow[rr, bend left, "f^p\varphi"] \arrow[dl, dashed] & \mathscr{F} \arrow[d, dashed] & f^pf_*\mathscr{F} \arrow[l, "\sigma_{\mathscr{F}}"'] \arrow[dl, dashed] \\
& f_*f^p\mathscr{G} \arrow[rr, bend right, "f_*\psi"'] & \mathscr{G} \arrow[l, "\rho_{\mathscr{G}}"'] \arrow[r, "\varphi"] \arrow[u, dashed] & f_*\mathscr{F} &
\end{tikzcd}$$

Now let $\mathscr{F}$ be a presheaf of sets on X. Suppose that $\psi : f^p\mathscr{G} \to \mathscr{F}$ is a map of presheaves of sets. The corresponding map $\psi^\flat : \mathscr{G} \to f_*\mathscr{F}$ is the composition

$$\psi^\flat : \mathscr{G} \xrightarrow{\rho_{\mathscr{G}}} f_*f^p\mathscr{G} \xrightarrow{f_*\psi} f_*\mathscr{F}$$

Suppose that $\varphi : \mathcal{G} \to f_*\mathcal{F}$ is a map of presheaves of sets. The map $\varphi^\sharp : f^p\mathcal{G} \to \mathcal{F}$ is then the composition

$$\varphi^\sharp : f^p\mathcal{G} \xrightarrow{f^p\varphi} f^p f_*\mathcal{F} \xrightarrow{\sigma_{\mathcal{F}}} \mathcal{F}$$

It can be verified that these tow maps are inverse of each other. Let $U \subseteq X$, then the map $(\psi^\flat)^\sharp : f^p\mathcal{G} \to \mathcal{F}$ is given by

$$f^p\mathcal{G}(U) = \varinjlim_{V \supseteq f(U)} \mathcal{G}(V) \to \varinjlim_{V \supseteq f(U)} \varinjlim_{V' \supseteq f(f^{-1}(V))} \mathcal{G}(V') \xrightarrow{\psi_{f^{-1}(V)}} \varinjlim_{V \supseteq f(U)} \mathcal{F}(f^{-1}(V)) \xrightarrow{\mathrm{res}^*_U} \mathcal{F}(U)$$

Let $s \in f^p\mathcal{G}(U)$ be represented by $v \in \mathcal{G}(V)$ for some $V \supseteq f(U)$. Since $f^{-1}(V) \supseteq U$, from the diagram

$$\begin{tikzcd} f^p\mathcal{G}(f^{-1}(V)) \arrow[r, "\psi_{f^{-1}(V)}"] \arrow[d, "\mathrm{res}_U^{f^{-1}(V)}"'] & \mathcal{F}(f^{-1}(V)) \arrow[d, "\mathrm{res}_U^{f^{-1}(V)}"] \\ f^p\mathcal{G}(U) \arrow[r, "\psi_U"] & \mathcal{F}(U) \end{tikzcd}$$

we obtain

$$\begin{aligned} (\psi^\flat)^\sharp(s) &= \mathrm{res}^*_U\big[\psi_{f^{-1}(V)}\big([v]_{f^{-1}(V)}\big)\big]_U = \mathrm{res}_U^{f^{-1}(V)} \circ \psi_{f^{-1}(V)}\big([v]_{f^{-1}(V)}\big) \\ &= \psi_U\big(\mathrm{res}_U^{f^{-1}(V)}([v]_{f^{-1}(V)})\big) = \psi_U([v]_U) = \psi_U(s). \end{aligned}$$

Thus $(\psi^\flat)^\sharp = \psi$. A similar argument gives $(\varphi^\sharp)^\flat = \varphi$, hence we are done. □

Remark 19.1.4. We will almost never use the concrete description of $f^p\mathcal{G}$ in the sequel. Very often we are given f, $\mathcal{F}$, and $\mathcal{G}$ as in the Proposition 19.1.23, and a morphism of sheaves $\varphi : \mathcal{G} \to f_*\mathcal{F}$. Then usually it will be sufficient to understand for each $x \in X$ the map

$$\varphi^\sharp_x : (f^p\mathcal{G})_x = \mathcal{G}_{f(x)} \to \mathcal{F}_x$$

induced by $\varphi^\sharp : f^p\mathcal{G} \to \mathcal{F}$ on stalks. The proof of Proposition 19.1.23 shows that we can describe this map in terms of as follows. For every open neighborhood $V \subseteq Y$ of $f(x)$, we have maps

$$\mathcal{G}(V) \xrightarrow{\varphi_V} \mathcal{F}(f^{-1}(V)) \longrightarrow \mathcal{F}_x$$

and taking the colimit over all V we obtain the map $\varphi^\sharp_x : \mathcal{G}_{f(x)} \to \mathcal{F}_x$.

Proposition 19.1.24. *Let $f : X \to Y$ be a continuous map. Let $x \in X$. Let $\mathcal{G}$ be a presheaf of sets on Y. There is a canonical bijection of stalks $(f^p\mathcal{G})_x = \mathcal{G}_{f(x)}$.*

Proof. This is obtained as follows

$$(f^p\mathcal{G})_x = \varinjlim_{U \ni x} f^p\mathcal{G}(U) = \varinjlim_{U \ni x} \varinjlim_{V \supseteq f(U)} \mathcal{G}(V) = \varinjlim_{V \ni f(x)} \mathcal{G}(V) = \mathcal{G}_{f(x)}.$$

Here we have used the fact that any V open in Y containing $f(x)$ occurs in the description above. The case for sheaves is obtained from Proposition 19.1.15. □

Let $\mathcal{G}$ be a sheaf of sets on Y. The **pullback sheaf** $f^{-1}\mathcal{G}$ is defined by the formula

$$f^{-1}\mathcal{G} = (f^p\mathcal{G})^{\#}.$$

Sheafification is a left adjoint to the inclusion of sheaves in presheaves, and f^p is a left adjoint to f_* on presheaves. As a formal consequence we obtain that f^{-1} is a left adjoint of pushforward on sheaves: for sheaves $\mathcal{F}$ and $\mathcal{G}$, we have

$$\begin{aligned}\mathrm{Mor}_{\mathbf{Shv}(X)}(f^{-1}\mathcal{G},\mathcal{F}) &= \mathrm{Mor}_{\mathbf{Shv}(X)}\big((f^p\mathcal{G})^{\#},\mathcal{F}\big) \cong \mathrm{Mor}_{\mathbf{Psh}(X)}\big(f^p\mathcal{G},\mathcal{F}\big)\\ &\cong \mathrm{Mor}_{\mathbf{Psh}(X)}(\mathcal{G},f_*\mathcal{F}) = \mathrm{Mor}_{\mathbf{Shv}(X)}(\mathcal{G},f_*\mathcal{F})\end{aligned}$$

Proposition 19.1.25. *There are canonical maps*

$$f^{-1}f_*\mathcal{F} \to \mathcal{F}, \quad \mathcal{G} \to f_*f^{-1}\mathcal{G}$$

for sheaves $\mathcal{F}$ on X and $\mathcal{G}$ on Y.

Proof. We already have maps

$$\sigma_{\mathcal{F}} : f^pf_*\mathcal{F} \to \mathcal{F}, \quad \rho_{\mathcal{G}} : \mathcal{G} \to f^pf_*\mathcal{G}.$$

The map $f^{-1}f_*\mathcal{F} \to \mathcal{F}$ is given by the universal property of sheafification:

$$\begin{tikzcd} f^pf_*\mathcal{F} \arrow[r, "sh"] \arrow[dr, "\sigma_{\mathcal{F}}"'] & f^{-1}f_*\mathcal{F} \arrow[d, dashed] \\ & \mathcal{F} \end{tikzcd}$$

and the map $\mathcal{G} \to f_*f^{-1}\mathcal{G}$ is given by the composition

$$\mathcal{G}(V) \xrightarrow{\rho_{\mathcal{G},V}} f^p\mathcal{G}(f^{-1}(V)) \xrightarrow{sh} f^{-1}\mathcal{G}(f^{-1}(V))$$

for $V \subseteq Y$ open. □

Proposition 19.1.26 (Inverse image and composition). *Let $f : X \to Y$ and $g : Y \to Z$ be continuous maps of topological spaces. The functors $(g \circ f)^{-1}$ and $f^{-1} \circ g^{-1}$ are canonically isomorphic. Similarly $(g \circ f)^p \cong f^p \circ g^p$ on presheaves.*

Proof. This comes from the formal consequence

$$\begin{aligned}\mathrm{Mor}_{\mathbf{Psh}(X)}\big((g\circ f)^p\mathcal{G},\mathcal{F}\big) &\cong \mathrm{Mor}_{\mathbf{Psh}(X)}\big(\mathcal{G},(g\circ f)_*\mathcal{F}\big) = \mathrm{Mor}_{\mathbf{Psh}(X)}\big(\mathcal{G},g_*\circ f_*\mathcal{F}\big)\\ &\cong \mathrm{Mor}_{\mathbf{Psh}(X)}\big(g^p\mathcal{G},f_*\mathcal{F}\big) \cong \mathrm{Mor}_{\mathbf{Psh}(X)}\big(f^p\circ g^p\mathcal{G},\mathcal{F}\big)\end{aligned}$$

By the uniqueness of adjoint functors, we obtain $(g \circ f)^p \cong f^p \circ g^p$. A similar computation holds for $(g \circ f)^{-1}$. □

To conclude this part, we use the direct image functor to produce an adjoint of the stalk functor. First, we need the following concept of a skyscraper sheaf.

Definition 19.1.27. *Let $x \in X$ be a point. Denote $i_x : \{x\} \mapsto X$ the inclusion map. Let A be a set and think of A as a sheaf on the one point space $\{x\}$. We define the* ***skyscraper sheaf*** *at x with value A as the pushforward sheaf $i_{x,*}A$. Explicitly,*

$$i_{x,*}A(U) = \begin{cases} A & \text{if } x \in U, \\ \varnothing & \text{if } x \notin U. \end{cases}$$

We say a sheaf $\mathscr{F}$ is a skyscraper sheaf if $\mathscr{F} \cong i_{x,*}A$ for some $x \in X$ and a set A.

Lemma 19.1.28. *Let X be a topological space, $x \in X$ a point, and A a set. For any point $y \in X$ the stalk of the skyscraper sheaf at x with value A at y is*

$$(i_{x,*}A)_y = \begin{cases} A & \text{if } y \in \overline{\{x\}} \\ \{*\} & \text{otherwise} \end{cases}$$

Proof. If $x \notin \overline{\{x\}}$, then there exist arbitrarily small open neighbourhoods U of y which do not contain x. Because $\mathscr{F}$ is a sheaf we have $\mathscr{F}(i_x^{-1}(U)) = \{*\}$ for any such U. □

Proposition 19.1.29. *Let X be a topological space, and let $x \in X$ be a point. The functors $\mathscr{F} \mapsto \mathscr{F}_x$ and $A \mapsto i_{x,*}A$ are adjoint. In a formula,*

$$\mathrm{Mor}_{\mathbf{Set}}(\mathscr{F}_x, A) \cong \mathrm{Mor}_{\mathbf{Shv}(X)}(\mathscr{F}, i_{x,*}A)$$

Proof. Consider the pull back functor of the map $i_x : \{x\} \to X$: for a sheaf $\mathscr{F}$ on X,

$$i_x^{-1}\mathscr{F}(\{x\}) = \varinjlim_{U \ni x} \mathscr{F}(U),$$

which is exactly the stalk of $\mathscr{F}$ at x. Thus the adjointness comes from that of i_x^{-1} and $i_{x,*}$. □

19.1.5 Open immersions and closed immersions

19.1.5.0.1 Open immersions and sheaves Let $j : U \hookrightarrow X$ be an open immersion (that is, an embedded of U into an open subset of X). It turns out that there is a functor $j_!$ which is left adjoint to j^{-1}, so that we get a triple $(j_!, j^{-1}, j_*)$ in which each consecutive pair is an adjunction and j^{-1} is exact. But first let us point out that j^{-1} has a particularly simple description in the case of an open immersion.

Proposition 19.1.30. *Let X be a topological space. Let $j : U \to X$ be the inclusion of an open subset U into X.*

(a) Let $\mathscr{G}$ be a presheaf of sets on X. The presheaf $j^p\mathscr{G}$ is given by the rule $V \mapsto \mathscr{G}(V)$ for $V \subseteq U$ open.

(b) Let $\mathscr{G}$ be a sheaf of sets on X. The sheaf $j^{-1}\mathscr{G}$ is given by the rule $V \mapsto \mathscr{G}(V)$ for $V \subseteq U$ open.

(c) On the category of presheaves of U we have $j^p j_* = \mathbf{1}$, and on the category of sheaves of U we have $j^{-1}j_* = \mathbf{1}$.

Proof. Note that $j^{-1}j_*\mathscr{F}(V) = j^p j_*\mathscr{F}(V) = \mathscr{F}(V)$ for open subsets $V \subseteq U$, so the claims follow immediately. □

Definition 19.1.31. *Let X be a topological space. Let $j : U \to X$ be the inclusion of an open subset.*

- *Let $\mathscr{G}$ be a presheaf of sets on X. The presheaf $j^p\mathscr{G}$ is called the* ***restriction*** *of $\mathscr{G}$ to U and denoted $\mathscr{G}|_U$.*
- *Let $\mathscr{G}$ be a sheaf of sets on X. The presheaf $j^{-1}\mathscr{G}$ is called the* ***restriction*** *of $\mathscr{G}$ to U and denoted $\mathscr{G}|_U$.*

Definition 19.1.32. *Let X be a topological space. Let $j : U \hookrightarrow X$ be the inclusion of an open subset.*

(a) Let $\mathscr{F}$ be a presheaf of sets on U. We define the ***extension of $\mathscr{F}$ by the empty set*** *$j_{p!}\mathscr{F}$ to be the presheaf of sets on X defined by the rule*

$$j_{p!} = \begin{cases} \mathscr{F}(V) & \text{if } V \subseteq U, \\ \varnothing & \text{otherwise.} \end{cases}$$

with obvious restriction mappings.

(b) Let $\mathscr{F}$ be a sheaf of sets on U. We define the ***extension of $\mathscr{F}$*** *by the empty set $j_!\mathscr{F}$ to be the sheafification of the presheaf $j_{p!}\mathscr{F}$.*

Proposition 19.1.33. *Let X be a topological space. Let $j : U \to X$ be the inclusion of an open subset.*

(a) The functor $j_{p!}$ is a left adjoint to the restriction functor j^p:

$$\mathrm{Mor}_{\mathbf{Psh}(X)}(j_{p!}\mathscr{F}, \mathscr{G}) \cong \mathrm{Mor}_{\mathbf{Psh}(U)}(\mathscr{F}, j^p\mathscr{G}) = \mathrm{Mor}_{\mathbf{Psh}(X)}(\mathscr{F}, \mathscr{G}|_U).$$

(b) The functor $j_!$ is a left adjoint to restriction,

$$\mathrm{Mor}_{\mathbf{Shv}(X)}(j_!\mathscr{F}, \mathscr{G}) \cong \mathrm{Mor}_{\mathbf{Shv}(U)}(\mathscr{F}, j^{-1}\mathscr{G}) = \mathrm{Mor}_{\mathbf{Shv}(U)}(\mathscr{F}, \mathscr{G}|_U).$$

(c) Let $\mathscr{F}$ be a sheaf of sets on U. The stalks of the sheaf $j_!\mathscr{F}$ are described as follows

$$(j_!\mathscr{F})_x = \begin{cases} \mathscr{F}_x & \text{if } x \in U, \\ \varnothing & \text{otherwise.} \end{cases}$$

Therefore the functor $j_!$ is exact.

(e) On the category of presheaves of U we have $j^p j_{p!} = \mathbf{1}$, and on the category of sheaves of U we have $j^{-1}j_! = \mathbf{1}$.

Proof. To map $j_{p!}\mathscr{F}$ into $\mathscr{G}$ it is enough to map $\mathscr{F}(V) \to \mathscr{G}(V)$ whenever $V \subseteq U$ compatibly with restriction mappings. And the same description holds for maps $\mathscr{F} \mapsto \mathscr{G}|_U$. The adjointness of $j_!$ and restriction follows from this and the properties of sheafification. The identification of stalks is obvious from the definition of the extension by the empty set and the definition of a stalk.

Finally, if $\mathscr{F}$ is a sheaf on U, consider the canonical maps

$$\mathscr{F} \mapsto j^p j_{p!}\mathscr{F}, \quad \mathscr{F} \mapsto j^{-1} j_! \mathscr{F}.$$

Since the induced maps on stalks are isomorphisms, the claim follows. □

Theorem 19.1.34. *Let X be a topological space. Let $j : U \to X$ be the inclusion of an open subset. The functor*

$$j_! : \mathbf{Shv}(U) \to \mathbf{Shv}(X)$$

is fully faithful. Its essential image consists exactly of those sheaves $\mathscr{G}$ whose support is contained in U.

Proof. Fully faithfulness follows formally from $j^{-1} j_! = \mathbf{1}$. We have seen that any sheaf in the image of the functor has the property on the stalks mentioned in the lemma. Conversely, suppose that $\mathscr{G}$ has the indicated property, then the canonical map

$$j_! j^{-1} \mathscr{G} \to \mathscr{G}$$

is an isomorphism on all stalks and hence an isomorphism. □

19.1.5.0.2 Closed immersions and sheaves Let X be a topological space. Let $i : Z \to X$ be the inclusion of a closed subset Z into X. In a similar fashion, we can extend the adjunction (i^{-1}, i_*). First we state an important result for the direct image i_*.

Lemma 19.1.35. *Let X be a topological space. Let $i : Z \hookrightarrow X$ be the inclusion of a closed subset Z into X. Let $\mathscr{F}$ be a sheaf of sets on Z. The stalks of $i_*\mathscr{F}$ are described By*

$$(i_*\mathscr{F})_x = \begin{cases} \mathscr{F}_x & x \in Z, \\ \{*\} & \textit{otherwise}. \end{cases}$$

Proof. This follows from the definition of $i_*\mathscr{F}$, and the fact that Z is closed. □

Theorem 19.1.36. *Let X be a topological space. Let $i : Z \to X$ be the inclusion of a closed subset. The functor*

$$i_* : \mathbf{Shv}(Z) \to \mathbf{Shv}(X)$$

is fully faithful. Its essential image consists exactly of those sheaves $\mathscr{G}$ whose support is contained in Z. The functor i^{-1} is a left inverse to i_*.

Proof. Fully faithfulness follows formally from $i^{-1} i_* = \mathbf{1}$. We have seen that any sheaf in the image of the functor has the property on the stalks mentioned in the lemma. Conversely, suppose that $\mathscr{G}$ has the indicated property. Then the map $\mathscr{G} \to i_* i^{-1} \mathscr{G}$ is an isomorphism on stalks, and hence an isomrophism. □

Now we define the functor $i^!$ for a closed immersion.

Proposition 19.1.37. *Let X be a topological space. Let $Z \subseteq X$ be a closed subset. Let $\mathscr{F}$ be a sheaf on X. Define a sheaf $\mathscr{H}_Z(\mathscr{F})$ by*

$$\Gamma(U, \mathscr{H}_Z(\mathscr{F})) = \{s \in \mathscr{F}(U) : \operatorname{supp}(s) \subseteq Z \cap U\}.$$

Then $\mathscr{H}_Z(\mathscr{F})$ is a subsheaf of $\mathscr{F}$. It is the largest subsheaf of $\mathscr{F}$ whose support is contained in Z. The construction $\mathscr{F} \mapsto \mathscr{H}_Z(\mathscr{F})$ is functorial in the sheaf $\mathscr{F}$.

Proof. □

Definition 19.1.38. *Let $i : Z \to X$ be the inclusion of a closed subset. For a sheaf $\mathscr{F}$ on X, define the* ***inverse image of $\mathscr{F}$ supported on Z*** *to be the sheaf $i^!\mathscr{F} = i^{-1}\mathscr{H}_Z(\mathscr{F})$.*

Proposition 19.1.39. *For a closed immersion $i : Z \hookrightarrow X$, the functor $i^!$ is right adjoint to i_*. In a formula*

$$\mathrm{Mor}_{\mathbf{Shv}(X)}(i_*\mathscr{G}, \mathscr{F}) = \mathrm{Mor}_{\mathbf{Shv}(Z)}(\mathscr{G}, i^!\mathscr{F})$$

Proof. Note that $i_*i^!\mathscr{F} = \mathscr{H}_Z(\mathscr{F})$ by Theorem 19.1.36. Since i_* is fully faithful we are reduced to showing that

$$\mathrm{Mor}_{\mathbf{Shv}(X)}(i_*\mathscr{G}, \mathscr{F}) = \mathrm{Mor}_{\mathbf{Shv}(Z)}(i_*\mathscr{G}, \mathscr{H}_Z(\mathscr{F})).$$

This follows since the support of the image via any homomorphism of a section of $i_*\mathscr{G}$ is contained in Z, by Theorem 19.1.36. □

Proposition 19.1.40. *Let $i : Z \hookrightarrow X$ be a closed embedding, set $U = Z^c$ and let $j : U \hookrightarrow X$ be the corresponding open embedding. Then for any sheaf $\mathscr{F}$ on X, the sequence*

$$0 \longrightarrow j_!j^{-1}\mathscr{F} \longrightarrow \mathscr{F} \longrightarrow j_*j^{-1}\mathscr{F} \longrightarrow 0$$

is exact. Moreover, for any morphism $\varphi : \mathscr{F} \to \mathscr{G}$ of sheaves on X we obtain a morphism of short exact sequences

$$\begin{tikzcd}
0 \arrow[r] & j_!j^{-1}\mathscr{F} \arrow[r] \arrow[d] & \mathscr{F} \arrow[r] \arrow[d] & j_*j^{-1}\mathscr{F} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & j_!j^{-1}\mathscr{G} \arrow[r] & \mathscr{G} \arrow[r] & j_*j^{-1}\mathscr{G} \arrow[r] & 0
\end{tikzcd}$$

Proof. The functoriality of the short exact sequence is immediate from the naturality of the adjunction mappings. We may check exactness on stalks: for $x \in X$, the sequence is

$$\begin{cases} 0 \to \mathscr{F}_x \to \mathscr{F}_x \to 0 \to 0 & x \in U, \\ 0 \to 0 \to \mathscr{F}_x \to \mathscr{F}_x \to 0 & x \in Z. \end{cases}$$

so the claim follows. □

19.1.6 Glueing sheaves

It is quite often that we want to glue a bunch of objects defined on the members of a covering of X to create a new one. In this paragraph we will see how to do this for morphisms and sheaves.

Proposition 19.1.41. *Let X be a topological space. Let $X = \bigcup_i U_i$ be an open covering. Let $\mathscr{F}, \mathscr{G}$ be sheaves of sets on X. Given a collection*

$$\varphi_i : \mathscr{F}|_{U_i} \to \mathscr{G}|_{U_i}$$

of maps of sheaves such that for all $i, j \in I$ the maps φ_i, φ_j restrict to the same map $\mathscr{F}|_{U_i \cap U_j} \to \mathscr{G}|_{U_i \cap U_j}$, there exists a unique map of sheaves

$$\varphi : \mathscr{F} \to \mathscr{G}$$

whose restriction to each U_i agrees with φ_i.

Proof. For $V \subseteq X$ open, we have $V = \bigcup_i (V \cap U_i)$, so for $s \in \mathscr{F}(V)$ we define $\varphi_V(s)$ by the equations

$$\big(\varphi_V(s)\big)|_{V \cap U_i} = (\varphi_i)_{V \cap U_i}(s|_{V \cap U_i}) \quad \text{for} \quad i \in I. \tag{1.6.1}$$

By the condition of sheaf, this is well-defined, and indeed defines a morphism of sheaves. It is clear that φ restrict to φ_i on each U_i. To see the uniqueness, if $\psi : \mathscr{F} \to \mathscr{G}$ is another morphism restricting to φ_i on each i, then for each $s \in \mathscr{F}(U)$, $\psi(s)$ also satisfies (1.6.1), so it must coincides with $\varphi(s)$ by the condition of sheaf. This shows $\varphi = \psi$, as desired. □

The previous proposition implies that given two sheaves $\mathscr{F}, \mathscr{G}$ on the topological space X the rule

$$U \mapsto \mathrm{Mor}_{\mathbf{Shv}(X)}(\mathscr{F}|_U, \mathscr{G}|_U)$$

defines a sheaf. This is a kind of **internal hom sheaf**. It is seldom used in the setting of sheaves of sets, and more usually in the setting of sheaves of modules.

Let X be a topological space. Let $X = \bigcup_i U_i$ be an open covering. For each $i \in I$ let $\mathscr{F}_i$ be a sheaf of sets on U_i. For each pair $i, j \in I$, let

$$\varphi_{ij} : \mathscr{F}_i|_{U_i \cap U_j} \to \mathscr{F}_j|_{U_i \cap U_j}$$

be an isomorphism of sheaves of sets. Assume in addition that for every triple of indices $i, j, k \in I$ the following diagram is commutative

$$\begin{tikzcd}
\mathscr{F}_i|_{U_i \cap U_j \cap U_k} \arrow[rr, "\varphi_{ik}"] \arrow[dr, "\varphi_{ij}"'] & & \mathscr{F}_k|_{U_i \cap U_j \cap U_k} \\
& \mathscr{F}_j|_{U_i \cap U_j \cap U_k} \arrow[ur, "\varphi_{jk}"'] &
\end{tikzcd}$$

We will call such a collection of data $(\mathscr{F}_i, \varphi_{ij})$ a **glueing data** for sheaves of sets with respect to the covering $X = \bigcup_i X_i$.

Proposition 19.1.42. *Let X be a topological space. Let $X = \bigcup_i U_i$ be an open covering. Given any glueing data $(\mathscr{F}_i, \varphi_{ij})$ for sheaves of sets with respect to the covering, there exists a sheaf of sets $\mathscr{F}$ on X together with isomorphisms*

$$\varphi_i : \mathscr{F}|_{U_i} \to \mathscr{F}_i$$

such that the diagrams

$$\begin{tikzcd}
\mathscr{F}|_{U_i \cap U_j} \arrow[r, "\varphi_i"] \arrow[d, equal] & \mathscr{F}_i|_{U_i \cap U_j} \arrow[d, "\varphi_{ij}"] \\
\mathscr{F}|_{U_i \cap U_j} \arrow[r, "\varphi_j"] & \mathscr{F}_j|_{U_i \cap U_j}
\end{tikzcd}$$

are commutative.

Proof. Actually we can write a formula for the set of sections of $\mathscr{F}$ over an open $W \subseteq X$. Namely, we define

$$\mathscr{F}(W) = \{(s_i)_{i\in I} \mid s_i \in \mathscr{F}_i(W \cap U_i) \text{ and } \varphi_{ij}(s_i|_{W\cap U_i\cap U_j}) = s_j|_{W\cap U_i\cap U_j}\}.$$

Restriction mappings for $W' \subseteq W$ are defined by the restricting each of the (s_i) to $W' \cap U_i$. The sheaf condition for $\mathscr{F}$ follows immediately from the sheaf condition for each of the $\mathscr{F}_i$.

We still have to prove that $\mathscr{F}|_{U_i}$ maps isomorphically to $\mathscr{F}_i$. Let $W \subseteq U_i$; then the commutativity of the diagrams in the definition of a glueing data assures that we may start with any section $s \in \mathscr{F}_i(W)$ and obtain a compatible collection by setting $s_i = s$ and $s_j = \varphi_{ij}(s_i|_{W\cap U_j})$. Thus the claim follows. □

Corollary 19.1.43. *Let X be a topological space. Let $X = \bigcup_i U_i$ be an open covering. The functor which associates to a sheaf of sets $\mathscr{F}$ the following collection of glueing data*

$$\left(\mathscr{F}|_{U_i}, (\mathscr{F}_i)|_{U_i\cap U_j} \to (\mathscr{F}_j)|_{U_i\cap U_j}\right)$$

with respect to the covering $X = \bigcup_i U_i$ defines an equivalence of categories between **Shv**(X) *and the category of glueing data.*

This result means that if the sheaf $\mathscr{F}$ was constructed from the glueing data $(\mathscr{F})_i, \varphi_{ij})$ and if $\mathscr{G}$ is a sheaf on X, then a morphism $f : \mathscr{F} \to \mathscr{G}$ is given by a collection of morphisms of sheaves

$$f_i : \mathscr{F}_i \to \mathscr{G}$$

compatible with the glueing maps φ_{ij}. Similarly, to give a morphism of sheaves $g : \mathscr{G} \to \mathscr{F}$ is the same as giving a collection of morphisms of sheaves

$$g_i : \mathscr{G}|_{U_i} \to \mathscr{F}_i$$

compatible with the glueing maps φ_{ij}.

19.1.7 Preheaves and sheaves over a basis

Sometimes there exists a basis for the topology consisting of opens that are easier to work with than general opens. For convenience we give here some definitions and simple lemmas in order to facilitate working with (pre)sheaves in such a situation.

Let X be a topological space. Let $\mathcal{B}$ be a basis for the topology on X. A **presheaf $\mathscr{F}$ of sets on $\mathcal{B}$** is a rule which assigns to each $U \in \mathcal{B}$ a set $\mathscr{F}(U)$ and to each inclusion $V \subseteq U$ of elements of $\mathcal{B}$ a map $\mathrm{res}^U_V : \mathscr{F}(U) \to \mathscr{F}(V)$ such that whenever $W \subseteq V \subseteq U$ in $\mathcal{B}$ we have $\mathrm{res}^U_V \circ \mathrm{res}^V_W = \mathrm{res}^U_W$. If $\mathscr{F}$ be a presheaf over the basis $\mathcal{B}$. We can associate $\mathscr{F}$ with a sheaf $\mathscr{F}_{\mathcal{B}}$ by defining

$$\mathscr{F}_{\mathcal{B}}(U) = \{(s_V) \in \prod_{\substack{V\in\mathcal{B}\\ V\subseteq U}} \mathscr{F}(V) : \text{for all } W, V \in \mathcal{B}, W \subseteq V, s_V|_W = s_W\} = \varprojlim_{\substack{V\in\mathcal{B}\\ V\subseteq U}} \mathscr{F}(V). \tag{1.7.1}$$

for any open subset U of X. If U and U' are two open sets of X such that $U \subseteq U'$, we define $\mathrm{res}^{U'}_U$ as the inverse limit (for $V \subseteq U$) of the canonical morphisms $\mathscr{F}_{\mathcal{B}}(U') \to \mathscr{F}(V)$, in other

words, the unique morphism $\mathscr{F}_{\mathcal{B}}(U') \to \mathscr{F}_{\mathcal{B}}(U)$ which, composed with the canonical morphisms $\mathscr{F}_{\mathcal{B}}(U) \to \mathscr{F}(V)$, gives the canonical morphisms $\mathscr{F}_{\mathcal{B}}(U') \to \mathscr{F}(V)$; it is then immediate that the transitivity holds. Moreover, if $U \in \mathcal{B}$, the canonical morphism $\mathscr{F}_{\mathcal{B}}(U) \to \mathscr{F}(U)$ is an isomorphism, allowing us to identify these two sets.

Proposition 19.1.44. *The following conditions are equivalent:*

(i) The presheaf $\mathscr{F}_{\mathcal{B}}$ is a sheaf on X.

(ii) For any covering (U_α) of $U \in \mathcal{B}$ given by elements of $\mathcal{B}$, the set $\mathscr{F}(U)$ corresponds bijectively to $(s_\alpha) \in \prod_\alpha \mathscr{F}(U_\alpha)$ such that $s_\alpha|_V = s_\beta|_V$ for any $V \in \mathcal{B}$ and $V \subseteq U_\alpha \cap U_\beta$.

(iii) For any covering (U_α) of $U \in \mathcal{B}$ given by elements of $\mathcal{B}$ and $(U_{\alpha\beta\gamma})$ of $U_{\alpha\beta} = U_\alpha \cap U_\beta$ by elements of $\mathcal{B}$, the set $\mathscr{F}(U)$ corresponds bijectively to $(s_\alpha) \in \prod_\alpha \mathscr{F}(U_\alpha)$ such that $s_\alpha|_{U_{\alpha\beta\gamma}} = s_\beta|_{U_{\alpha\beta\gamma}}$ for all γ.

Proof. It is clear that (i)⇒(iii)⇒(ii). Now assume (ii) and let (U_α) be a covering of $U \in \mathcal{B}$ by elements of $\mathcal{B}$ and $(U_{\alpha\beta\gamma})$ a covering of $U_{\alpha\beta}$ by elements of $\mathcal{B}$. Let $(s_\alpha) \in \prod_\alpha \mathscr{F}(U_\alpha)$ be a family such that $s_\alpha|_{U_{\alpha\beta\gamma}} = s_\beta|_{U_{\alpha\beta\gamma}}$ for all γ. Let $V \subseteq U_\alpha \cap U_\beta$ be an basis element in $\mathcal{B}$. For each index γ, let $(V_{\mu\gamma})$ be a covering of $V \cap U_{\alpha\beta\gamma}$ by elements of $\mathcal{B}$, so that the family $(V_{\mu\gamma})_{\mu,\gamma}$ is a covering of V by elements of $\mathcal{B}$. For each pair (μ, γ) of indices, set

$$t^\alpha_{\mu\gamma} = s_\alpha|_{V_{\mu\gamma}}, \quad t^\beta_{\mu\gamma} = s_\beta|_{V_{\mu\gamma}}.$$

By hypothesis $s_\alpha|_{U_{\alpha\beta\gamma}} = s_\beta|_{U_{\alpha\beta\gamma}}$ and $V_{\mu\gamma} \subseteq U_{\alpha\beta\gamma}$, so we have $t^\alpha_{\mu\gamma} = t^\beta_{\mu\gamma}$. Moreover, for each $W \in \mathcal{B}$ and $W \subseteq V_{\mu\gamma} \cap V_{\tilde{\mu}\tilde{\gamma}}$, since $V_{\mu\gamma}$ and $V_{\tilde{\mu}\tilde{\gamma}}$ are both contained in $U_{\alpha\beta}$,

$$t^\alpha_{\mu\gamma}|_W = s_\alpha|_W = t^\alpha_{\tilde{\mu}\tilde{\gamma}}|_W, \quad t^\beta_{\mu\gamma}|_W = s_\beta|_W = t^\beta_{\tilde{\mu}\tilde{\gamma}}|_W.$$

Applying (ii) on the open set V and the covering $(V_{\mu\gamma})$, we then conclude that $s_\alpha|_V = s_\beta|_V$, which again by condition (ii) implies that (s_α) corresponds to a section on $\mathscr{F}(U)$. This proves (ii)⇒(iii).

Now we prove the implication (iii)⇒(i). Before this, we first note that, if (iii) holds and $\mathcal{B}'$ is a basis of X contained in $\mathcal{B}$, then the presheaf $\mathscr{F}_{\mathcal{B}'}$ associated to the presheaf $(\mathscr{F}(U))_{U\in\mathcal{B}'}$ is canonically isomorphic to the presheaf $\mathscr{F}_{\mathcal{B}}$ associated to $(\mathscr{F}(U))_{U\in\mathcal{B}}$. Indeed, first of all the inverse limit (for $V \in \mathcal{B}' \subseteq \mathcal{B}$, $V \subseteq U$) of the canonical morphisms $\mathscr{F}_{\mathcal{B}}(U) \to \mathscr{F}(V)$ gives a morphism

$$\mathscr{F}_{\mathcal{B}}(U) \to \mathscr{F}_{\mathcal{B}'}(U)$$

for any open set U. We claim that this is an isomorphism if $U \in \mathcal{B}$. To see this, let (U_α) be a covering of U by elements of $\mathcal{B}'$ and for each (α, β), choose a covering $(U_{\alpha\beta\gamma})$ of $U_{\alpha\beta} = U_\alpha \cap U_\beta$ by elements of $\mathcal{B}'$. For each γ, we have a commutative diagram

$$\begin{tikzcd}
 & & \mathscr{F}(U_\alpha) \arrow[dr] & \\
\mathscr{F}_{\mathcal{B}'}(U) \arrow[rr, dashed] \arrow[urr, bend left] \arrow[drr, bend right] & & \mathscr{F}(U) \arrow[u] \arrow[d] & \mathscr{F}(U_{\alpha\beta\gamma}) \\
 & & \mathscr{F}(U_\beta) \arrow[ur] &
\end{tikzcd}$$

so condition (iii) shows that the canonical morphism $\mathscr{F}_{\mathcal{B}'}(U) \to \mathscr{F}(U_\alpha)$ factors through $\mathscr{F}(U)$. It is immediate that the morphisms $\mathscr{F}_{\mathcal{B}}(U) \to \mathscr{F}_{\mathcal{B}'}(U)$ and $\mathscr{F}_{\mathcal{B}'}(U) \to \mathscr{F}_{\mathcal{B}}(U)$ thus defined are inverses of each other. This being so, for all open set U of X, the morphisms

$$\mathscr{F}_{\mathcal{B}'}(U) \to \mathscr{F}_{\mathcal{B}'}(W) = \mathscr{F}_{\mathcal{B}}(W) = \mathscr{F}(W)$$

for $W \in \mathcal{B}$, $W \subseteq U$ satisfy the conditions characterizing the inverse limit of the $\mathscr{F}(W)$'s, so our claim follows from the uniqueness of the inverse limit.

Now let U be any open set of X, (U_α) a covering of U by open sets contained in U, and let $\mathcal{B}'$ be the subfamily of $\mathcal{B}$ consisting of the sets of $\mathcal{B}$ contained in at least one U_α. It is clear that $\mathcal{B}'$ is still a basis of the topology of X, so $\mathscr{F}_{\mathcal{B}}(U)$ (resp. $\mathscr{F}_{\mathcal{B}}(U_\alpha)$) is the inverse limit of the $\mathscr{F}(V)$ for $V \in \mathcal{B}'$ and $V \subseteq U$ (resp. $V \subseteq U_\alpha$); the sheaf axiom is then verified immediately by virtue of the definition of the inverse limit. □

We say $\mathscr{F}$ is a **sheaf on** $\mathcal{B}$ if it satisfies the equivalent conditions in Proposition 19.1.44.

Corollary 19.1.45. *Let X be a topological space. Let $\mathcal{B}$ be a basis for the topology on X. Assume that for every pair $U, U' \in \mathcal{B}$ we have $U \cap U' \in \mathcal{B}$. Let $\mathscr{F}$ be a presheaf of sets on $\mathcal{B}$. The following are equivalent:*

(i) The presheaf $\mathscr{F}$ is a sheaf on $\mathcal{B}$.

(ii) For every $U \in \mathcal{B}$ and for every family of sections $s_i \in \mathscr{F}(U_i)$ such that $s_i|_{U_i \cap U_j} = s_j|_{U_i \cap U_j}$ there exists a unique section $s \in \mathscr{F}(U)$ which restricts to s_i on U_i.

Proof. This is a reformulation of Proposition 19.1.44, as we can take V to be $U_\alpha \cap U_\beta$. □

Note that for any $x \in X$ we have $\mathscr{F}_x = (\mathscr{F}_{\mathcal{B}})_x$ in the situation of the proposition. This is so because the collection of elements of $\mathcal{B}$ containing x forms a fundamental system of open neighbourhoods of x.

Let $\mathscr{F}$, $\mathscr{G}$ be two presheaves over $\mathcal{B}$. A morphism $\varphi : \mathscr{F} \to \mathscr{G}$ is defined to be a family $(\varphi_V)_{V \in \mathcal{B}}$ of morphisms $\varphi_V : \mathscr{F}(V) \to \mathscr{F}(V)$ satisfying the compatible conditions with restriction maps. By passing to inverse limits, we get a morphism $\varphi_{\mathcal{B}} : \mathscr{F}_{\mathcal{B}} \to \mathscr{G}_{\mathcal{B}}$ of presheaves (it is easy to verify the compatible conditions with restriction maps).

Theorem 19.1.46. *Let X be a topological space. Let $\mathcal{B}$ be a basis for the topology on X. Denote* $\mathbf{Shv}(\mathcal{B})$ *the category of sheaves on $\mathcal{B}$. There is an equivalence of categories*

$$\mathbf{Shv}(X) \to \mathbf{Shv}(\mathcal{B})$$

which assigns to a sheaf on X its restriction to the members of $\mathcal{B}$.

Proof. If $\mathscr{F}$ is a sheaf on $\mathcal{B}$, then the sheaf $\mathscr{F}_{\mathcal{B}}$ satisfies $\mathscr{F}(U) = \mathscr{F}_{\mathcal{B}}(U)$ for $U \in \mathcal{B}$, thus the restriction of $\mathscr{F}_{\mathcal{B}}$ equals $\mathscr{F}$. Conversely, if $\mathscr{F}$ is a sheaf on X, then the restriction $\mathscr{F}|_{\mathcal{B}}$ induces a sheaf $\mathscr{F}' := (\mathscr{F}|_{\mathcal{B}})_{\mathcal{B}}$ on X. Then $\mathscr{F}$ and $\mathscr{F}'$ has the same stalk, so we conclude $\mathscr{F} \cong \mathscr{F}'$. Moreover, by looking at stalks, we see the Hom sets are canonically identified, whence the claim. □

19.1.8 The category of presheaves and sheaves

In this subsection, we derive some result for the categories $\mathbf{Psh}(X)$ and $\mathbf{Shv}(X)$.

19.1.8.0.1 The category of presheaves We first consider the category of presheaves, with morphisms are defined to be morphisms of presheaves. As we will see, this category behaves much like the base category **Set**.

Example 19.1.47 (Final object of presheaves). Let X be a topological space. Consider a rule $\mathscr{F}$ that associates to every open subset a singleton set. Since every set has a unique map into a singleton set, there exist unique restriction maps res^U_V. The resulting structure is a presheaf of sets. It is a final object in the category of presheaves of sets, by the property of singleton sets mentioned above. Hence it is also unique up to unique isomorphism. We will sometimes write $*$ for this presheaf.

Proposition 19.1.48. *Let $\mathcal{I}$ be a small category and let $\mathscr{F} : \mathcal{I} \to \mathbf{Psh}(X)$ be an $\mathcal{I}$-diagram of presheaves on X. Then the limit and colimit of $\mathscr{F}$ both exist, whichi are given by*

$$(\varprojlim_i \mathscr{F}_i)(U) := \varprojlim_i \mathscr{F}_i(U), \quad (\varinjlim_i \mathscr{F}_i)(U) := \varinjlim_i \mathscr{F}_i(U).$$

and the restriction maps are induced by that of the $\mathscr{F}_i$'s.

Proof. The given constructions are clearly meaningful and define presheaves, where the restriction map is given by the limit (or colimit) of that of $\mathscr{F}_i$. For the colimit, if we are given morphisms $\varphi_i : \mathscr{F}_i \to G$ such that the following diagram commutes

$$\begin{tikzcd} \mathscr{F}_i \arrow[rr] \arrow[dr] & & \mathscr{F}_j \arrow[dl] \\ & \mathscr{G} & \end{tikzcd}$$

Then for each $U \subseteq X$ open we can take limit of the system $(\varphi_{i,U})$ to get a morphism $\varphi : \varinjlim_i \mathscr{F}_i(U) \to \mathscr{G}(U)$. Moreover, these morphisms are compatible with the restriction maps of $\mathscr{F}_i$, hence compatible with that of $\varinjlim_i \mathscr{F}_i$. This gives a morphism $\varinjlim_i \mathscr{F}_i \to \mathscr{G}$, so $\varinjlim_i \mathscr{F}_i$ satisfies the universal property of colimits. Similarly, we can show that $\varprojlim_i \mathscr{F}_i$ satisfies the universal property of limits. □

Definition 19.1.49. *Let $\varphi : \mathscr{F} \to \mathscr{G}$ be a morphism of presheaves of sets.*

*(a) We say that φ is **injective** if for every open subset $U \subseteq X$ the map $\varphi_U : \mathscr{F}(U) \to \mathscr{G}(U)$ is injective.*

*(b) We say that φ is **surjective** if for every open subset $U \subseteq X$ the map $\varphi_U : \mathscr{F}(U) \to \mathscr{G}(U)$ is injective.*

We show that the injectivity and surjectivity gives monomorphisms and epimorphisms in the category of presheaves.

Proposition 19.1.50. *The injective (resp. surjective) maps defined above are exactly the monomorphisms (resp. epimorphisms) of* $\mathbf{Psh}(X)$. *A map is an isomorphism if and only if it is both injective and surjective.*

Proof. We shall show that $\varphi : \mathscr{F} \to \mathscr{G}$ is injective if and only if it is an monomorphism of $\mathbf{Psh}(X)$. Indeed, the only if direction is straightforward, so let us show the if direction. If

φ is a monomorphism, let $U \subseteq X$ be an open subset; we are going to show that φ_U is a monomorphism in the category **Set**. For this, consider any two maps $f, g : A \to \mathscr{F}(U)$ such that $\varphi_U \circ f = \varphi_U \circ g$. We define a presheaf $\mathscr{A}$ by

$$\mathscr{A}(V) = \begin{cases} A & V \subseteq U, \\ \varnothing & \text{otherwise.} \end{cases}$$

Then we have induced morphism of presheaves ψ_f and ψ_g given by the diagram

$$\begin{tikzcd} \mathscr{A}(U) \arrow[r, shift left, "f"] \arrow[r, shift right, "g"'] \arrow[d, equal] & \mathscr{F}(U) \arrow[d, "\mathrm{res}_V^U"] \\ \mathscr{A}(V) \arrow[r, dashed, "\psi_V"] & \mathscr{F}(V) \end{tikzcd}$$

Then we can see $\varphi \circ \psi_f = \varphi \circ \psi_g$, which implies $\psi_f = \psi_g$ since φ is monic. This gives $f = g$ by our construction, so φ_U is monic in the category of sets, hence injective.

Now we show that $\varphi : \mathscr{F} \to \mathscr{G}$ is surjective if and only if it is an epimorphism of $\mathbf{Psh}(X)$. Similarly, the only if direction is straightforward, so let us show the if direction. Assume that φ is an epimorphism, and we show φ_U is epic in **Set**. For any maps $f, g : \mathscr{G}(U) \to B$ such that $f \circ \varphi_U = g \circ \varphi_U$, we define a presheaf $\mathscr{B}$ by

$$\mathscr{B}(V) = \begin{cases} B & V \supseteq U, \\ \varnothing & \text{othewise.} \end{cases}$$

Similarly, we can define morphism of presheaves by the diagram

$$\begin{tikzcd} \mathscr{G}(V) \arrow[r, dashed, "\psi_V"] \arrow[d, "\mathrm{res}_V^U"] & \mathscr{B}(V) \arrow[d, equal] \\ \mathscr{G}(U) \arrow[r, shift left, "f"] \arrow[r, shift right, "g"'] & \mathscr{B}(U) \end{tikzcd}$$

and we have $\psi_f \circ \varphi_U = \psi_g \circ \varphi_U$, which implies $f = g$, so φ_U is surjective. □

19.1.8.0.2 The category of sheaves We have already seen that limits and colimits exist in the category of presheaves. Now we consider them in the category of sheaves.

Proposition 19.1.51. *Let $\mathscr{I}$ be a small category and let $\mathscr{F} : \mathscr{I} \to \mathbf{Psh}(X)$ be an $\mathscr{I}$-diagram of sheaves on X. Then the limit and colimit of $\mathscr{F}$ both exist, whichi are given by*

$$\varprojlim_{i,\mathbf{Shv}(X)} \mathscr{F}_i = \varprojlim_{i,\mathbf{Psh}(X)} \mathscr{F}_i, \qquad \varinjlim_{i,\mathbf{Shv}(X)} \mathscr{F}_i := (\varinjlim_{i,\mathbf{Psh}(X)} \mathscr{F}_i)^{\#}.$$

Proof. Since the limit and colimit exist in $\mathbf{Psh}(X)$, we can define

$$\varprojlim_{i,\mathbf{Shv}(X)} \mathscr{F}_i := (\varprojlim_{i,\mathbf{Psh}(X)} \mathscr{F}_i)^{\#}, \qquad \varinjlim_{i,\mathbf{Shv}(X)} \mathscr{F}_i := (\varinjlim_{i,\mathbf{Psh}(X)} \mathscr{F}_i)^{\#}.$$

Using the universal property of sheafification, we can show that the construction above indeed

gives the colimits in the category of sheaves. Now we note that, since the forgetful functor $\iota : \mathbf{Shv}(X) \to \mathbf{Psh}(X)$ has a left adjoint given by the sheafification, it commutes with limits. In other words, if $\mathcal{I}$ is a small category and $\mathcal{F} : \mathcal{I} \to \mathbf{Psh}(X)$ be an $\mathcal{I}$-diagram of sheaves on X. Then the limit $\varprojlim_i \mathcal{F}_i$ satisfies

$$\iota(\varprojlim_{i,\mathbf{Shv}(X)} \mathcal{F}_i) = \varprojlim_{i,\mathbf{Psh}(X)} \iota(\mathcal{F}_i).$$

But the forgetful functor does nothing actually, so the limit $\varprojlim_i \mathcal{F}_i$ is in fact given by the limit in $\mathbf{Psh}(X)$, i.e.,

$$\varprojlim_{i,\mathbf{Shv}(X)} \mathcal{F}_i = \varprojlim_{i,\mathbf{Psh}(X)} \mathcal{F}_i.$$

However, since ι may not commutes with colimits, the colimit of $\mathcal{F}$ should be defined as the sheafification of that in $\mathbf{Psh}(X)$:

$$\varinjlim_{i,\mathbf{Shv}(X)} \mathcal{F}_i := (\varinjlim_{i,\mathbf{Psh}(X)} \mathcal{F}_i)^{\#}.$$

This completes the proof. □

Proposition 19.1.52. *Let $x \in X$ be a point. Then there are maps*

$$(\varprojlim_i \mathcal{F}_i)_x \to \varprojlim_i (\mathcal{F}_i)_x, \quad (\varinjlim_i \mathcal{F}_i)_x \cong \varinjlim_i (\mathcal{F}_i)_x$$

for limits and colimits of (pre)sheaves. The second map is always bijective, and the first map becomes an bijection when $\mathcal{I}$ is finite,

Proof. First we consider (co)limit of presheaves. The maps $\mathcal{F}_i(U) \to (\mathcal{F}_i)_x$ yield maps

$$\varprojlim_i \mathcal{F}_i(U) \to \varprojlim_i (\mathcal{F}_i)_x \quad \text{and} \quad \varinjlim_i \mathcal{F}_i(U) \to \varinjlim_i (\mathcal{F}_i)_x.$$

Taking the filtered colimit over the open neighborhoods of x we obtain maps

$$(\varprojlim_i \mathcal{F}_i)_x \to \varprojlim_i (\mathcal{F}_i)_x, \quad (\varinjlim_i \mathcal{F}_i)_x \to \varinjlim_i (\mathcal{F}_i)_x$$

As filtered colimits commute with finite limits, the first map is an isomorphism if $\mathcal{I}$ is finite. And since colimits commute with each other, the second is always bijective.

In the case of sheaves, we need to take sheafification. Since the sheafification does not change stalk, the result is the same. □

Proposition 19.1.53. *Suppose $\varphi : \mathcal{F} \to \mathcal{G}$ is a morphism of sheaves of sets on a topological space X. Then the following are equivalent.*

(a) φ is a monomorphism in the category of sheaves.

(b) φ is injective on the level of stalks: $\varphi_x : \mathcal{F}_x \to \mathcal{G}_x$ is injective for all $x \in X$.

(c) φ is injective on the level of open sets: $\varphi(U) : \mathcal{F}(U) \to \mathcal{G}(U)$ is injective for all open $U \subseteq X$.

*If these conditions hold, we say that $\mathscr{F}$ is a **subsheaf** of $\mathscr{G}$.*

Proof. The last two statements are equivalent by Proposition 19.1.10, and the implication (c)⇒(a) is immediate, since a monomorphism in $\mathbf{Psh}(X)$ is clearly monic in $\mathbf{Shv}(X)$.

Now assume that φ is a monomorphism, and let $s, t \in \mathscr{F}(U)$ be such that $\varphi_U(s) = \varphi_U(t)$. Then by Example 19.1.20 there are morphisms $\psi_s, \psi_t : \mathscr{U}^\# \to \mathscr{F}$. From $\varphi_U(s) = \varphi_U(t)$ we see $\varphi \circ \psi_s = \varphi \circ \psi_t$, which implies $\psi_s = \psi_t$. By the isomorphism in Example 19.1.20, we conclude $s = t$, so φ_U is injective. □

Proposition 19.1.54. *Suppose $\varphi : \mathscr{F} \to \mathscr{G}$ is a morphism of sheaves of sets on a topological space X. Then the following are equivalent.*

(a) φ is a epimorphism in the category of sheaves.

(b) φ is surjective on the level of stalks: $\varphi_x : \mathscr{F}_x \to \mathscr{G}_x$ is injective for all $x \in X$.

(c) For any open subsets $U \subseteq X$ and every $t \in \mathscr{G}(U)$ there exist an open covering $U = \bigcup_i U_i$ and sections $s_i \in \mathscr{F}(U_i)$ such that $\varphi_{U_i}(s_i) = t|_{U_i}$, i.e., we can locally find preimage of t.

*If these conditions hold, we say that $\mathscr{G}$ is a **quotient sheaf** of $\mathscr{F}$.*

Proof. If $\varphi_x : \mathscr{F}_x \to \mathscr{G}_x$ is surjective for all $x \in X$, then by Proposition 19.1.10 and the diagram

$$\begin{tikzcd}
\mathscr{F}(U) \arrow[r, "\varphi_U"] \arrow[d, hook] & \mathscr{G} \arrow[r, "\psi_U"] \arrow[d, hook] & \mathscr{H}(U) \arrow[d, hook] \\
\prod_{x\in U} \mathscr{F}_x \arrow[r, "\varphi_x"] & \prod_{x\in U} \mathscr{G}_x \arrow[r, "\psi_x"] & \prod_{x\in U} \mathscr{H}_x
\end{tikzcd}$$

we see φ is an epimorphism.

Now assume that φ is an epimorphism, and let $f, g : \mathscr{G}_x \to B$ be two maps such that $f \circ \varphi_x = g \circ \varphi_x$. Then by Proposition 19.1.29 we have induced morphism of sheaves $\psi_f, \psi_g : \mathscr{G} \to i_{x,*}(B)$ such that $\psi_f \circ \varphi = \psi_g \circ \varphi$. Since φ is an epic, this implies $f = g$, which means φ_x is surjective.

Finally, the condition (b) clearly implies (c), and if (c) holds, let $t_x \in \mathscr{G}_x$ with $t_x = (t, V)$ for some $V \subseteq X$ open and $t \in \mathscr{G}_x$. Then there is a covering $V = \bigcup_i V_i$ and $s_i \in \mathscr{F}(U_i)$ such that $\varphi_{V_i}(s_i) = t|_{V_i}$. Choose a $x \in V_i$, then $\varphi_x\big((s_i)_x\big) = t_x$. Thus φ_x is surjective. □

Remark 19.1.5. The condition for φ in Proposition 19.1.54 does not imply that φ_U is surjective for all open sets U of X as Example 19.1.55 shows. In other words, being epic in the category of sheaves is a weaker that begin surjective on objects.

Example 19.1.55. Let $\mathcal{O}_X$ be the sheaf of holomorphic functions on an open subset X of $\mathbb{C}$. For every open subspace $U \subseteq X$ and $f \in \mathcal{O}_X(U)$ we let $D_U(f) = f'$ be the derivative. We obtain a morphism $D : \mathcal{O}_X \to \mathcal{O}_X$ of sheaves of $\mathbb{C}$-vector spaces. Then D is an epimorphism, because locally every holomorphic function has a primitive. But there exist open subsets U of X and functions f on U that have no primitive., for instance $U = \mathbb{B}(z_0) \setminus \{z_0\} \subseteq \mathbb{C}$ contained in X and $f = 1/(z - z_0)$. More precisely, by complex analysis we know that D_U is surjective if and only if every connected component of U is simply connected. Thus D is not surjective.

19.2 Sheaf of modules

19.2.1 Presheaf of moudles

Definition 19.2.1. *Let X be a topological space, and let $\mathcal{O}$ be a presheaf of rings on X.*

- *A presheaf of $\mathcal{O}$-modules is given by an abelian presheaf $\mathcal{F}$ together with a map of presheaves of sets*
$$\mathcal{O} \times \mathcal{F} \to \mathcal{F}$$
such that for every open $U \subseteq X$ the map $\mathcal{O}(U) \times \mathcal{F}(U) \to \mathcal{F}(U)$ defines the structure of an $\mathcal{O}(U)$-module structure on the abelian group $\mathcal{F}(U)$.

- *A morphism $\varphi : \mathcal{F} \to \mathcal{G}$ of presheaves of $\mathcal{O}$-modules is a morphism of abelian presheaves $\varphi : \mathcal{F} \to \mathcal{G}$ such that the diagram*
$$\begin{tikzcd} \mathcal{O} \times \mathcal{F} \arrow[r] \arrow[d, "1\times\varphi"'] & \mathcal{F} \arrow[d, "\varphi"] \\ \mathcal{O} \times \mathcal{G} \arrow[r] & \mathcal{G} \end{tikzcd}$$
commutes.

- *The set of $\mathcal{O}$-module morphisms as above is denoted* $\mathrm{Hom}_{\mathcal{O}}(\mathcal{F}, \mathcal{G})$. *The category of presheaves of $\mathcal{O}$-modules is denoted* $\mathbf{PMod}(\mathcal{O})$.

Suppose that $\mathcal{O}_1 \to \mathcal{O}_2$ is a morphism of presheaves of rings on X. In this case, if $\mathcal{F}$ is a presheaf of $\mathcal{O}_2$-modules then we can think of $\mathcal{F}$ as a presheaf of $\mathcal{O}_2$-modules by using the composition
$$\mathcal{O}_1 \times \mathcal{F} \to \mathcal{O}_2 \times \mathcal{F} \to \mathcal{F}.$$
We sometimes denote this by $\mathcal{F}_{\mathcal{O}_1}$ to indicate the restriction of rings. We call this the **restriction of** $\mathcal{F}$. We obtain the restriction functor
$$\mathbf{PMod}(\mathcal{O}_2) \to \mathbf{PMod}(\mathcal{O}_1).$$
On the other hand, given a presheaf of $\mathcal{O}_1$-modules $\mathcal{G}$ we can construct a presheaf of $\mathcal{O}_2$-modules $\mathcal{O}_2 \otimes_{p,\mathcal{O}_1} \mathcal{F}$ by the rule
$$(\mathcal{O}_2 \otimes_{p,\mathcal{O}_1} \mathcal{F})(U) = \mathcal{O}_2(U) \otimes_{p,\mathcal{O}_1} \mathcal{F}(U).$$
The index p stands for presheaf. This presheaf is called the **tensor product presheaf**. We obtain the change of rings functor
$$\mathbf{PMod}(\mathcal{O}_1) \to \mathbf{PMod}(\mathcal{O}_2).$$

Proposition 19.2.2. *With $\mathcal{O}_1, \mathcal{O}_2$ and $\mathcal{F}, \mathcal{G}$ as above there exists a canonical bijection*
$$\mathrm{Hom}_{\mathcal{O}_1}(\mathcal{G}, \mathcal{F}_{\mathcal{O}_1}) = \mathrm{Hom}_{\mathcal{O}_2}(\mathcal{O}_2 \otimes_{p,\mathcal{O}_1} \mathcal{G}, \mathcal{F}).$$
In other words, the restriction and change of rings functors are adjoint to each other.

Proof. This follows from the fact that for a ring map $A \to B$ the restriction functor and the change of ring functor are adjoint to each other. □

The stalk of a sheaf of $\mathcal{O}$-module is defined in the same as that of sheaf of sets.

Proposition 19.2.3. *Let X be a topological space. Let $\mathcal{O}$ be a presheaf of rings on X. Let $\mathcal{F}$ be a presheaf of $\mathcal{O}$-modules. Let $x \in X$. The canonical map $\mathcal{O}_x \times \mathcal{F}_x \to \mathcal{F}_x$ coming from the multiplication map $\mathcal{O} \times \mathcal{F} \to \mathcal{F}$ defines a $\mathcal{O}_x$-module structure on the abelian group $\mathcal{F}_x$.*

Proposition 19.2.4. *Let X be a topological space. Let $\mathcal{O} \to \mathcal{O}'$ be a morphism of presheaves of rings on X. Let $\mathcal{F}$ be a presheaf of $\mathcal{O}$-modules. Let $x \in X$. We have*

$$\mathcal{F}_x \otimes_{\mathcal{O}_x} \mathcal{O}'_x = (\mathcal{F} \otimes_{p,\mathcal{O}} \mathcal{O}')_x.$$

as $\mathcal{O}'_x$-modules.

Proof. Tensor product is left-adjoint, so it commutes with colimit. □

19.2.2 Sheaf of moudles

Definition 19.2.5. *Let X be a topological space. Let $\mathcal{O}$ be a sheaf of rings on X.*

- *A sheaf of $\mathcal{O}$-modules is a presheaf of $\mathcal{O}$-modules $\mathcal{F}$, such that the underlying presheaf of abelian groups $\mathcal{F}$ is a sheaf.*
- *A morphism of sheaves of $\mathcal{O}$-modules is a morphism of presheaves of $\mathcal{O}$-modules.*
- *Given sheaves of $\mathcal{O}$-modules $\mathcal{F}$ and $\mathcal{G}$ we denote $\mathrm{Hom}_{\mathcal{O}}(\mathcal{F}, \mathcal{G})$ the set of morphism of sheaves of $\mathcal{O}$-modules. The category of sheaves of $\mathcal{O}$-modules is denoted $\mathbf{Mod}(\mathcal{O})$.*

19.2.3 Sheafification of presheaves of modules

Proposition 19.2.6. *Let X be a topological space. Let $\mathcal{O}$ be a presheaf of rings on X. Let $\mathcal{F}$ be a presheaf $\mathcal{O}$-modules. Let $\mathcal{O}^\#$ be the sheafification of $\mathcal{O}$. Let $\mathcal{F}^\#$ be the sheafification of $\mathcal{F}$ as a presheaf of abelian groups. There exists a map of sheaves of sets*

$$\mathcal{O}^\# \times \mathcal{F}^\# \to \mathcal{F}^\#.$$

which makes the diagram

$$\begin{tikzcd} \mathcal{O} \times \mathcal{F} \arrow[r] \arrow[d] & \mathcal{F} \arrow[d] \\ \mathcal{O}^\# \times \mathcal{F}^\# \arrow[r] & \mathcal{F}^\# \end{tikzcd}$$

commute and which makes $\mathcal{F}^\#$ into a sheaf of $\mathcal{O}^\#$-modules. In addition, if $\mathcal{G}$ is a presheaf of $\mathcal{O}$-modules, then any morphism of presheaves of $\mathcal{O}$-modules $\mathcal{F} \to \mathcal{G}$ induced a unique morphism $\mathcal{F}^\# \to \mathcal{G}^\#$ of sheaf of $\mathcal{O}^\#$-modules.

Proof. Since finite product and coproduct coincide in the category of modules, the sheafification commutes with both of them. Thus we can apply the universal property of sheafification on the map $\mathcal{O} \times \mathcal{F} \to \mathcal{F}$ to get a map

$$\mathcal{O}^\# \times \mathcal{F}^\# \to \mathcal{F}^\#$$

Moreover, for a morphism of $\mathcal{O}$-modules $\mathcal{F} \to \mathcal{G}$, apply sheafification on the diagram

$$\begin{tikzcd} \mathcal{O} \times \mathcal{F} \arrow[r] \arrow[d] & \mathcal{F} \arrow[d] \\ \mathcal{O} \times \mathcal{G} \arrow[r] & \mathcal{G} \end{tikzcd}$$

we get the desired morphism. □

This actually means that the functor $\iota : \mathbf{Mod}(\mathcal{O}^\#) \to \mathbf{PMod}(\mathcal{O})$ and the sheafification functor of the lemma $\# : \mathbf{PMod}(\mathcal{O}) \to \mathbf{Mod}(\mathcal{O}^\#)$ are adjoint. In a formula

$$\mathrm{Hom}_{\mathbf{Mod}(\mathcal{O}^\#)}(\mathcal{F}^\#, \mathcal{G}) = \mathrm{Hom}_{\mathbf{PMod}(\mathcal{O})}(\mathcal{F}, \iota\mathcal{G}).$$

Let X be a topological space. Let $\mathcal{O}_1 \to \mathcal{O}_2$ be a morphism of sheaves of rings on X. We defined a restriction functor and a change of rings functor on presheaves of modules associated to this situation. If $\mathcal{F}$ is a sheaf of $\mathcal{O}_2$-modules then the restriction $\mathcal{F}_{\mathcal{O}_2}$ of $\mathcal{F}$ is clearly a sheaf of $\mathcal{O}_1$-modules. We obtain the restriction functor

$$\mathbf{Mod}(\mathcal{O}_2) \to \mathbf{Mod}(\mathcal{O}_1).$$

On the other hand, given a sheaf of $\mathcal{O}_1$-modules $\mathcal{G}$ the presheaf of $\mathcal{O}_2$-modules $\mathcal{O}_2 \otimes_{p,\mathcal{O}_1} \mathcal{G}$ is in general not a sheaf. Hence we define the tensor product sheaf $\mathcal{O}_2 \otimes_{\mathcal{O}_1} \mathcal{G}$ by the formula

$$\mathcal{O}_2 \otimes_{\mathcal{O}_1} \mathcal{G} = (\mathcal{O}_2 \otimes_{p,\mathcal{O}_1} \mathcal{G})^\#.$$

Proposition 19.2.7. *With X, $\mathcal{O}_1, \mathcal{O}_2$, $\mathcal{F}$ and $\mathcal{G}$ as above there exists a canonical bijection*

$$\mathrm{Hom}_{\mathcal{O}_1}(\mathcal{G}, \mathcal{F}_{\mathcal{O}_1}) = \mathrm{Hom}_{\mathcal{O}_2}(\mathcal{O}_2 \otimes_{\mathcal{O}_1} \mathcal{G}, \mathcal{F}).$$

In other words, the restriction and change of rings functors are adjoint to each other.

Proof. This follows from Proposition 19.2.2 and the fact that

$$\mathrm{Hom}_{\mathcal{O}_2}(\mathcal{O}_2 \otimes_{\mathcal{O}_1} \mathcal{G}, \mathcal{F}) = \mathrm{Hom}_{\mathcal{O}_2}(\mathcal{O}_2 \otimes_{p,\mathcal{O}_1} \mathcal{G}, \mathcal{F}, \mathcal{F})$$

by the property of sheafification. □

Proposition 19.2.8. *Let X be a topological space. Let $\mathcal{O} \to \mathcal{O}'$ be a morphism of sheaves of rings on X. Let $\mathcal{F}$ be a sheaf $\mathcal{O}$-modules. Let $x \in X$. We have*

$$\mathcal{F}_x \otimes_{\mathcal{O}_x} \mathcal{O}'_x = (\mathcal{F} \otimes_{\mathcal{O}} \mathcal{O}')_x.$$

19.2.4 Continuous maps

The case of sheaves of modules is more complicated. First we state a few obvious lemmas.

Lemma 19.2.9. *Let $f : X \to Y$ be a continuous map of topological spaces. Let $\mathcal{O}$ be a presheaf of rings on X. Let $\mathcal{F}$ be a presheaf of $\mathcal{O}$-modules. There is a natural map of underlying presheaves of sets*

$$f_*\mathcal{O} \times f_*\mathcal{F} \to f_*\mathcal{F}$$

which turns $f_*\mathcal{F}$ into a presheaf of $f_*\mathcal{O}$-modules. This construction is functorial in $\mathcal{F}$.

Proof. Let $V \subseteq Y$ is open. We define the map of the lemma to be the map

$$f_*\mathcal{O}(V) \times f_*\mathcal{F}(V) = \mathcal{O}(f^{-1}(V)) \times \mathcal{F}(f^{-1}(V)) \to \mathcal{F}(f^{-1}(V)) = f_*\mathcal{F}(V).$$

Here the arrow in the middle is the multiplication map on X. □

Lemma 19.2.10. *Let $f : X \to Y$ be a continuous map of topological spaces. Let $\mathcal{O}$ be a presheaf of rings on Y. Let G be a presheaf of $\mathcal{O}$-modules. There is a natural map of underlying presheaves of sets*

$$f^p\mathcal{O} \times f^p\mathcal{G} \to \mathcal{G}$$

which turns $f^p\mathcal{G}$ into a presheaf of $f^p\mathcal{O}$-modules. This construction is functorial in $\mathcal{G}$.

Proof. Let $U \subseteq X$ is open. We define the map of the lemma to be the map

$$\begin{aligned} f^p\mathcal{O}(U) \times f^p\mathcal{G}(U) &= \varinjlim_{f(U)\subseteq V} \mathcal{O}(V) \times \varinjlim_{f(U)\subseteq V} \mathcal{G}(V) = \varinjlim_{f(U)\subseteq V} \big(\mathcal{O}(V) \times \mathcal{G}(V)\big) \\ &\to \varinjlim_{f(U)\subseteq V} \mathcal{G}(V) = f^p\mathcal{G}(V) \end{aligned}$$

Here the arrow in the middle is the multiplication map on Y. The second equality holds because directed colimits commute with finite limits. □

Let $f : X \to Y$ be a continuous map. Let $\mathcal{O}_X$ be a presheaf of rings on X and let $\mathcal{O}_Y$ be a presheaf of rings on Y. So at the moment we have defined functors

$$f_* : \mathbf{PMod}(\mathcal{O}_X) \to \mathbf{PMod}(f_*\mathcal{O}_X), \quad f^p : \mathbf{PMod}(\mathcal{O}_Y) \to \mathbf{PMod}(f^p\mathcal{O}_Y).$$

These satisfy some compatibilities as follows.

Proposition 19.2.11. *Let $f : X \to Y$ be a continuous map of topological spaces. Let $\mathcal{O}$ be a presheaf of rings on Y. Let $\mathcal{G}$ be a presheaf of $\mathcal{O}$-modules. Let $\mathcal{F}$ be a presheaf of $f^p\mathcal{O}$-modules. Then*

$$\mathrm{Hom}_{\mathbf{PMod}(f^p\mathcal{O})}(f^p\mathcal{G}, \mathcal{F}) = \mathrm{Hom}_{\mathbf{PMod}(\mathcal{O})}(\mathcal{G}, f_*\mathcal{F})$$

Here we think of $f_*\mathcal{F}$ as an $\mathcal{O}$-module via the map $\rho_{\mathcal{O}} : \mathcal{O} \to f_*f^p\mathcal{O}$.

Proof. Note that we have

$$\mathrm{Mor}_{\mathbf{PAb}(X)}(f^p\mathcal{G}, \mathcal{F}) = \mathrm{Mor}_{\mathbf{PAb}(Y)}(\mathcal{G}, f_*\mathcal{F}).$$

So what we have to prove is that under this correspondence, the subsets of module maps correspond. In addition, the correspondence is determined by the rule

$$(\psi : f^p\mathcal{G} \to \mathcal{F}) \to (f_*\psi \circ \rho_{\mathcal{G}} : \mathcal{G} \to f_*\mathcal{F})$$

and in the other direction by the rule

$$(\varphi : \mathcal{G} \to f_*\mathcal{F}) \mapsto (\sigma_{\mathcal{F}} \circ f^p\varphi : f^p\mathcal{F} \to \mathcal{G})$$

Hence, using the functoriality of f_* and f^p we see that it suffices to check that the maps $\rho_{\mathcal{G}} : \mathcal{G} \to f_* f^p \mathcal{G}$ and $\sigma_{\mathcal{F}} : f^p f_* \mathcal{F} \to \mathcal{F}$ are compatible with module structures, which can be done by tracing definitions. □

Proposition 19.2.12. *Let $f : X \to Y$ be a continuous map of topological spaces. Let $\mathcal{O}$ be a presheaf of rings on X. Let $\mathcal{F}$ be a presheaf of $\mathcal{O}$-modules. Let $\mathcal{G}$ be a presheaf of $f_*\mathcal{O}$-modules. Then*

$$\mathrm{Hom}_{\mathbf{PMod}(\mathcal{O})}(\mathcal{O} \otimes_{p, f^p f_* \mathcal{O}} f^p \mathcal{G}, \mathcal{F}) = \mathrm{Hom}_{\mathbf{PMod}(f_*\mathcal{O})}(\mathcal{G}, f_* \mathcal{F}).$$

Here we use the map $\sigma_{\mathcal{O}} : f^p f_* \mathcal{O} \to \mathcal{O}$ in the definition of the tensor product.

Proof. This follows from the equalities

$$\begin{aligned}
\mathrm{Hom}_{\mathbf{PMod}(\mathcal{O})}(\mathcal{O} \otimes_{p, f^p f_* \mathcal{O}} f^p \mathcal{G}, \mathcal{F}) &= \mathrm{Hom}_{\mathbf{PMod}(f^p f_* \mathcal{O})}(f^p \mathcal{G}, \mathcal{F}_{f^p f_* \mathcal{O}}) \\
&= \mathrm{Hom}_{\mathbf{PMod}(f_* \mathcal{O})}\big(\mathcal{G}, f_*(\mathcal{F}_{f^p f_* \mathcal{O}})\big) \\
&= \mathrm{Hom}_{\mathbf{PMod}(f_* \mathcal{O})}\big(\mathcal{G}, f_* \mathcal{F}\big).
\end{aligned}$$

For the third equality, note that $\mathbf{1}_{f_*\mathcal{O}}$ corresponds to $\sigma_{\mathcal{O}}$ under the adjunction described in the proof of Proposition 19.2.11 and thus we have the equality $\mathbf{1}_{f_*\mathcal{O}} = f_* \sigma_{\mathcal{O}} \circ \rho_{f_*\mathcal{O}}$. Now consider the module structures:

$$\begin{aligned}
\mathcal{F}_{f^p f_* \mathcal{O}} : &\qquad f^p f_* \mathcal{O} \times \mathcal{F} \xrightarrow{\sigma_{\mathcal{O}} \times \mathbf{1}} \mathcal{O} \times \mathcal{F} \longrightarrow \mathcal{F} \\
f_*(\mathcal{F}_{f^p f_* \mathcal{O}}) : &\qquad f_* \mathcal{O} \times f_* \mathcal{F} \xrightarrow{\rho_{f_*\mathcal{O}} \times \mathbf{1}} f_* f^p f_* \mathcal{O} \times f_* \mathcal{F} \xrightarrow{f_* \sigma_{\mathcal{O}} \times \mathbf{1}} f_* \mathcal{O} \times f_* \mathcal{F} \longrightarrow f_* \mathcal{F}
\end{aligned}$$

we conclude that $f_*(\mathcal{F}_{f^p f_* \mathcal{O}}) = f_* \mathcal{F}$. □

Now we consider the case of sheaves.

Lemma 19.2.13. *Let $f : X \to Y$ be a continuous map of topological spaces. Let $\mathcal{O}$ be a sheaf of rings on X. Let $\mathcal{F}$ be a sheaf of $\mathcal{O}$-modules. The pushforward $f_* \mathcal{F}$ is a sheaf of $f_* \mathcal{O}$-modules.*

Lemma 19.2.14. *Let $f : X \to Y$ be a continuous map of topological spaces. Let $\mathcal{O}$ be a sheaf of rings on Y. Let $\mathcal{G}$ be a sheaf of $\mathcal{O}$-modules. There is a natural map of underlying presheaves of sets*

$$f^{-1}\mathcal{O} \times f^{-1}\mathcal{G} \to f^{-1}\mathcal{G}$$

which turns $f^{-1}\mathcal{G}$ into a sheaf of $f^{-1}\mathcal{O}$-modules.

Proof. Recall that f^{-1} is defined as the composition of the functor f^p and sheafification. Thus the lemma is a combination of Lemma 19.2.10 and Proposition 19.2.6. □

Let $f : X \to Y$ be a continuous map. Let $\mathcal{O}_X$ be a sheaf of rings on X and let $\mathcal{O}_Y$ be a sheaf of rings on Y. So now we have defined functors

$$f_* : \mathbf{Mod}(\mathcal{O}_X) \to \mathbf{Mod}(f_* \mathcal{O}_X), \quad f^{-1} : \mathbf{Mod}(\mathcal{O}_Y) \to \mathbf{Mod}(f^{-1}\mathcal{O}_Y).$$

These satisfy some compatibilities as follows.

Proposition 19.2.15. *Let $f : X \to Y$ be a continuous map of topological spaces. Let $\mathcal{O}$ be a sheaf of rings on Y. Let $\mathcal{G}$ be a sheaf of $\mathcal{O}$-modules. Let $\mathcal{F}$ be a sheaf of $f^{-1}\mathcal{O}$-modules. Then*

$$\mathrm{Hom}_{\mathbf{Mod}(f^{-1}\mathcal{O})}(f^{-1}\mathcal{G}, \mathcal{F}) = \mathrm{Hom}_{\mathbf{Mod}(\mathcal{O})}(\mathcal{G}, f_*\mathcal{F}).$$

Here we think of $f_*\mathcal{F}$ as an $\mathcal{O}$-module by restriction via $\mathcal{O} \to f_*f^{-1}\mathcal{O}$.

Proof. Argue by the equalities

$$\mathrm{Hom}_{\mathbf{Mod}(f^{-1}\mathcal{O})}(f^{-1}\mathcal{G}, \mathcal{F}) = \mathrm{Hom}_{\mathbf{Mod}(f^{p}\mathcal{O})}(f^{p}\mathcal{G}, \mathcal{F}) = \mathrm{Hom}_{\mathbf{Mod}(\mathcal{O})}(\mathcal{G}, f_*\mathcal{F}).$$

which holds by the property of sheafification. □

Proposition 19.2.16. *Let $f : X \to Y$ be a continuous map of topological spaces. Let $\mathcal{O}$ be a sheaf of rings on X. Let $\mathcal{F}$ be a sheaf of $\mathcal{O}$-modules. Let $\mathcal{G}$ be a sheaf of $f_*\mathcal{O}$-modules. Then*

$$\mathrm{Hom}_{\mathbf{Mod}(\mathcal{O})}(\mathcal{O} \otimes_{f^{-1}f_*\mathcal{O}} f^{-1}\mathcal{G}, \mathcal{F}) = \mathrm{Hom}_{\mathbf{Mod}(f_*\mathcal{O})}(\mathcal{G}, f_*\mathcal{F}).$$

Here we use the canonical map $f^{-1}f_*\mathcal{O} \to \mathcal{O}$ in the definition of the tensor product.

Proof. This follows from the equalities

$$\begin{aligned}\mathrm{Hom}_{\mathbf{Mod}(\mathcal{O})}(\mathcal{O} \otimes_{f^{-1}f_*\mathcal{O}} f^{-1}\mathcal{G}, \mathcal{F}) &= \mathrm{Hom}_{\mathbf{Mod}(f^{-1}f_*\mathcal{O})}(f^{-1}\mathcal{G}, \mathcal{F}_{f^{-1}f_*\mathcal{O}}) \\ &= \mathrm{Hom}_{\mathbf{Mod}(f_*\mathcal{O})}\big(\mathcal{G}, f_*(\mathcal{F}_{f^{-1}f_*\mathcal{O}})\big) \\ &= \mathrm{Hom}_{\mathbf{Mod}(f_*\mathcal{O})}(\mathcal{G}, f_*\mathcal{F}).\end{aligned}$$

where the last equality is obtained in Proposition 19.2.12. □

19.2.5 Supports of modules and sections

Definition 19.2.17. *Let $(X, \mathcal{O}_X)$ be a ringed space. Let $\mathcal{F}$ be a sheaf of $\mathcal{O}_X$-modules.*

- *The support of $\mathcal{F}$ is the set of points $x \in X$ such that $\mathcal{F}_x = 0$. We denote it by $\mathrm{supp}(\mathcal{F})$.*
- *Let $s \in \Gamma(X, \mathcal{F})$ be a global section. The support of s is the set of points $x \in X$ such that the image $s_x \in \mathcal{F}_x$ of s is not zero.*

Of course the support of a local section is then defined also since a local section is a global section of the restriction of $\mathcal{F}$.

Lemma 19.2.18. *Let $(X, \mathcal{O}_X)$ be a ringed space. Let $\mathcal{F}$ be a sheaf of $\mathcal{O}_X$-modules. Let $U \subseteq X$ open.*

- *The support of $s \in \mathcal{F}(U)$ is closed in U.*
- *The support of fs is contained in the intersections of the supports of $f \in \mathcal{O}_X(U)$ and $s \in \mathcal{F}(U)$.*
- *The support of $s + s'$ is contained in the union of the supports of $s, s' \in \mathcal{F}(U)$.*
- *The support of $\mathcal{F}$ is the union of the supports of all local sections of $\mathcal{F}$.*
- *If $\varphi : \mathcal{F} \to \mathcal{G}$ is a morphism of $\mathcal{O}_X$-modules, then the support of $\varphi(s)$ is contained in the support of $s \in \mathcal{F}(U)$.*

In general the support of a sheaf of modules is not closed. Namely, the sheaf could be an abelian sheaf on $\mathbb{R}$ (with the usual archimedean topology) which is the direct sum of infinitely many nonzero skyscraper sheaves each supported at a single point p_i of $\mathbb{R}$. Then the support would be the set of points pi which may not be closed.

Another example is to consider the open immersion $j : U = (0, \infty) \to \mathbb{R} = X$, and the abelian sheaf $j_!\mathbb{Z}_U$. By Proposition 19.1.33 the support of this sheaf is exactly U.

Lemma 19.2.19. *Let X be a topological space. The support of a sheaf of rings is closed.*

Proof. This is true because a ring is 0 if and only if $1 = 0$, and hence the support of a sheaf of rings is the support of the unit section. □

19.2.6 Modules generated by sections

Let $(X, \mathcal{O}_X)$ be a ringed space. Let $\mathcal{F}$ be a sheaf of $\mathcal{O}_X$-modules. Then there is an canonical identification $\mathrm{Hom}_{\mathcal{O}_X}(\mathcal{O}_X, \mathcal{F}) = \Gamma(X, \mathcal{F})$ which associate a global section $s \in \Gamma(X, \mathcal{F})$ with the unique homomorphism of $\mathcal{O}_X$-modules $\mathcal{O}_X \to \mathcal{F}, f \mapsto fs$. That is, a local section f of $\mathcal{O}_X$, i.e., a section f over some open U, is mapped to the multiplication of f with the restriction of s to U. We say that $\mathcal{F}$ is **generated by global sections** if there exist a set I and global sections $s_i \in \Gamma(X, \mathcal{F})$, $i \in I$ such that the homomorphism

$$\mathcal{O}_X^{\oplus I} \to \mathcal{F}$$

which is the homomorphism associated to s_i on the summand corresponding to i, is surjective. In this case we say that the sections s_i **generate** $\mathcal{F}$.

Proposition 19.2.20. *Let $(X, \mathcal{O}_X)$ be a ringed space and $\mathcal{F}$ be a sheaf of $\mathcal{O}_X$-modules. Let $(s_i)_{i\in I}$ be a family of global sections of $\mathcal{F}$. Then the sections s_i generate $\mathcal{F}$ if and only if for any point $x \in X$ the elements $s_{i,x} \in \mathcal{F}_x$ generate the $\mathcal{O}_{X,x}$-module $\mathcal{F}_x$.*

Proof. The homomorphism $\mathcal{O}_X^{\oplus I} \to \mathcal{F}$ is surjective if and only if for each point $x \in X$ the homomorphism $(\mathcal{O}_X^{\oplus I})_x \to \mathcal{F}_x$ is surjective. Since taking stalk commutes with colimit, we have $(\mathcal{O}_X)_x^{\oplus I}\mathcal{O}_{X,x}^{\oplus I}$, which implies the claim. □

Proposition 19.2.21. *Let $(X, \mathcal{O}_X)$ be a ringed space and $\mathcal{F}$ be a sheaf of $\mathcal{O}_X$-modules. Let $(s_i)_{i\in I}$ be a collection of local sections of $\mathcal{F}$, i.e., $s_i \in \Gamma(U_i, \mathcal{F})$ for some open subset U_i of X. Then there exists a unique smallest sub-$\mathcal{O}_X$-module $\mathcal{G}$ of $\mathcal{F}$ such that each s_i corresponds to a local section of $\mathcal{G}$, which is called the **sub-$\mathcal{O}_X$-module generated by the s_i**.*

Proof. Consider the subpresheaf of $\mathcal{F}$ defined by the rule

$$U \mapsto \{\sum_{i\in J} f_i(s_i|_U) : J \subseteq I \text{ is finite}, U \subseteq U_i \text{ for every } i \in J \text{ and } f_i \in \Gamma(U, \mathcal{O}_X)\}.$$

Let $\mathcal{G}$ be the sheafification of this subpresheaf. This is a subsheaf of $\mathcal{F}$ by Proposition 19.1.16. Since all the finite sums clearly have to be in $\mathcal{F}$ this is the smallest subsheaf as desired. □

Proposition 19.2.22. *Let $(X, \mathcal{O}_X)$ be a ringed space and $\mathcal{F}$ be a sheaf of $\mathcal{O}_X$-modules. Let $(s_i)_{i\in I}$ be a family of local sections of $\mathcal{F}$ and $\mathcal{G}$ be the subsheaf generated by the s_i and let $x \in X$. Then $\mathcal{G}_x$ is the $\mathcal{O}_{X,x}$-submodule of $\mathcal{F}_x$ generated by the elements $s_{i,x}$ for those i such that s_i is defined at x.*

Proof. This is clear from the construction of $\mathcal{G}$ in the proof of Proposition 19.2.21. □

Example 19.2.23. Consider the open immersion $j : U = (0, \infty) \to \mathbb{R} = X$, and the abelian sheaf $j_!(\mathbb{Z}_U)$. By Proposition 19.1.33 the stalk of $j_!(\mathbb{Z}_U)$ at $x = 0$ is 0. In fact the sections of this sheaf over any open interval containing 0 are 0. Thus there is no open neighbourhood of the point 0 over which the sheaf can be generated by global sections.

Let $(X, \mathcal{O}_X)$ be a ringed space. Let $\mathcal{F}$ be a sheaf of $\mathcal{O}_X$-modules. We say that $\mathcal{F}$ is **locally generated by sections** if for every $x \in X$ there exists an open neighbourhood U such that $\mathcal{F}|_U$ is globally generated as a sheaf of $\mathcal{O}_U$-modules. In other words there exists a set I and for each i a section $s_i \in \mathcal{F}(U)$ such that the associated map

$$\bigoplus_{i \in I} \mathcal{O}_U \to \mathcal{F}|_U$$

is surjective.

Proposition 19.2.24. *Let $(f, f^\#) : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ be a morphism of ringed spaces. Let $\mathcal{G}$ be a $\mathcal{O}_Y$-module. The pullback $f^*\mathcal{G}$ is locally generated by sections if $\mathcal{G}$ is locally generated by sections.*

Proof. Given an open subspace V of Y we may consider the commutative diagram of ringed spaces

$$\begin{tikzcd}
(f^{-1}(V), \mathcal{O}_{f^{-1}(V)}) \arrow[r, "i"] \arrow[d, "\tilde{f}"] & (X, \mathcal{O}_X) \arrow[d, "f"] \\
(V, \mathcal{O}_V) \arrow[r, "j"] & (Y, \mathcal{O}_Y)
\end{tikzcd}$$

We know that $(f^*\mathcal{G})|_{f^{-1}(V)} \cong (\tilde{f})^*(\mathcal{G}|_V)$, so we may assume that $\mathcal{G}$ is globally generated. We have seen that f^* commutes with all colimits, and is right exact. Thus if we have a surjection $\mathcal{O}_Y^{\oplus I} \to \mathcal{G} \to 0$, then upon applying f^* we obtain the surjection $\mathcal{O}_X^{\oplus I} \to f^*\mathcal{G} \to 0$, where we use the observation that

$$f^*\mathcal{O}_Y = \mathcal{O}_X \otimes_{f^{-1}\mathcal{O}_Y} f^{-1}\mathcal{O}_Y = \mathcal{O}_X.$$

This implies the assertion. □

19.2.7 Tensor product

Let $(X, \mathcal{O}_X)$ be a ringed space. Let $\mathcal{F}, \mathcal{G}$ be $\mathcal{O}_X$-modules. We define first the tensor product presheaf

$$\mathcal{F} \otimes_{p, \mathcal{O}_X} \mathcal{G}$$

as the rule which assigns to $U \subseteq X$ open the $\mathcal{O}_X(U)$-module $\mathcal{F}(U)_{\mathcal{O}_X(U)}\mathcal{G}(U)$. Having defined this we define the tensor product sheaf as the sheafification of the above:

$$\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G} = (\mathcal{F} \otimes_{p, \mathcal{O}_X} \mathcal{G})^\#$$

This can be characterized as the sheaf of $\mathcal{O}_X$-modules such that for any third sheaf of $\mathcal{O}_X$-modules $\mathcal{H}$ we have

$$\mathrm{Hom}_{\mathcal{O}_X}(\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G}, \mathcal{H}) = \mathrm{Bilin}_{\mathcal{O}_X}(\mathcal{F} \times \mathcal{G}, \mathcal{H}).$$

Here the right hand side indicates the set of bilinear maps of sheaves of $\mathcal{O}_X$-modules.

The tensor product of modules M, N over a ring R satisfies symmetry, hence the same holds for tensor products of sheaves of modules, i.e., we have

$$\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G} = \mathcal{G} \otimes_{\mathcal{O}_X} \mathcal{F}$$

functorial in $\mathcal{F}$, $\mathcal{G}$. And since tensor product of modules satisfies associativity we also get canonical functorial isomorphisms

$$(\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G}) \otimes_{\mathcal{O}_X} \mathcal{H} = \mathcal{F} \otimes_{\mathcal{O}_X} (\mathcal{G} \otimes_{\mathcal{O}_X} \mathcal{H}).$$

functorial in $\mathcal{F}, \mathcal{G}$, and $\mathcal{H}$.

Proposition 19.2.25. *Let $(X, \mathcal{O}_X)$ be a ringed space. Let $\mathcal{F}$, $\mathcal{G}$ be $\mathcal{O}_X$-modules. Let $x \in X$. There is a canonical isomorphism of $\mathcal{O}_{X,x}$-modules*

$$(\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G})_x = \mathcal{F}_x \otimes_{\mathcal{O}_{X,x}} \mathcal{G}_x.$$

functorial in $\mathcal{F}$ and $\mathcal{G}$.

Proposition 19.2.26. *Let $(X, \mathcal{O}_X)$ be a ringed space. Let $\mathcal{F}', \mathcal{G}'$ be presheaves of $\mathcal{O}_X$-modules with sheafifications $\mathcal{F}, \mathcal{G}$. Then $\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G} = (\mathcal{F}' \otimes_{p,\mathcal{O}_X} \mathcal{G}')^{\#}$.*

Proof. On stalks we have

$$(\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G})_x = \mathcal{F}_x \otimes_{\mathcal{O}_{X,x}} \mathcal{G}_x = \mathcal{F}'_x \otimes_{\mathcal{O}_{X,x}} \mathcal{G}'_x = \mathcal{F}'_x \otimes_{p,\mathcal{O}_{X,x}} \mathcal{G}'_x$$

Thus by Proposition 19.1.17 we conclude the result. □

Proposition 19.2.27. *Let $(X, \mathcal{O}_X)$ be a ringed space. Let $\mathcal{G}$ be an $\mathcal{O}_X$-module. If $\mathcal{F}_1 \to \mathcal{F}_2 \to \mathcal{F}_3 \to 0$ is an exact sequence of $\mathcal{O}_X$-modules then the induced sequence*

$$\mathcal{F}_1 \otimes_{\mathcal{O}_X} \mathcal{G} \to \mathcal{F}_2 \otimes_{\mathcal{O}_X} \mathcal{G} \to \mathcal{F}_3 \to 0$$

is exact.

Proof. This follows from the fact that exactness may be checked at stalks, the description of stalks and the corresponding result for tensor products of modules □

Proposition 19.2.28. *Let $f : X \to Y$ be a morphism of ringed spaces. Let $\mathcal{F}, \mathcal{G}$ be $\mathcal{O}_Y$-modules. Then $f^*(\mathcal{F} \otimes_{\mathcal{O}_Y} \mathcal{G}) = f^*\mathcal{F} \otimes_{\mathcal{O}_X} f^*\mathcal{G}$ functorially in $\mathcal{F}, \mathcal{G}$.*

Proof. Let $x \in X$, we check that

$$\begin{aligned}
\left(f^*(\mathcal{F} \otimes_{\mathcal{O}_Y} \mathcal{G})\right)_x &= \mathcal{O}_{X,x} \otimes_{\mathcal{O}_{Y,f(x)}} (\mathcal{F} \otimes_{\mathcal{O}_Y} \mathcal{G})_{f(x)} = \mathcal{O}_{X,x} \otimes_{\mathcal{O}_{Y,f(x)}} (\mathcal{F}_{f(x)} \otimes_{\mathcal{O}_{Y,f(x)}} \mathcal{G}_{f(x)}) \\
&= \mathcal{O}_{X,x} \otimes_{\mathcal{O}_{X,x}} \mathcal{O}_{X,x} \otimes_{\mathcal{O}_{Y,f(x)}} \mathcal{F}_{f(x)} \otimes_{\mathcal{O}_{Y,f(x)}} \mathcal{G}_{f(x)} \\
&= \mathcal{O}_{X,x} \otimes_{\mathcal{O}_{Y,f(x)}} \mathcal{F}_{f(x)} \otimes_{\mathcal{O}_{X,x}} \mathcal{O}_{X,x} \otimes_{\mathcal{O}_{Y,f(x)}} \mathcal{G}_{f(x)} \\
&= (f^*\mathcal{F})_x \otimes_{X,x} (f^*\mathcal{G})_x.
\end{aligned}$$

as desired. □

Proposition 19.2.29. *Let $(X, \mathcal{O}_X)$ be a ringed space. Let $\mathcal{F}, \mathcal{G}$ be $\mathcal{O}_X$-modules.*

(i) If $\mathcal{F}, \mathcal{G}$ are locally generated by sections, so is $\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G}$.

(ii) If $\mathcal{F}, \mathcal{G}$ are of finite type, so is $\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G}$.

(iii) If $\mathcal{F}, \mathcal{G}$ are quasi-coherent, so is $\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G}$.

(iv) If $\mathcal{F}, \mathcal{G}$ are of finite presentation, so is $\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G}$.

(v) If $\mathcal{F}$ is of finite presentation and $\mathcal{G}$ is coherent, then $\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G}$ is coherent.

(vi) If $\mathcal{F}, \mathcal{G}$ are coherent, so is $\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G}$.

(vii) If $\mathcal{F}, \mathcal{G}$ are locally free, so is $\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G}$.

Proof. We first prove that the tensor product of locally free $\mathcal{O}_X$-modules is locally free. This follows if we show that

$$(\bigoplus_{i\in I} \mathcal{O}_X) \otimes_{\mathcal{O}_X} (\bigoplus_{j\in J} \mathcal{O}_X) \cong \bigoplus_{(i,j)\in I\times J} \mathcal{O}_X.$$

The sheaf $\bigoplus_{i\in I} \mathcal{O}_X$ is the sheaf associated to the presheaf $U \mapsto \bigoplus_{i\in I} \mathcal{O}_X(U)$. Hence the tensor product is the sheaf associated to the presheaf

$$U \mapsto \Big(\bigoplus_{i\in I} \mathcal{O}_X(U)\Big) \otimes_{\mathcal{O}_X(U)} \Big(\bigoplus_{j\in J} \mathcal{O}_X(U)\Big).$$

We deduce what we want since for any ring R we have $(\bigoplus_{i\in I} R) \otimes_R (\bigoplus_{j\in J} R) \cong \bigoplus_{(i,j)\in I\times J} R$.

If $\mathcal{F}_2 \to \mathcal{F}_1 \to \mathcal{F} \to 0$ is exact, then by Proposition 19.2.27 the complex $\mathcal{F}_2 \otimes \mathcal{G} \to \mathcal{F}_1 \otimes \mathcal{G} \to \mathcal{F} \otimes \mathcal{G} \to 0$ is exact. Using this we can prove (v). Namely, in this case there exists locally such an exact sequence with $\mathcal{F}_i, i = 1, 2$ finite free. Hence the two terms $\mathcal{F}_i \otimes \mathcal{G}$ are isomorphic to finite direct sums of $\mathcal{G}$. Since finite direct sums are coherent sheaves, these are coherent and so is the cokernel of the map.

If we also have another exact sequence $\mathcal{G}_2 \to \mathcal{G}_1 \to \mathcal{G} \to 0$, then tensoring together we get an exact sequence

$$(\mathcal{F}_2 \otimes \mathcal{G}_1) \oplus (\mathcal{F}_1 \otimes \mathcal{G}_2) \longrightarrow \mathcal{F}_1 \otimes \mathcal{G}_1 \longrightarrow \mathcal{F} \otimes \mathcal{G} \longrightarrow 0$$

This can be used to prove $(i), (ii), (iii), (iv), (vi)$. □

Proposition 19.2.30. *Let $(X, \mathcal{O}_X)$ be a ringed space. For any $\mathcal{O}_X$-module $\mathcal{F}$ the functor $\mathcal{F} \otimes_{\mathcal{O}_X}$ commutes with arbitrary colimits.*

Proof. Let I be a partially ordered set and let $\{\mathcal{G}_i\}$ be a system over I. Set $\mathcal{G} = \varinjlim_i \mathcal{G}_i$. Recall that $\mathcal{G}$ is the sheaf associated to the presheaf $\mathcal{G}' : U \mapsto \varinjlim_i \mathcal{G}_i(U)$. By the tensor product $\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G}$ is the sheafification of the presheaf

$$U \mapsto \mathcal{F}(U) \otimes_{\mathcal{O}_X(U)} \varinjlim_i \mathcal{G}_i(U) = \varinjlim_i \mathcal{F}(U) \otimes_{\mathcal{O}_X(U)} \mathcal{G}_i(U)$$

where the equality sign follows from the property of tensor product of modules. Hence the lemma follows from the description of colimits in $\mathbf{Mod}(\mathcal{O}_X)$. □

19.2.8 Internal Hom

Let $(X, \mathcal{O}_X)$ be a ringed space. Let $\mathcal{F}, \mathcal{G}$ be $\mathcal{O}_X$-modules. Consider the rule

$$U \mapsto \mathrm{Hom}_{\mathcal{O}_X|_U}(\mathcal{F}|_U, \mathcal{G}|_U)$$

It follows from Proposition 19.1.41 that this is a sheaf of abelian groups. In addition, given an element $\varphi \in \mathrm{Hom}_{\mathcal{O}_X|_U}(\mathcal{F}|_U, \mathcal{G}|_U)$ and a section $f \in \mathcal{O}_X(U)$ then we can define $f\varphi \in \mathrm{Hom}_{\mathcal{O}_X|_U}(\mathcal{F}|_U, \mathcal{G}|_U)$ by either precomposing with multiplication by f on $\mathcal{F}|_U$ or postcomposing with multiplication by f on $\mathcal{G}|_U$ (it gives the same result). Hence we in fact get a sheaf of $\mathcal{O}_X$-modules. We will denote this sheaf $\mathcal{H}om_{\mathcal{O}_X}(\mathcal{F}, \mathcal{G})$. For every $x \in X$ there is also a canonical morphism

$$\mathcal{H}om_{\mathcal{O}_X}(\mathcal{F}, \mathcal{G})_x \to \mathrm{Hom}_{\mathcal{O}_{X,x}}(\mathcal{F}_x, \mathcal{G}_x)$$

which is rarely an isomorphism.

Proposition 19.2.31. *Let $(X, \mathcal{O}_X)$ be a ringed space. Let $\mathcal{F}, \mathcal{G}, \mathcal{H}$ be $\mathcal{O}_X$-modules. There is a canonical isomorphism*

$$\mathcal{H}om_{\mathcal{O}_X}(\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G}, \mathcal{H}) \to \mathcal{H}om_{\mathcal{O}_X}(\mathcal{F}, \mathcal{H}om_{\mathcal{O}_X}(\mathcal{G}, \mathcal{H}))$$

which is functorial in all three entries. In particular, to give a morphism $\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G} \to \mathcal{H}$ is the same as giving a morphism $\mathcal{F} \to \mathcal{H}om_{\mathcal{O}_X}(\mathcal{G}, \mathcal{H})$.

Proof. This is the analogue of that for modules. □

Due to this proposition, the functors $\mathcal{H}om(-, \mathcal{G})$ and $\mathcal{H}om(\mathcal{F}, -)$ are left-exact.

Proposition 19.2.32. *Let $(X, \mathcal{O}_X)$ be a ringed space. Let $\mathcal{F}, \mathcal{G}$ be $\mathcal{O}_X$-modules.*

- *If $\mathcal{F}_2 \to \mathcal{F}_1 \to \mathcal{F} \to 0$ is an exact sequence of $\mathcal{O}_X$-modules, then*

$$0 \longrightarrow \mathcal{H}om(\mathcal{F}, \mathcal{G}) \longrightarrow \mathcal{H}om(\mathcal{F}_1, \mathcal{G}) \longrightarrow \mathcal{H}om(\mathcal{F}_2, \mathcal{G})$$

  is exact.

- *If $0 \to \mathcal{G} \to \mathcal{G}_1 \to \mathcal{G}_2 \to 0$ is an exact sequence of $\mathcal{O}_X$-modules, then*

$$0 \longrightarrow \mathcal{H}om(\mathcal{F}, \mathcal{G}) \longrightarrow \mathcal{H}om(\mathcal{F}, \mathcal{G}_1) \longrightarrow \mathcal{H}om(\mathcal{F}, \mathcal{G}_2)$$

  is exact.

Proposition 19.2.33. *Let $(X, \mathcal{O}_X)$ be a ringed space. Let $\mathcal{F}, \mathcal{G}$ be $\mathcal{O}_X$-modules. If $\mathcal{F}$ is finitely presented then the canonical map*

$$\mathcal{H}om_{\mathcal{O}_X}(\mathcal{F}, \mathcal{G})_x \to \mathrm{Hom}_{\mathcal{O}_{X,x}}(\mathcal{F}_x, \mathcal{G}_x)$$

is an isomorphism.

Proof. By localizing on X we may assume that $\mathcal{F}$ has a presentation

$$\bigoplus_{j=1}^m \mathcal{O}_X \longrightarrow \bigoplus_{i=1}^n \mathcal{O}_X \longrightarrow \mathcal{F} \longrightarrow 0$$

Then this gives an exact sequence

$$0 \longrightarrow \mathcal{H}om_{\mathcal{O}_X}(\mathcal{F}, \mathcal{G}) \longrightarrow \bigoplus_{i=1}^n \mathcal{G} \longrightarrow \bigoplus_{j=1}^m \mathcal{G}$$

Taking stalks we get an exact sequence

$$0 \longrightarrow \mathcal{H}om_{\mathcal{O}_X}(\mathcal{F}, \mathcal{G})_x \longrightarrow \bigoplus_{i=1}^n \mathcal{G}_x \longrightarrow \bigoplus_{j=1}^m \mathcal{G}_x$$

The result now follows since $\mathcal{F}_x$ sits in an exact sequence

$$\bigoplus_{j=1}^m \mathcal{O}_{X,x} \longrightarrow \bigoplus_{i=1}^n \mathcal{O}_{X,x} \longrightarrow \mathcal{F}_x \longrightarrow 0$$

which induces the exact sequence

$$0 \longrightarrow \mathrm{Hom}_{\mathcal{O}_{X,x}}(\mathcal{F}_x, \mathcal{G}_x) \longrightarrow \bigoplus_{i=1}^n \mathcal{G}_x \longrightarrow \bigoplus_{j=1}^m \mathcal{G}_x$$

which is the same as the one above. □

Proposition 19.2.34. *Let $f : X \to Y$ be a morphism of ringed spaces. Let $\mathcal{F}, \mathcal{G}$ be $\mathcal{O}_Y$-modules. If $\mathcal{F}$ is finitely presented then the canonical map*

$$f^*\mathcal{H}om_{\mathcal{O}_Y}(\mathcal{F}, \mathcal{G}) \to \mathcal{H}om_{\mathcal{O}_X}(f^*\mathcal{F}, f^*\mathcal{G})$$

is an isomorphism.

Proof. Note that $f^*\mathcal{F}$ is also finitely presented. Let $x \in X$ map to $y \in Y$. Looking at the stalks at x we get an isomorphism by Proposition 19.2.33 and that in this case Hom commutes with base change by $\mathcal{O}_{Y,y} \to \mathcal{O}_{X,x}$. □

Proposition 19.2.35. *Let $(X, \mathcal{O}_X)$ be a ringed space. Let $\mathcal{F}, \mathcal{G}$ be $\mathcal{O}_X$-modules. If $\mathcal{F}$ is finitely presented then the sheaf $\mathcal{H}om_{\mathcal{O}_X}(\mathcal{F}, \mathcal{G})$ is locally a kernel of a map between finite direct sums of copies of $\mathcal{G}$. In particular, if $\mathcal{G}$ is coherent then $\mathcal{H}om_{\mathcal{O}_X}(\mathcal{F}, \mathcal{G})$ is coherent too.*

Proof. The first assertion we saw in the proof of Proposition 19.2.33. And the result for coherent sheaves then follows from Proposition 19.4.18. □

Proposition 19.2.36. *Let X be a topological space. Let $\mathcal{O}_1 \to \mathcal{O}_2$ be a homomorphism of sheaves of rings. Then we have*

$$\mathrm{Hom}_{\mathcal{O}_1}(\mathcal{F}_{\mathcal{O}_1}, \mathcal{G}) = \mathrm{Hom}_{\mathcal{O}_2}(\mathcal{F}, \mathcal{H}om_{\mathcal{O}_1}(\mathcal{O}_2, \mathcal{G}))$$

bifunctorially in $\mathcal{F} \in \mathbf{Mod}(\mathcal{O}_2)$ and $\mathcal{G} \in \mathbf{Mod}(\mathcal{O}_1)$.

Proof. This is the analogue of the result for modules. □

19.2.9 The abelian category of sheaves of modules

Let $(X, \mathcal{O}_X)$ be a ringed space. Let $\mathcal{F}, \mathcal{G}$ be sheaves of $\mathcal{O}_X$-modules. Let $\varphi, \psi : \mathcal{F} \to \mathcal{G}$ be morphisms of sheaves of $\mathcal{O}_X$-modules. We define $\varphi + \psi : \mathcal{F} \to \mathcal{G}$ to be the map which on each open $U \subseteq X$ is the sum of the maps induced by φ, ψ. This is clearly again a map of sheaves of

$\mathcal{O}_X$-modules. It is also clear that composition of maps of $\mathcal{O}_X$-modules is bilinear with respect to this addition. Thus $\mathbf{Mod}(\mathcal{O}_X)$ is a pre-additive category. We will denote 0 the sheaf of $\mathcal{O}_X$-modules which has constant value $\{0\}$ for all open $U \subseteq X$. Clearly this is both a final and an initial object of $\mathbf{Mod}(\mathcal{O}_X)$. Moreover, given a pair $\mathcal{F}, \mathcal{G}$ of sheaves of $\mathcal{O}_X$-modules we may define the direct sum as

$$\mathcal{F} \oplus \mathcal{G} = \mathcal{F} \times \mathcal{G}$$

Thus $\mathbf{Mod}(\mathcal{O}_X)$ is an additive category.

Let $\varphi : \mathcal{F} \to \mathcal{G}$ be a morphism of $\mathcal{O}_X$-modules. We may define the **presheaf kernel** $\ker \varphi$ and the **presheaf cokernel** to be

$$(\ker_p \varphi)(U) = \ker \varphi_U, \quad (\operatorname{coker}_p \varphi)(U) = \operatorname{coker} \varphi_U.$$

for open subsets $U \subseteq X$. We define $\operatorname{coker} \varphi$ be the sheafification of $\operatorname{coker}_p \varphi$.

Proposition 19.2.37. *The presheaf kernel is a presheaf of $\mathcal{O}_X$-modules, so is the presheaf cokernel.*

Proof. For $U \subseteq V$ open in X, consider the diagram

$$\begin{tikzcd} 0 \arrow[r] & \ker_p \varphi_V \arrow[r, hook] \arrow[d, dashed] & \mathcal{F}(V) \arrow[r, "\varphi_V"] \arrow[d, "\mathrm{res}_U^V"] & \mathcal{G}(V) \arrow[d, "\mathrm{res}_U^V"] \\ 0 \arrow[r] & \ker_p \varphi_U \arrow[r, hook] & \mathcal{F}(U) \arrow[r, "\varphi_U"] & \mathcal{G}(U) \end{tikzcd} \tag{2.9.1}$$

By the comutativity, there is a unique map $\mathrm{res}_U^V : \ker \varphi_V \to \ker \varphi_U$ fitting in the diagram. This makes $\ker_p \varphi$ into a presheaf of $\mathcal{O}_X$-modules, and essentially the same argument works for $\operatorname{coker}_p \varphi$. □

Proposition 19.2.38. *The presheaf (co)kernel satisfies the universal property of (co)kernel in the category of presheaves of $\mathcal{O}_X$-modules.*

Proof. Let $\psi : \mathcal{G} \to \mathcal{H}$ be another morphism of presheaves of $\mathcal{O}_X$-modules such that $(\psi \circ \varphi)_U = \psi_U \circ \varphi_U = 0$ for any $U \subseteq X$. Then we have an induced map $\tilde{\psi}_U : \ker \varphi_U \to \mathcal{H}(U)$ for each U. For $U \subseteq V$ open in X, it is easy to verify that the following commutative diagram:

$$\begin{tikzcd} \ker \varphi_V \arrow[r, "\tilde{\psi}_V"] \arrow[d, "\mathrm{res}_U^V"] & \mathcal{H}(V) \arrow[d, "\mathrm{res}_U^V"] \\ \ker \varphi_U \arrow[r, "\tilde{\psi}_U"] & \mathcal{H}(U) \end{tikzcd}$$

so $\ker \varphi$ is the kernel in the category of presheaves. A similar verification works for cokernels. □

Proposition 19.2.39. *Suppose $\varphi : \mathcal{F} \to \mathcal{G}$ is a morphism of sheaves. Then the presheaf kernel $\ker_p \varphi$ satisfies the universal property of kernels in $\mathbf{Mod}(\mathcal{O}_X)$, and the sheafification of $\operatorname{coker}_p \varphi$ satisfies the universal property of cokernels in $\mathbf{Mod}(\mathcal{O}_X)$.*

Proof. Let $U = \bigcup_i U_i$ be an open covering in X, and $s_i \in \ker \varphi(U_i)$ such that $s_i|_{U_i \cap U_j} = s_j|_{U_i \cap U_j}$ for all i, j. Then by the sheaf condition of $\mathcal{F}$, there is a unique $s \in \mathcal{F}(U)$ such that $s|_{U_i} = s_i$.

Moreover, from the diagram (2.9.1) we get

$$\left(\varphi_U(s)\right)_{U_i} = \varphi_{U_i}(s|_{U_i}) = 0.$$

Thus by the sheaf condition of $\mathscr{G}$, we conclude $\varphi_U(s) = 0$. This implies $s \in \varphi_U$, so $\ker \varphi$ is a sheaf.

For the cokernel, given any sheaf $\mathscr{E}$ and a diagram

$$\begin{tikzcd}
\mathscr{F} \arrow[r, "\varphi"] & \mathscr{G} \arrow[r, "\psi"] \arrow[d] & \mathscr{E} \\
& \operatorname{coker}_p \varphi \arrow[ur] \arrow[r] & (\operatorname{coker}_p \varphi)^{\#} \arrow[u, dashed, "\tilde{\psi}"']
\end{tikzcd}$$

we construct the map $\tilde{\psi}$ by using the universal property of $\operatorname{coker}_p \varphi$ and that of sheafification. □

In view of Proposition 19.2.39, for a morphism $\varphi : \mathscr{F} \to \mathscr{G}$, we define the kernel and cokernel of φ by

$$\ker \varphi = \ker_p \varphi, \quad \operatorname{coker} \varphi = (\operatorname{coker}_p \varphi)^{\#}.$$

Since taking stalks commutes with taking sheafification, the following result is immediate.

Proposition 19.2.40. *Suppose $\mathscr{F} \to \mathscr{G}$ is a morphism of sheaves of $\mathscr{O}_X$-modules, then for all $x \in X$, we have canonical isomorphisms*

$$(\ker \varphi)_x \cong \ker \varphi_x, \quad (\operatorname{coker} \varphi)_x \cong \operatorname{coker} \varphi_x.$$

Proof. Let $\varphi : \mathscr{F} \to \mathscr{G}$ be a morphism of sheaves. We have the commutative diagram:

$$\begin{tikzcd}
\mathscr{F}(U) \arrow[r, "\varphi_U"] \arrow[d] & \mathscr{G}(U) \arrow[d] \\
\mathscr{F}_x \arrow[r, "\varphi_x"] & \mathscr{G}_x
\end{tikzcd}$$

Let $s \in \ker \varphi_U$, then its image $\bar{s}$ is mapped to zero by φ_x, so $\bar{s} \in \ker \varphi_x$. Conversely, if $\bar{s} \in \ker \varphi_x$ and $\bar{s} = (U, s)$ where $s \in \mathscr{F}(U)$, then the image of $t = \varphi(s) \in \mathscr{G}(U)$ is zero in $\mathscr{G}_x$. Therefore in some neighborhood, say $V \subseteq U$, $t|_V = 0$. Then we have the commutative diagram

$$\begin{tikzcd}
\mathscr{F}(V) \arrow[r, "\varphi_V"] \arrow[d] & \mathscr{G}(V) \arrow[d] \\
\mathscr{F}_x \arrow[r, "\varphi_x"] & \mathscr{G}_x
\end{tikzcd}$$

where now $\varphi_V(s|_V) = 0$. This shows $\bar{s} \in (\ker \varphi)_p$. The proof is similar for cokernels. □

Now that we kernel and cokernels, we can prove that $\mathbf{Mod}(\mathscr{O}_X)$ is an abelian category.

Theorem 19.2.41. *Let $(X, \mathscr{O}_X)$ be a ringed space. The category $\mathbf{Mod}(\mathscr{O}_X)$ is an abelian category. Moreover, a complex $\mathscr{F} \to \mathscr{G} \to \mathscr{H}$ is exact at $\mathscr{G}$ if and only if for all $x \in X$ the complex $\mathscr{F}_x \to \mathscr{G}_x \to \mathscr{H}_x$ is exact at $\mathscr{G}_x$.*

Proof. We have to show that image and coimage agree. By Proposition 19.1.10 it is enough to show that image and coimage have the same stalk at every $x \in X$. By the constructions of kernels and cokernels above these stalks are the coimage and image in the categories of $\mathcal{O}_{X,x}$-modules. Thus we get the result from the fact that the category of modules over a ring is abelian. □

Actually the category $\mathbf{Mod}(\mathcal{O}_X)$ has many more properties. Here are two constructions we can do.

- Given any set I and for each $i \in I$ a $\mathcal{O}_X$-module we can form the product
$$\prod_{i \in I} \mathcal{F}_i$$
which is the sheaf that associates to each open U the product of the modules $\mathcal{F}_i(U)$.
- Given any set I and for each $i \in I$ a $\mathcal{O}_X$-module we can form the direct sum
$$\bigoplus_{i \in I} \mathcal{F}_i$$
which is the sheafification of the presheaf that associates to each open U the direct sum of the modules $\mathcal{F}_i(U)$.

Using these we conclude that all limits and colimits exist in $\mathbf{Mod}(\mathcal{O}_X)$.

Proposition 19.2.42. *Let $(X, \mathcal{O}_X)$ be a ringed space.*

(a) All limits exist in $\mathbf{Mod}(\mathcal{O}_X)$. Limits are the same as the corresponding limits of presheaves of $\mathcal{O}_X$-modules.

(b) All colimits exist in $\mathbf{Mod}(\mathcal{O}_X)$. Colimits are the sheafification of the corresponding colimit in the category of presheaves. Taking colimits commutes with taking stalks.

(c) Filtered colimits are exact.

(d) Finite direct sums are the same as the corresponding finite direct sums of presheaves of $\mathcal{O}_X$-modules.

Proof. As $\mathbf{Mod}(\mathcal{O}_X)$ is abelian it has all finite limits and colimits. Thus the existence of limits and colimits and their description follows from the existence of products and coproducts and their description. Since sheafification commutes with taking stalks we see that colimits commute with taking stalks. Part (c) signifies that given a system $0 \to \mathcal{F}_i \to \mathcal{G}_i \to \mathcal{H}_i \to 0$ of exact sequences of $\mathcal{O}_X$-modules over a directed partially ordered set I the sequence $0 \to \varinjlim_i \mathcal{F}_i \to \varinjlim_i \mathcal{G}_i \to \varinjlim_i \mathcal{H}_i \to 0$ is exact as well. Since we can check exactness on stalks, this follows from the case of modules. Part (d) comes from the fact that finite direct sum coincides with finite product in an Abelian category. □

Remark 19.2.1. For an arbitrary direct sum $\bigoplus_{i \in I} \mathcal{O}_X$, by the construction of sheafification we see that an element $s \in \bigoplus_{i \in I} \mathcal{O}_X$ satisfies the following property: For any $x \in X$ there is a neighborhood of x such that $s|_U$ is a finite sum $\sum_{i \in I'} f_i$ with $f_i \in \mathcal{O}_X(U)$.

The existence of limits and colimits allows us to consider exactness properties of functors defined on the category of $\mathscr{O}_X$-modules in terms of limits and colimits.

Proposition 19.2.43. *Let $(f, f^\#) : (X, \mathscr{O}_X) \to (Y, \mathscr{O}_Y)$ be a morphism of ringed spaces.*

(a) The functor $f_* : \mathbf{Mod}(\mathscr{O}_X) \to \mathbf{Mod}(\mathscr{O}_Y)$ is left exact. In fact it commutes with all limits.

(b) The functor $f^* : \mathbf{Mod}(\mathscr{O}_X) \to \mathbf{Mod}(\mathscr{O}_Y)$ is right exact. In fact it commutes with all colimits.

(c) The functor $f^{-1} : \mathbf{Ab}(Y) \to \mathbf{Ab}(X)$ on abelian sheaves is exact.

Proof. Recall that (f^*, f_*) is an adjoint pair of functors. The last part holds because exactness can be checked on stalks and the description of stalks of the pullback. □

Proposition 19.2.44. *Let $j : U \to X$ be an open immersion of topological spaces. The functor $j_! : \mathbf{Ab}(U) \to \mathbf{Ab}(X)$ is exact.*

Proof. This follows from the description of stalks given in Proposition 19.1.33. □

Proposition 19.2.45. *Let $(X, \mathscr{O}_X)$ be a ringed space. Let I be a set. For $i \in I$, let $\mathscr{F}_i$ be a sheaf of $\mathscr{O}_X$-modules. For $U \subseteq X$ quasi-compact open the map*

$$\bigoplus_{i\in I} \mathscr{F}_i(U) \to \Big(\bigoplus_{i\in I} \mathscr{F}_i\Big)(U)$$

is bijective.

Proof. If s is an element of the right hand side, then there exists an open covering $U = \bigcup_{j\in J} U_j$ such that $s|_{U_j}$ is a finite sum $\sum_{i\in I_j} s_{ji}$ with $s_{ji} \in \mathscr{F}_i(U_j)$. Because U is quasi-compact we may assume that the covering is finite, i.e., that J is finite. Then $I' = \bigcup_{j\in J} I_j$ is a finite subset of I. Clearly, s is a section of the subsheaf $\bigoplus_{i\in I'} \mathscr{F}_i$. The result follows from the fact that for a finite direct sum sheafification is not needed. □

19.3 Ringed spaces

19.3.1 Ringed spaces, $\mathscr{A}$-modules, and $\mathscr{A}$-algebras

A **ringed space** (resp. **topologically ringed space**) is defiend to be a couple $(X, \mathscr{A})$ formed by a topological space X and a sheaf of rings (resp. a sheaf of topological rings) $\mathscr{A}$ on X. We call X the topological space underling the ringed space $(X, \mathscr{A})$, and $\mathscr{A}$ is the structural sheaf. We only denote by $\mathscr{O}_X$ the structural sheaf, and for $x \in X$, $\mathscr{O}_{X,x}$ denotes the stalk of $\mathscr{O}_X$ at x. If $\mathscr{A}$ is a sheaf of commutative rings, we say $(X, \mathscr{A})$ is a **commutative ringed space**. Without further specifications, we only consider commutative ringed spaces.

The ringed spaces (resp. topologically ringed spaces) form a category, if we define a morphism $(X, \mathscr{A}) \to (Y, \mathscr{B})$ as a couple $(f, f^\#)$ formed by a continuous map $f : X \to Y$ and a f-morphism $f^\# : \mathscr{B} \to \mathscr{A}$ (that is, a morphism from $\mathscr{B}$ to $f_*(\mathscr{A})$) of sheaf of rings (resp. sheaf of topological rings). As the category of rings admits inductive limits, for any $x \in X$ we have a homomorphism $f^\#_x : \mathscr{B}_{f(x)} \to \mathscr{A}_x$. The composition of two morphisms $(f, f^\#) : (X, \mathscr{A}) \to (Y, \mathscr{B})$ and $(g, g^\#) : (Y, \mathscr{B}) \to (Z, \mathscr{C})$ is then defined to be the couple $(h, h^\#)$, where $h = g \circ f$ and $g^\#$ is the composition of $f^\#$ and $g^\#$ (which equals to $g_*(f^\#) \circ g^\#$). For any $x \in X$, we then have

$h^\#_x = g^\#_{f(x)} \circ f^\#_x$, so if the homomorphisms $f^\#$ and $f^\#$ are injective (resp. surjective), then so is $h^\#$. We then verify that, if f is a injective continuous map and $f^\#$ is a surjective homomorphism of sheaf of rings, then the morphism $(f, f^\#)$ is a monomorphism of category of ringed spaces.

By abuse of language, we only replace $(f, f^\#)$ by f, and say that $f : (X, \mathscr{A}) \to (Y, \mathscr{B})$ is a morphism of ringed spaces. In this case, it is understood that the homomorphism $f^\#$ is also given.

For any subset U of X, the couple $(U, \mathscr{A}|_U)$ is clearly a ringe space, called induced over U by $(X, \mathscr{A})$, or the restriction of $(X, \mathscr{A})$ to U. If $j : U \to X$ is the injection and $j^\# : \mathscr{A} \to j_*(\mathscr{A}|_U)$ is the canonical homomorphism, we then have a *monomorphism* $(j, j^\#) : (U, \mathscr{A}|_U) \to (X, \mathscr{A})$ of ringed spaces, called the **canonical injection**. The composition of a morphism $f : (X, \mathscr{A}) \to (Y, \mathscr{B})$ with this canonical injection is said to be the restriction of f to U, and denoted by $f|_U$.

Example 19.3.1. Let $f : X \to Y$ be a continuous map of topological spaces. Consider the sheaves of continuous real valued functions C^0_X on X and C^0_Y on Y. We claim that there is a natural f-map $f^\# : C^0_Y \to C^0_X$ associated to f. Namely, we simply define it by the rule

$$C^0_Y(V) \to C^0_X(f^{-1}(V)), \quad h \mapsto h \circ f$$

Strictly speaking we should write $f^\#(h) = h \circ f|_{f^{-1}(V)}$. It is clear that this is an f-map of sheaves of $\mathbb{R}$-algebras.

Of course there are lots of other situations where there is a canonical morphism of ringed spaces associated to a geometrical type of morphism. For example, if M, N are C^∞-manifolds and $f : M \to N$ is a smooth map, then f induces a canonical morphism of ringed spaces $(M, C^\infty_M) \to (N, C^\infty_N)$.

We will not review the definition of the $\mathscr{A}$-modules for a ringed space $(X, \mathscr{A})$. If $\mathscr{A}$ is a sheaf of commutative rings, and we replace the module structure by the algebra structure in the definition of $\mathscr{A}$-modules, we obtain the definition of an $\mathscr{A}$-algebra over X. In other words, an $\mathscr{A}$-algebra (not necessarily commutative) is an $\mathscr{A}$-module $\mathscr{C}$ endowed with a homomorphism of $\mathscr{A}$-modules $\varphi : \mathscr{C} \otimes_{\mathscr{A}} \mathscr{C} \to \mathscr{C}$ and of a section e above X, such that:

(i) the diagram

$$\begin{tikzcd} \mathscr{C} \otimes_{\mathscr{A}} \mathscr{C} \otimes_{\mathscr{A}} \mathscr{C} \arrow[r, "\varphi\otimes 1"] \arrow[d, "1\otimes\varphi"'] & \mathscr{C} \otimes_{\mathscr{A}} \mathscr{C} \arrow[d, "\varphi"] \\ \mathscr{C} \otimes_{\mathscr{A}} \mathscr{C} \arrow[r, "\varphi"] & \mathscr{C} \end{tikzcd}$$

is commutative;

(ii) for any open subset $U \subseteq X$ and any section $s \in \Gamma(U, \mathscr{C})$, we have $\varphi((e|_U) \otimes s) = \varphi(s \otimes (e|_U)) = s$.

Saying that $\mathscr{C}$ is a commutative $\mathscr{A}$-algebra amounts to the fact that the diagram

$$\begin{tikzcd} \mathscr{C} \otimes_{\mathscr{A}} \mathscr{C} \arrow[rr, "\sigma"] \arrow[dr, "\varphi"'] & & \mathscr{C} \otimes_{\mathscr{A}} \mathscr{C} \arrow[dl, "\varphi"] \\ & \mathscr{C} & \end{tikzcd}$$

is commutative, where σ is the canonical symmetry of the tensor producr $\mathscr{C} \otimes_{\mathscr{A}} \mathscr{C}$.

The homomorphism of $\mathscr{A}$ are defined just as that of $\mathscr{A}$-modules, where we replace the "modules" by "algebras". If $\mathscr{M}$ is a sub-$\mathscr{A}$-module of an $\mathscr{A}$-algebra $\mathscr{C}$, the sub-$\mathscr{A}$-algebra of $\mathscr{C}$ **generated by** $\mathscr{M}$ is the sum of images of the homomorphisms $\otimes^n \mathscr{M} \to \mathscr{C}$ (for $n \geq 0$). This is the sheaf associated with the presheaf $U \mapsto \mathscr{B}(U)$ of algebras, where $\mathscr{B}(U)$ is the sub-algebra of $\mathscr{C}(U)$ generated by the sub-module $\mathscr{M}(U)$.

We say a sheaf of rings $\mathscr{A}$ over a topological space X is **reduced** (resp. **integral**) at a point x of X if the stalk $\mathscr{A}_x$ is a reduced ring (resp. integral ring). We say that $\mathscr{A}$ is reduced if it is reduced at every point of X. Recall that a ring A is called regular if for any prime ideal $\mathfrak{p}$ of A, the local ring $A_\mathfrak{p}$ is a regular local ring. We say a sheaf of ring $\mathscr{A}$ over X is **regular at a point x** (resp. **regular**) if the stalk $\mathscr{A}_x$ is a regular local ring (resp. if $\mathscr{A}$ is regular at every point). Finally, we say that a sheaf of rings $\mathscr{A}$ over X is **normal at a point x** (resp. **normal**) if the stalk $\mathscr{A}_x$ is an integrally closed ring (resp. if $\mathscr{A}$ is normal at every point). We say the ringed space $(X, \mathscr{A})$ is reduced (resp. normal, regular) if the structural sheaf $\mathscr{A}$ satisfies this property.

A **sheaf of graded rings** is by definition a sheaf or rings $\mathscr{A}$ which is the direct sum of a family $(\mathscr{A}_n)_{n\in\mathbb{Z}}$ of sheaves of abelian groups which satisfies the condition $\mathscr{A}_n\mathscr{A}_m \subseteq \mathscr{A}_{m+n}$. A graded $\mathscr{A}$-module is an $\mathscr{A}$-module $\mathscr{F}$ which is a direct sum of a family $(\mathscr{F}_n)_{n\in\mathbb{Z}}$ of sheaves of abelian groups, satisfying $\mathscr{A}_m\mathscr{F}_n \subseteq \mathscr{F}_{m+n}$.

Given a ringed space $(X, \mathscr{A})$ (commutative, and we shall not specify this condition further), we recall that definition of the bifunctors $\mathscr{F} \otimes_\mathscr{A} \mathscr{G}$, $\mathscr{H}om_\mathscr{A}(\mathscr{F}, \mathscr{G})$, and $\mathrm{Hom}_\mathscr{A}(\mathscr{F}, \mathscr{G})$ on the category of $\mathscr{A}$-modules, with values in the category of sheaves of abelian groups. the stalk $(\mathscr{F} \otimes_\mathscr{A} \mathscr{G})_x$ at any point $x \in X$ is identified canonically with $\mathscr{F}_x \otimes_{\mathscr{A}_x} \mathscr{G}_x$ and we define a functorial homomorphism $(\mathscr{H}om_\mathscr{A}(\mathscr{F}, \mathscr{G}))_x \mapsto \mathrm{Hom}_{\mathscr{A}_x}(\mathscr{F}_x, \mathscr{G}_x)$ which is, in general, neither injective nor surjective. These bifunctors are additive and, in particular, commutes with finite direct sums. The functor $\mathscr{F} \otimes_\mathscr{A} \mathscr{G}$ is right exact on $\mathscr{F}$ and $\mathscr{G}$, commutes with inductive limits, and $\mathscr{A} \otimes_\mathscr{A} \mathscr{G}$ (resp. $\mathscr{F} \otimes_\mathscr{A} \mathscr{A}$) is canonically identified with $\mathscr{G}$ (resp. $\mathscr{F}$). The functor $\mathscr{H}om_\mathscr{A}(\mathscr{F}, \mathscr{G})$ and $\mathrm{Hom}_\mathscr{A}(\mathscr{F}, \mathscr{G})$ are left exact on $\mathscr{F}$ and $\mathscr{G}$ (but note that $\mathscr{H}om_\mathscr{A}(-, \mathscr{G})$ and $\mathrm{Hom}_\mathscr{A}(\mathscr{F}, \mathscr{G})$ are contravariant). Moreover, $\mathscr{H}om_\mathscr{A}(\mathscr{A}, \mathscr{G})$ is canonically identified with $\mathscr{G}$, and for open subset $U \subseteq X$, we have

$$\Gamma(U, \mathscr{H}om_\mathscr{A}(\mathscr{F}, \mathscr{G})) = \mathrm{Hom}_{\mathscr{A}|_U}(\mathscr{F}|_U, \mathscr{G}|_U).$$

In particular, $\mathrm{Hom}_\mathscr{A}(\mathscr{A}, \mathscr{G})$ is identified with $\Gamma(X, \mathscr{G})$. For any $\mathscr{A}$-module $\mathscr{F}$, we denote by $\mathscr{F}^*$ the **dual** of $\mathscr{F}$, which is $\mathscr{H}om_\mathscr{A}(\mathscr{F}, \mathscr{A})$.

Finally, if $\mathscr{A}$ is a sheaf of rings and $\mathscr{F}$ is an $\mathscr{A}$-module, then $U \mapsto \bigwedge^p \Gamma(U, \mathscr{F})$ is a presheaf whose associated sheaf is an $\mathscr{A}$-module and is denoted by $\bigwedge^p \mathscr{F}$, called the **p-th exterior power** of $\mathscr{F}$. We can easily verify that the cannical map from the presheaf $U \mapsto \bigwedge^p \Gamma(U, \mathscr{F})$ to $\bigwedge^p \mathscr{F}$ is injective, and for $x \in X$, we have $(\bigwedge^p \mathscr{F})_x = \bigwedge^p (\mathscr{F}_x)$. It is clear that $\bigwedge^p \mathscr{F}$ is a covariant functor on $\mathscr{F}$. We can similarly define the functors $\boldsymbol{T}_p(\mathscr{F})$ and $\boldsymbol{S}_p(\mathscr{F})$, which are the **$p$-th tensor power** and **p-th symmetric power** of $\mathscr{F}$.

Let $\mathscr{I}$ be an ideal of $\mathscr{A}$ and $\mathscr{F}$ be an $\mathscr{A}$-module. Then we note that $\mathscr{I}\mathscr{F}$, the image of $\mathscr{I} \otimes_\mathscr{A} \mathscr{F}$ by the canonical map $\mathscr{I} \otimes_\mathbb{Z} \mathscr{F} \to \mathscr{F}$, is a sub-$\mathscr{A}$-module of $\mathscr{F}$. It is clear that for any $x \in X$, we have $(\mathscr{I}\mathscr{F})_x = \mathscr{I}_x\mathscr{F}_x$. It is immediate that $\mathscr{I}\mathscr{F}$ is also the $\mathscr{A}$-module associated sheaf of the presheaf $U \mapsto \Gamma(U, \mathscr{I})\Gamma(U, \mathscr{F})$. If $\mathscr{I}_1$, $\mathscr{I}_2$ are ideals of $\mathscr{A}$, we have $\mathscr{I}_1(\mathscr{I}_2\mathscr{F}) = (\mathscr{I}_1\mathscr{I}_2)\mathscr{F}$.

Let $(X_\lambda, \mathscr{A}_\lambda)_{\lambda\in L}$ be a family of ringed spaces; for each couple (λ, μ), suppose that we are given an open subset $V_{\lambda\mu} \subseteq X_\lambda$, and an isomorphism $\varphi_{\lambda\mu} : (V_{\mu\lambda}, \mathscr{A}_\mu|_{V_{\mu\lambda}}) \to (V_{\lambda\mu}, \mathscr{A}_\lambda|_{V_{\lambda\mu}})$ of ringed spaces, with $V_{\lambda\lambda} = X_\lambda$ and $\varphi_{\lambda\lambda}$ being the identity. Suppose moreover that, for any triple

(λ, μ, ν), we have $\varphi_{\lambda\nu} = \varphi_{\lambda\mu} \circ \varphi_{\mu\nu}$ on the open subset $V_{\lambda\mu} \cap V_{\lambda\nu}$ (glueing condition for $\varphi_{\lambda\mu}$). We can then consider the topological space obtained by glueing (via the morphism $\varphi_{\lambda\mu}$) the X_λ along $V_{\lambda\mu}$. If we identify X_λ with the corresponding open subset X'_λ of X, the hypotheses implies that $V_{\lambda\mu} \cap V_{\lambda\nu}$, $V_{\mu\nu} \cap V_{\mu\lambda}$, $V_{\nu\lambda} \cap V_{\nu\mu}$ are identified with $X'_\lambda \cap X'_\mu \cap X'_\nu$. We an then transport the ringed space structure of X_λ to X'_λ, and if $\mathscr{A}'_\lambda$ is the sheaf of rings transported by $\mathscr{A}_\lambda$, the $\mathscr{A}'_\lambda$ satisfies the glueing condition for sheaves and define a sheaf of rings $\mathscr{A}$ over X. We say that $(X, \mathscr{A})$ is the ringed space obtained by glueing $(X_\lambda, \mathscr{A}_\lambda)$ along $V_{\lambda\mu}$ via the morphisms $\varphi_{\lambda\mu}$.

Let $(X, \mathscr{O}_X)$ be a ringed space. For a section $s \in \Gamma(U, \mathscr{I}_X)$ over an open subset U of X to be **invertible**, it is necessary and sufficient that for any open cover (U_α) of U, the restriction of s to U_α is invertible in $\Gamma(U_\alpha, \mathscr{O}_X)$, in view of the uniqueness of inverse element. There then exists a sub-sheaf of multiplication groups $\mathscr{O}_X^\times$ of $\mathscr{O}_X$ such that, for any open subset U of X, $\Gamma(U, \mathscr{O}_X^\times)$ is the group of invertible elements of the ring $\Gamma(U, \mathscr{O}_X)$. For any $x \in X$, the stalk $(\mathscr{O}_X^\times)_x$ is the set of invertible elements of the ring $\mathscr{O}_{X,x}$, because if $s_x \in \mathscr{O}_{X,x}$ admits an inverse t_x in this ring, s_x and t_x are the germs of two sections s, t of $\mathscr{O}_X$ over a neighborhood V of x, and the relation $(st)_x = 1_x$ implies $st|_W = 1$ over a smaller neighborhood $W \subseteq V$ of x.

On the other hand, with the same notations, if s is a regular element (that is, not a zero divisor) of $\Gamma(U, \mathscr{O}_X)$ and V is an open subset of U, $s|_V$ is not necessarily regular in $\Gamma(V, \mathscr{O}_X)$, because if $(s|_V)t = 0$ for a section $t \in \Gamma(V, \mathscr{O}_X)$, t does not necessarily admits an extension to U. We denote by $\mathscr{S}(\mathscr{O}_X)$ the presheaf of sets such that $\mathscr{S}(\mathscr{O}_X)(U)$, for each open subset U of X, is the set of sections $s \in \Gamma(U, \mathscr{O}_X)$ whose restriction to *any* open subset $V \subseteq U$ is a regular element of the ring $\Gamma(V, \mathscr{O}_X)$. From this definition, it is clear that $\mathscr{S}(\mathscr{O}_X)$ is a sheaf, since if s is a section of $\mathscr{O}_X$ over U and $s|_V$ is regular in $\Gamma(V, \mathscr{O}_X)$ is regular for some open subset $V \subseteq U$, then s is regular in $\Gamma(U, \mathscr{O}_X)$. For a section $s \in \Gamma(U, \mathscr{O}_X)$, to be in $\mathscr{S}(\mathscr{O}_X)(U)$ amount to saying that for any open subset $V \subseteq U$, the map $t \mapsto (s|_V)$ on $\Gamma(V, \mathscr{O}_X)$ is injective (recall that we always assume that $\mathscr{O}_X$ is commutative). In this case, by the exactness of the functor $\varinjlim$ on the category of modules, it follows that for any $x \in U$, the germ s_x is regular in $\mathscr{O}_{X,x}$. Conversely, if this does not hold, then for some $x \in U$, then there exists a section $t \in \Gamma(V, \mathscr{O}_X)$ for some open subset $V \subseteq U$ such that $(s|_V)t = 0$, so $s \notin \mathscr{S}(\mathscr{O}_X)(U)$. We then say that $\mathscr{S}(\mathscr{O}_X)$ is the sheaf of sets defined by the condition that $\Gamma(U, \mathscr{O}_X)$ is the set of sections of $\Gamma(U, \mathscr{O}_X)$ whose germ at every point $x \in U$ is regular. We also note that the stalk $(\mathscr{S}(\mathscr{O}_X))_x$, which is contained in the set of regular elements of $\mathscr{O}_{X,x}$, does not necessarily equal to this set.

We say a ringed space $(X, \mathscr{O}_X)$ is **local** if for each $x \in X$, the stalk $\mathscr{O}_{X,x}$ is a local ring. In this case, we say $(X, \mathscr{O}_X)$ is a **locally ringed space**. We denote by $\mathfrak{m}_x$ the maximal idea lof $\mathscr{O}_{X,x}$ and $\kappa(x) = \mathscr{O}_{X,x}/\mathfrak{m}_x$ the residue field. For any $\mathscr{O}_X$-module $\mathscr{F}$, any open subset $U \subseteq X$, any point $x \in U$ and any section $f \in \Gamma(U, \mathscr{F})$, we denote by $f(x) \in \kappa(x)$ the class of the germ $f_x \in \mathscr{F}_x$ modulo $\mathfrak{m}_x\mathscr{F}_x$, and we say $f(x)$ is the **value** of f at x. The relation $f(x) = 0$ then signifies $f_x \in \mathfrak{m}_x\mathscr{F}_x$ (do not confuse with the condition $f_x = 0_x$). We denote by U_f the set of $x \in U$ such that $f(x) \neq 0$ (or equivalently $f_x \notin \mathfrak{m}_x\mathscr{F}_x$). We note that if $f \in \Gamma(X, \mathscr{F})$, then X_f is contained in $\operatorname{supp}(\mathscr{F})$.

Proposition 19.3.2. *Let $(X, \mathscr{O}_X)$ be a locally ringed space, $\mathscr{F}$ and $\mathscr{F}$ be two $\mathscr{O}_X$-module. For any $x \in X$, $(\mathscr{F} \otimes_{\mathscr{O}_X} \mathscr{G})_x/\mathfrak{m}_x(\mathscr{F} \otimes_{\mathscr{O}_X} \mathscr{G})_x$ is canonically identified with $(\mathscr{F}_x/\mathfrak{m}_x\mathscr{F}_x) \otimes_{\kappa(x)} (\mathscr{G}_x/\mathfrak{m}_x\mathscr{G}_x)$. If s (resp. t) is a section of $\mathscr{F}$ (resp. $\mathscr{G}$) over X, $(s \otimes t)(x)$ is identified with $s(x) \otimes t(x)$ and we have $X_{s\otimes t} = X_s \cap X_t$.*

Proof. In fact $(\mathscr{F} \otimes_{\mathscr{O}_X} \mathscr{G})_x = \mathscr{F}_x \otimes_{\mathscr{O}_{X,x}} \mathscr{G}_x$, and $(\mathscr{F}_x \otimes_{\mathscr{O}_{X,x}} \mathscr{G}_x) \otimes_{\mathscr{O}_{X,x}} (\mathscr{O}_{X,x}/\mathfrak{m}_x)$ is canonically iso-

morphic to $(\mathscr{F} \otimes_{\mathscr{O}_X} \mathscr{G})_x/\mathfrak{m}_x(\mathscr{F} \otimes_{\mathscr{O}_X} \mathscr{G})_x$, hence to $(\mathscr{F}_x/\mathfrak{m}_x\mathscr{F}_x) \otimes_{\kappa(x)} (\mathscr{G}_x/\mathfrak{m}_x\mathscr{G}_x)$. The relation $X_{s\otimes t} = X_s \cap X_t$ then follows from the fact that a product $a \otimes b$ in a tensor product of vector spaces is nonzero if and only if a and b are both nonzero. □

Proposition 19.3.3. *Let $(X, \mathscr{O}_X)$ be a locally ringed space. The set of idempotents of the ring $\Gamma(X, \mathscr{O}_X)$ corresponds to the set of clopen subsets of X. In particular, for X to be connected, it is necessary and sufficent that $\Gamma(X, \mathscr{O}_X)$ has no nontrivial idempotents.*

Proof. Let U be a clopen subset of X. Then it corresponds to the section $s \in \Gamma(X, \mathscr{O}_X)$ such that $s|_V = 1$ for any open subset $V \subseteq U$ and $s|_V = 0$ for any open subset $V \subseteq X - U$; these open subsets by hypotheses form a base for the topology of X, so we define a section $s = e_U$ of $\mathscr{O}_X$ over X, which is an idempotent of $\Gamma(X, \mathscr{O}_X)$. Conversely, if s is an idempotent, for any $x \in X$, s_x is an idempotent of $\mathscr{O}_{X,x}$, hence equal to 0_x or 1_x because $\mathscr{O}_{X,x}$ is a local ring ($s_x(1 - s_x) = 0$, and if $s_x \in \mathfrak{m}_x$, then $1 - s_x$ is invertible so $s_x = 0$). It is clear that the set U of $x \in X$ such that $s_x = 1_x$ is open, and so is the set $X - U$ of $x \in X$ such that $s_x = 0_x$, so U is a clopen subset of X and we have $s = e_U$. □

A morphism of locally ringed space $f : (X, \mathscr{O}_X) \to (Y, \mathscr{O}_Y)$ is defined to be a morphism of ringed spaces such that for each $x \in X$ the homomorphism $f_x^\# : \mathscr{O}_{Y,f(x)} \to \mathscr{O}_{X,x}$ is local. Note that by this definition, the category of locally ringed spaces is not a full subcategory of that of ringed spaces.

Proposition 19.3.4. *Let $f : X \to Y$ be a morphism of locally ringed spaces, x be a point of X, and $y = f(x)$. For any $\mathscr{O}_Y$-module $\mathscr{G}$, $(f^*(\mathscr{G}))_x/\mathfrak{m}_x(f^*(\mathscr{G}))_x$ is canonically identified with $(\mathscr{G}_y/\mathfrak{m}_y\mathscr{G}_y)\otimes_{\kappa(y)}\kappa(x)$. If t is a section of $\mathscr{G}$ over Y and $s = \rho_{\mathscr{G}}(t)$ is the corresponding section of $f^*(\mathscr{G})$ over X, then $s(x)$ is identified with $t(y) \otimes 1$ and we have $X_s = f^{-1}(Y_t)$.*

Proof. We have $(f^*(\mathscr{G}))_x = \mathscr{G}_y \otimes_{\mathscr{O}_{Y,y}} \mathscr{O}_X$, so $(f^*(\mathscr{G}))_x/\mathfrak{m}_x(f^*(\mathscr{G}))_x$ is identified with $\mathscr{G}_y \otimes_{\mathscr{O}_{Y,y}} \kappa(x)$. The homomorphism $\mathscr{O}_{Y,y} \to \mathscr{O}_{X,x}$ is local by hypotheses, so $\mathfrak{m}_y$ annihilates $\kappa(x)$ and $\mathscr{G}_y \otimes_{\mathscr{O}_{Y,y}} \kappa(x)$ is isomorphic to $(\mathscr{G}_y/\mathfrak{m}_y\mathscr{G}_y)\otimes_{\kappa(y)}\kappa(x)$. The last assertion follows from the fact that $t(y)\otimes 1 = 0$ is equivalent to $t(y) = 0$. □

19.3.2 Direct image of $\mathscr{A}$-modules

Let $(X, \mathscr{A})$ and $(Y, \mathscr{B})$ be ringed spaces, f be a morphism $(X, \mathscr{A}) \to (Y, \mathscr{B})$. Then $f_*(\mathscr{A})$ is a sheaf of rings over Y, and $f^\#$ is a homomorphism $\mathscr{B} \to f_*(\mathscr{A})$ of sheaf of rings. Let $\mathscr{F}$ be an $\mathscr{A}$-module; the direct image $f_*(\mathscr{F})$ is then a sheaf of abelian groups over Y. Moreover, for any open subset $U \subseteq Y$,

$$\Gamma(U, f_*(\mathscr{F})) = \Gamma(f^{-1}(U), \mathscr{F})$$

is endowed with a module structure over the ring $\Gamma(U, f_*(\mathscr{A})) = \Gamma(f^{-1}(U), \mathscr{A})$. These bilinear maps are compatible with restrictions, so $f_*(\mathscr{F})$ becomes an $f_*(\mathscr{A})$-module. The homomorphism $f^\# : \mathscr{B} \to f_*(\mathscr{A})$ then makes $f_*(\mathscr{F})$ a $\mathscr{B}$-module. We say that this $\mathscr{B}$-module is the direct image of $\mathscr{F}$ under the morphism f, still denoted by $f_*(\mathscr{F})$. If $\mathscr{F}_1, \mathscr{F}_2$ are two $\mathscr{A}$-modules over X and $u : \mathscr{F}_1 \to \mathscr{F}_2$ is an $\mathscr{A}$-homomorphism, it is immediate that $f_*(u)$ is an $f_*(\mathscr{A})$-homomorphism $f_*(\mathscr{F}_1) \to f_*(\mathscr{F}_2)$, and a fortiori a $\mathscr{B}$-homomorphism, also denoted by $f_*(u)$. We then see that f_* is a covariant funtor from the category of $\mathscr{A}$-modules to that of $\mathscr{B}$-modules. Moreover, it is immediate that this functor is left exact.

Over $f_*(\mathscr{A})$, the $\mathscr{B}$-module structure and the sheaf of rings structure define a structure of $\mathscr{B}$-algebras; we denote by $f_*(\mathscr{A})$ this $\mathscr{B}$-algebra. Let $(Z, \mathscr{C})$ be a third ringed space, $g : (Y, \mathscr{B}) \to (Z, \mathscr{C})$ be a morphism; if $h = g \circ f$ is the composition morphism, then we have $h_* = g_* \circ f_*$.

Let $\mathscr{M}, \mathscr{N}$ be two $\mathscr{A}$-modules. For any open subset U of Y, we have a canonical map

$$\Gamma(f^{-1}(U), \mathscr{M}) \times \Gamma(f^{-1}(U), \mathscr{N}) \to \Gamma(f^{-1}(U), \mathscr{M} \otimes_{\mathscr{A}} \mathscr{N})$$

which is bilinear over the ring $\Gamma(f^{-1}(U), \mathscr{A}) = \Gamma(U, f_*(\mathscr{A}))$, and a fortiori over $\Gamma(U, \mathscr{B})$; this defines a homomorphism

$$\Gamma(U, f_*(\mathscr{M})) \otimes_{\Gamma(U,\mathscr{B})} \Gamma(U, f_*(\mathscr{N})) \to \Gamma(U, f_*(\mathscr{M} \otimes_{\mathscr{A}} \mathscr{N}))$$

and as we can verify that these homomorphisms are compatible with restrictions, we obtain a canonical homomorphism of $\mathscr{B}$-modules

$$f_*(\mathscr{M}) \otimes_{\mathscr{B}} f_*(\mathscr{N}) \to f_*(\mathscr{M} \otimes_{\mathscr{A}} \mathscr{N}) \tag{3.2.1}$$

which in general is neither injective nor surjective. If $\mathscr{P}$ is a third $\mathscr{A}$-module, we verify that the diagram

$$\begin{array}{ccc} f_*(\mathscr{M}) \otimes_{\mathscr{B}} f_*(\mathscr{N}) \otimes_{\mathscr{B}} f_*(\mathscr{P}) & \longrightarrow & f_*(\mathscr{M} \otimes_{\mathscr{A}} \mathscr{N}) \otimes_{\mathscr{B}} f_*(\mathscr{P}) \\ \downarrow & & \downarrow \\ f_*(\mathscr{M}) \otimes_{\mathscr{B}} f_*(\mathscr{N} \otimes_{\mathscr{A}} \mathscr{P}) & \longrightarrow & f_*(\mathscr{M} \otimes_{\mathscr{A}} \mathscr{N} \otimes_{\mathscr{A}} \mathscr{P}) \end{array}$$

is commutative.

Let $\mathscr{M}, \mathscr{N}$ be two $\mathscr{A}$-modules. For any open $U \subseteq Y$, we have by definition

$$\Gamma(f^{-1}(U), \mathscr{H}om_{\mathscr{A}}(\mathscr{M}, \mathscr{N})) = \mathrm{Hom}_{\mathscr{A}|_V}(\mathscr{M}|_V, \mathscr{N}|_V),$$

where we put $V = f^{-1}(U)$. The map $u \mapsto f_*(u)$ is a homomorphism

$$\mathrm{Hom}_{\mathscr{A}|_V}(\mathscr{M}|_V, \mathscr{N}|_V) \to \mathrm{Hom}_{\mathscr{B}|_U}(f_*(\mathscr{M})|_U, f_*(\mathscr{N})|_U)$$

for the structure of $\Gamma(U, \mathscr{B})$-modules. These homomorphisms are compatible with restrictions, so define a canonical homomorphism of $\mathscr{B}$-modules

$$f_*(\mathscr{H}om_{\mathscr{A}}(\mathscr{M}, \mathscr{N})) \to \mathscr{H}om_{\mathscr{B}}(f_*(\mathscr{M}), f_*(\mathscr{N})).$$

If $\mathscr{C}$ is an $\mathscr{A}$-algebra, the composition homomorphism

$$f_*(\mathscr{C}) \otimes_{\mathscr{B}} f_*(\mathscr{C}) \to f_*(\mathscr{C} \otimes_{\mathscr{A}} \mathscr{C}) \to f_*(\mathscr{C})$$

defines on $f_*(\mathscr{C})$ a $\mathscr{B}$-algebra structure. We see that if $\mathscr{M}$ is a $\mathscr{C}$-module, $f_*(\mathscr{M})$ is an $f_*(\mathscr{C})$-module.

Consider in particular the case where X is a closed subspace of Y and f is the canonical injection $j : X \to Y$. If $\mathscr{B}' = \mathscr{B}|_X = j^{-1}(\mathscr{B})$ is the restriction of $\mathscr{B}$ to X, an $\mathscr{A}$-module $\mathscr{M}$ can be considered as a $\mathscr{B}'$-module via the homomorphism $f^\sharp : \mathscr{B}' \to \mathscr{A}$; $f_*(\mathscr{M})$ is then the $\mathscr{B}$-module inducing $\mathscr{M}$ on X and 0 elsewhere. If $\mathscr{N}$ is a second $\mathscr{A}$-module, $f_*(\mathscr{M}) \otimes_{\mathscr{B}} f_*(\mathscr{N})$ is identified

with $f_*(\mathscr{M} \otimes_{\mathscr{B}'} \mathscr{N})$ and $\mathscr{H}om_{\mathscr{B}}(f_*(\mathscr{M}), f_*(\mathscr{N}))$ with $f_*(\mathscr{H}om_{\mathscr{B}'}(\mathscr{M}, \mathscr{N}))$.

Let $(S, \mathscr{O}_S)$ be a ringed space and let $f : (X, \mathscr{O}_X) \to (S, \mathscr{O}_S)$ be a morphism of ringed spaces. If we fix S, we denote by $\mathscr{A}(X)$ (if there is no confusion) the direct image $f_*(\mathscr{O}_X)$, which is an $\mathscr{O}_S$-algebra. For any open subset U of S, we have $\mathscr{A}(f^{-1}(U)) = \mathscr{A}(X)|_U$. Simialrly, for any $\mathscr{O}_X$-module $\mathscr{F}$ (resp. any $\mathscr{O}_X$-algebra $\mathscr{B}$), we denote by $\mathscr{A}(\mathscr{F})$ (resp. $\mathscr{A}(\mathscr{B})$) the direct image $f_*(\mathscr{F})$ (resp. $f_*(\mathscr{B})$), which is an $\mathscr{A}(X)$-module (resp. an $\mathscr{A}(X)$-algebra) and also an $\mathscr{O}_S$-module (resp. $\mathscr{O}_S$-algebra).

We can define $\mathscr{A}(X)$ as a contravariant functor on X, from the category of S-ringed spaces to the category of $\mathscr{O}_S$-algebras. In fact, consider two morphisms $f : X \to S$, $g : Y \to S$ and let $h : X \to Y$ be a morphism, such that the diagram

$$\begin{tikzcd} X \arrow[rr, "h"] \arrow[dr, "f"'] & & Y \arrow[dl, "g"] \\ & S & \end{tikzcd}$$

is commutative. Then by definition $h^\# : \mathscr{O}_Y \to h_*(\mathscr{O}_X)$ is a homomorphism of sheaves of rings; we also deduce a homomorphism $g_*(h^\#) : g_*(\mathscr{O}_Y) \to g_*(h_*(\mathscr{O}_X)) = f_*(\mathscr{O}_X)$ of $\mathscr{O}_S$-algebras, which is a homomorphism $\mathscr{A}(Y) \to \mathscr{A}(X)$, denoted by $\mathscr{A}(h)$. If $h' : Y \to Z$ is a second S-morphism, then we have $\mathscr{A}(h' \circ h) = \mathscr{A}(h) \circ \mathscr{A}(h')$.

Now let $\mathscr{F}$ be an $\mathscr{O}_X$-module, $\mathscr{G}$ be an $\mathscr{O}_Y$-module, and $u : \mathscr{G} \to h_*(\mathscr{F})$ be a homomorphism of $\mathscr{O}_Y$-modules. Then $g_*(u) : g_*(\mathscr{G}) \to g_*(h_*(\mathscr{F})) = f_*(\mathscr{F})$ is a homomorphism $\mathscr{A}(\mathscr{G}) \to \mathscr{A}(\mathscr{F})$ of $\mathscr{O}_S$-modules, which we denote by $\mathscr{A}(u)$. Moreover, the couple $(\mathscr{A}(h), \mathscr{A}(u))$ is a bi-homomorphism from $\mathscr{A}(Y)$-module $\mathscr{A}(\mathscr{G})$ to the $\mathscr{A}(X)$-module $\mathscr{A}(\mathscr{F})$. The ringed space S being fixed, we can consider the couples $(X, \mathscr{F})$, where X is a S-ringed space and $\mathscr{F}$ is an $\mathscr{O}_X$-module, which form a category, and define a morphism $(X, \mathscr{F}) \to (Y, \mathscr{G})$ to be a couple (h, u), where $h : X \to Y$ is an S-morphism and $u : \mathscr{G} \to h_*(\mathscr{F})$ is a homomorphism of $\mathscr{O}_Y$-modules. We can then say that $(X, \mathscr{F}) \mapsto (\mathscr{A}(X), \mathscr{A}(\mathscr{F}))$ is a contravariant functor from this category to the cateogry of couples formed by an $\mathscr{O}_S$-algebra and a module of this algebra.

19.3.3 Inverse image of a $\mathscr{B}$-module

Let $f : (X, \mathscr{A}) \to (Y, \mathscr{B})$ be a morphism of ringed spaces. Let $\mathscr{G}$ be a $\mathscr{B}$-module and $f^{-1}(\mathscr{G})$ be the inverse image of $\mathscr{G}$, which is a sheaf of abelian groups over X. The definition of sections of $f^{-1}(\mathscr{G})$ and of $f^{-1}(\mathscr{B})$ shows that $f^{-1}(\mathscr{G})$ is canonically endowed with an $f^{-1}(\mathscr{B})$-module structure. On the other hand, the homomorphism $f^\sharp : f^{-1}(\mathscr{B}) \to \mathscr{A}$ endows $\mathscr{A}$ with an $f^{-1}(\mathscr{B})$-module structure. The tensor product $f^{-1}(\mathscr{G}) \otimes_{f^{-1}(\mathscr{B})} \mathscr{A}$ is then an $\mathscr{A}$-module, called the inverse image of $\mathscr{G}$ under the morphism $(f, f^\#)$ and denoted by $f^*(\mathscr{G})$. If $\mathscr{G}_1$, $\mathscr{G}_2$ are two $\mathscr{B}$-modules over Y and $v : \mathscr{G}_1 \to \mathscr{G}_2$ is a $\mathscr{B}$-homomorphism, $f^{-1}(v)$ is then an $f^{-1}(\mathscr{B})$-homomorphism from $f^{-1}(\mathscr{G}_1)$ to $f^{-1}(\mathscr{G}_2)$; therefore $f^{-1}(v) \otimes 1_{\mathscr{A}}$ is an $\mathscr{A}$-homomorphism $f^*(\mathscr{G}_1) \to f^*(\mathscr{G}_2)$, which we denote by $f^*(v)$. We then define f^* as a covariant functor from the category of $\mathscr{B}$-modules to that of $\mathscr{A}$-modules. Note that this functor (contrary to f^{-1}) is not in general exact, and is only right exact, since the tensor product with $\mathscr{A}$ is only right exact. We will see that f^* is the left adjoint of the functor f_*. For any $x \in X$, we have $(f^*(\mathscr{G}))_x = \mathscr{G}_{f(x)} \otimes_{\mathscr{B}_{f(x)}} \mathscr{A}_x$ in view of the formula for the stalk of tensor products. The support of $f^*(\mathscr{G})$ is tens contained in $f^{-1}(\mathrm{supp}(\mathscr{G}))$.

Let $(Z, \mathscr{C})$ be a third ringed space and $g : (Y, \mathscr{B}) \to (Z, \mathscr{C})$ be a morphism. Then if $h = g \circ f$ is the composition morphism, then it follows from the definitions that $h^* = f^* \circ g^*$.

Let $(\mathscr{G}_\lambda)$ be a inductive system of $\mathscr{B}$-modules, and $\mathscr{G} = \varinjlim \mathscr{G}_\lambda$ be the inductive limit. The canonical homomorphisms $\mathscr{G}_\lambda \to \mathscr{G}$ define an $f^{-1}(\mathscr{B})$-homomorphism $f^{-1}(\mathscr{G}_\lambda) \to f^{-1}(\mathscr{G})$, which gives a canonical homomorphism $\varinjlim f^{-1}(\mathscr{G}_\lambda) \to f^{-1}(\mathscr{G})$. As taking stalk commutes with inductive limits, this canonical homomorphism is bijective. Moreover, tensor product also commutes with inductive limits, and we then have a canonical functorial isomorphism $\varinjlim f^*(\mathscr{G}_\lambda) \cong f^*(\varinjlim \mathscr{G}_\lambda)$ of $\mathscr{A}$-modules.

On the other hand, for a finite direct sum $\bigoplus_i \mathscr{G}_i$ of $\mathscr{B}$-modules, it is clear that

$$f^*(\bigoplus_i \mathscr{G}_i) = \bigoplus_i f^*(\mathscr{G}_i).$$

By passing to inductive limits, we then deduce that, in view of the preceding, that this equality holds for arbitrary direct sums.

Let $\mathscr{G}_1, \mathscr{G}_2$ be two $\mathscr{B}$-modules; from the definition of inverse images of sheaves of abelian groups we deduce a canonical homomorphism

$$f^{-1}(\mathscr{G}_1) \otimes_{f^{-1}(\mathscr{B})} f^{-1}(\mathscr{G}_2) \to f^{-1}(\mathscr{G}_1 \otimes_{\mathscr{B}} \mathscr{G}_2)$$

of $f^{-1}(\mathscr{B})$, and since the stalk of a tensor product is the rensor product of stalks, this homomorphism is an isomorphism. By tensoring with $\mathscr{A}$, we then deduce a canonical isomorphism

$$f^*(\mathscr{G}_1) \otimes_{\mathscr{A}} f^*(\mathscr{G}_2) \xrightarrow{\sim} f^*(\mathscr{G}_1 \otimes \mathscr{G}_2). \tag{3.3.1}$$

Let $\mathscr{C}$ be a $\mathscr{B}$-algebra. The algebra structure over $\mathscr{C}$ is given by a $\mathscr{B}$-homomorphism $\mathscr{C} \otimes_{\mathscr{B}} \mathscr{C} \to \mathscr{C}$ satisfying the associativity and commutativity conditions (which can be verified on stalks); the isomorphism (3.3.1) then provides a homomorphism $f^*(\mathscr{C}) \otimes_{\mathscr{A}} f^*(\mathscr{C}) \to f^*(\mathscr{C})$ satisfying the same conditions, whence $f^*(\mathscr{C})$ is endowed with an $\mathscr{A}$-algebra structure. In particular, it follows from the definitions that the $\mathscr{A}$-algebra $f^*(\mathscr{B})$ is equal to $\mathscr{A}$. If $\mathscr{C}_1, \mathscr{C}_2$ are two $\mathscr{B}$-algebras and $v : \mathscr{C}_1 \to \mathscr{C}_2$ is a homomorphism of $\mathscr{B}$-algebras, then $f^*(v) : f^*(\mathscr{C}_1) \to f^*(\mathscr{C}_2)$ is a homomorphism of $\mathscr{A}$-algebras.

Similarly, if $\mathscr{M}$ is a $\mathscr{C}$-module, then a $\mathscr{B}$-module structure is given by a $\mathscr{B}$-homomorphism $\mathscr{C} \otimes_{\mathscr{B}} \mathscr{M} \to \mathscr{M}$ satisfying the associativity condition; by transporting structure, we see that $f^*(\mathscr{C})$ is endowed with a $f^*(\mathscr{C})$-module structure.

Let $\mathscr{I}$ be an ideal of $\mathscr{B}$; as the functor f^{-1} is exact, the $f^{-1}(\mathscr{B})$-module $f^{-1}(\mathscr{I})$ is canonically identified an ideal of $f^{-1}(\mathscr{B})$; the canonical injection $f^{-1}(\mathscr{I}) \to f^{-1}(\mathscr{B})$ then gives a homomorphism of $\mathscr{A}$-modules

$$f^*(\mathscr{I}) = f^{-1}(\mathscr{I}) \otimes_{f^{-1}(\mathscr{B})} \mathscr{A} \to \mathscr{A};$$

we denote by $f^*(\mathscr{I})\mathscr{A}$, or simply $\mathscr{I}\mathscr{A}$ if there is no confusion, the image of $f^*(\mathscr{I})$ under this hommorphism. We then have $\mathscr{I}\mathscr{A} = f^\sharp(f^{-1}(\mathscr{I}))\mathscr{A}$ and in particular, for any $x \in X$, $(\mathscr{I}\mathscr{A})_x = f_x^\sharp(\mathscr{I}_{f(x)})\mathscr{A}_x$, in view of the canonical identification of the stalk $f^{-1}(\mathscr{I})$. If $\mathscr{I}_1, \mathscr{I}_2$ are two ideals of $\mathscr{B}$, we have $(\mathscr{I}_1\mathscr{I}_2)\mathscr{A} = \mathscr{I}_1(\mathscr{I}_2\mathscr{A}) = (\mathscr{I}_1\mathscr{A})(\mathscr{I}_2\mathscr{A})$. If $\mathscr{F}$ is an $\mathscr{A}$-module, we put $\mathscr{I}\mathscr{F} = (\mathscr{I}\mathscr{A})\mathscr{F}$.

Remark 19.3.1. Over any topological space, we can define a canonical sheaf of rings $\mathbb{Z}_X$, which is the constant sheaf associated the presheaf $U \mapsto \mathbb{Z}$. It is clear thet the sheaves of abelian

groups over X are identified with the $\mathbb{Z}_X$-modules over the ringed space $(X, \mathbb{Z}_X)$, and we can in particular consider the tensor product $\mathscr{F} \otimes_{\mathbb{Z}_X} \mathscr{G}$ of two sheaves of rings $\mathscr{F}, \mathscr{G}$ over X. If $f : X \to Y$ is a continuous map, for any open subset V of Y, we have a canonical homomorphism $\mathbb{Z} \to \Gamma(f^{-1}(V), \mathbb{Z}_X)$ of rings and this defines a homomorphism $f^{\#} : \mathbb{Z}_Y \to f_*(\mathbb{Z}_X)$ of sheaves of rings over Y. We then obtain a morphism $(f, f^{\#}) : (X, \mathbb{Z}_X) \to (Y, \mathbb{Z}_Y)$ of ringed spaces. If $\mathscr{F}$ is a sheaf of abelian groups over Y, $f^*(\mathscr{F})$ is canonically identified with $f^{-1}(\mathscr{F})$; if $\mathscr{F}, \mathscr{G}$ are two sheves of abelian groups over Y, we then have a canonical isomorphism $f^{-1}(\mathscr{F} \otimes_{\mathbb{Z}_Y} \mathscr{G}) = f^{-1}(\mathscr{F}) \otimes_{\mathbb{Z}_X} f^{-1}(\mathscr{G})$. We then deduce that if f is a quasi-homeomorphism, f^{-1} is not only an equivalence from the category of sheaf of abelian groups over Y to that of sheaf of abelian groups over X, but also an equivalence from the category of sheaf of rings over Y to that of sheaf of rings over X.

Given two ringed spaces $(X, \mathscr{O}_X)$, $(Y, \mathscr{O}_Y)$, we say a morphism $f : (X, \mathscr{O}_X) \to (Y, \mathscr{O}_Y)$ is a **quasi-isomorphism** if f is a quasi-homeomorphism and $f^{\sharp} : f^{-1}(\mathscr{O}_Y) \to \mathscr{O}_X$ is an isomorphism of sheaf of rings. If this is the case, the ringed space $(X, \mathscr{O}_X)$ is entirely determined up to isomorphism, by $(Y, \mathscr{O}_Y)$, the space X, and the quasi-homeomorphism.

If f is a quasi-isomorphism of ringed spaces, the functor $\mathscr{F} \to f^*(\mathscr{F})$ is an equivalence from category of $\mathscr{O}_Y$-modules to the category of $\mathscr{O}_X$-modules, since $f^*(\mathscr{F})$ is identified with $f^{-1}(\mathscr{F})$. We then conclude for example the isomorphisms of bi-∂-functors

$$\mathrm{Ext}^i_{\mathscr{O}_Y}(\mathscr{F}, \mathscr{G}) \xrightarrow{\sim} \mathrm{Ext}^i_{\mathscr{O}_X}(f^*(\mathscr{F}), f^*(\mathscr{G})).$$

In general, we can say that the usual constructions of the sheaf theory and homological algebra on the ringed space Y or X, are equivalent.

19.3.4 Relations of direct images and inverse images

Again we let $f : (X, \mathscr{O}_X) \to (Y, \mathscr{O}_Y)$ be a morphism of ringed spaces. By definition, a homomorphism $u : \mathscr{G} \to f_*(\mathscr{F})$ of $\mathscr{B}$-modules is called an **f-morphism** from $\mathscr{G}$ to $\mathscr{F}$ and we denote it by $u : \mathscr{G} \to \mathscr{F}$ if there is no confusion. Given such a homomorphism, for any couple (U, V) where U is an open subset of X and V is an open subset of Y such that $f(U) \subseteq V$, a **homomorphism** $u_{U,V} : \Gamma(V, \mathscr{G}) \to \Gamma(U, \mathscr{F})$ of $\Gamma(V, \mathscr{B})$ modules, where $\Gamma(U, \mathscr{F})$ is considered as a $\Gamma(V, \mathscr{B})$-module via the ring homomorphism $f^{\sharp}_{U,V} : \Gamma(V, \mathscr{B}) \to \Gamma(U, \mathscr{A})$. The homomorphisms $u_{U,V}$ fits into the commutative diagram

$$\begin{tikzcd} \mathscr{G}(V) \arrow[r, "u_{U,V}"] \arrow[d] & \mathscr{F}(U) \arrow[d] \\ \mathscr{G}(V') \arrow[r, "u_{U',V'}"] & \mathscr{F}(U') \end{tikzcd}$$

for $U' \subseteq U$, $V' \subseteq V$, $f(U') \subseteq V'$. Moreover, for the homomorphism u, it suffices to define $u_{U,V}$ for U (resp. V) in a base $\mathscr{B}$ (resp. $\mathscr{B}'$) of the topology of X (resp. Y). Let $g : (Y, \mathscr{B}) \to (Z, \mathscr{C})$ be another morphism and $h = g \circ f$. Let $\mathscr{H}$ be a $\mathscr{C}$-module, and $v : \mathscr{H} \to g_*(\mathscr{G})$ be a g-morphism; then

$$w : \mathscr{H} \xrightarrow{v} g_*(\mathscr{G}) \xrightarrow{g_*(u)} g_*(f_*(\mathscr{F}))$$

is an h-morphism which is called the **composition** of u and v.

We will now see that there is a canonical isomorphism of bifunctors on $\mathscr{F}$ and $\mathscr{G}$

$$\mathrm{Hom}_{\mathscr{A}}(f^*(\mathscr{G}), \mathscr{F}) \xrightarrow{\sim} \mathrm{Hom}_{\mathscr{B}}(\mathscr{G}, f_*(\mathscr{F})) \tag{3.4.1}$$

which we denote by $v \mapsto v^\flat$, and the inverse of this isomorphism is denoted by $u \mapsto u^\sharp$. The definition is the folowing: for an $\mathscr{A}$-homomorphism $v : f^*(\mathscr{G}) \to \mathscr{F}$, by composing with the canonical homomorphism $f^{-1}(\mathscr{G}) \to f^*(\mathscr{G})$, we obtain a hommorphism $\tilde{v} : f^{-1}(\mathscr{G}) \to \mathscr{F}$ of sheaves of abelian groups, which is also a homomorphism of $f^{-1}(\mathscr{B})$-modules. We then deduce a homomorphism $\tilde{v}^\flat : \mathscr{G} \to f_*(\mathscr{F})$ by the adjointness of f_* and f^{-1}, which is a homomorphism of $\mathscr{B}$-modules, and we denote by $v^\flat$. Similarly, for a $\mathscr{B}$-homomorphism $u : \mathscr{G} \to f_*(\mathscr{F})$, we deduce a homomorphism $u^\sharp : f^{-1}(\mathscr{G}) \to \mathscr{F}$ of $f^{-1}(\mathscr{B})$-modules, whence by tensoring with $\mathscr{A}$ a homomorphism of $\mathscr{A}$-modules $f^*(\mathscr{G}) \to \mathscr{F}$, still denoted by $u^\sharp$. It is immediate that $(u^\sharp)^\flat = u$ and $(v^\flat)^\sharp = v$, as well as the functoriality in $\mathscr{F}$ of the isomorphism $v \mapsto v^\flat$. The functoriality in $\mathscr{G}$ of $u \mapsto u^\sharp$ can be then deduced formally and we then see that f^* is left adjoint to f_*.

If we choose v to be the identify homomorphism of $f^*(\mathscr{G})$, then $v^\flat$ is a homomorphism

$$\rho_{\mathscr{G}} : \mathscr{G} \to f_*(f^*(\mathscr{G}));$$

if we choose u to be the identify homomorphism on $f_*(\mathscr{F})$, then $u^\sharp$ is a homomorphism

$$\sigma_{\mathscr{F}} : f^*(f_*(\mathscr{F})) \to \mathscr{F};$$

these homomorphism are called canonical, and are in general neither injective nor surjective. As always, for a homomorphism $v : \mathscr{G} \to f_*(\mathscr{F})$, we have a canonical factorization

$$v^\flat : \mathscr{G} \xrightarrow{\rho_{\mathscr{G}}} f_*(f^*(\mathscr{G})) \xrightarrow{f_*(v)} f_*(\mathscr{F}) \tag{3.4.2}$$

and for a homomorphism $u : \mathscr{G} \to f_*(\mathscr{F})$, we have a canonical factorization

$$u^\sharp : f^*(\mathscr{G}) \xrightarrow{f^*(u)} f^*(f_*(\mathscr{F})) \xrightarrow{\sigma_{\mathscr{F}}} \mathscr{F} \tag{3.4.3}$$

Now let $g : (Y, \mathscr{B}) \to (Z, \mathscr{C})$ be another morphism and $h = g \circ f$ be the composition. Let $\mathscr{H}$ be a $\mathscr{C}$-module, $u : \mathscr{G} \to \mathscr{F}$ and $v : \mathscr{H} \to \mathscr{G}$ be homomorphisms, and $w = g_*(u) \circ v$ be the composition of u and v. Then $w^\sharp$ is the composition homomorphism

$$w^\sharp : f^*(g^*(\mathscr{H})) \xrightarrow{f^*(v^\sharp)} f^*(\mathscr{G}) \xrightarrow{u^\sharp} \mathscr{F}. \tag{3.4.4}$$

To verify this, we use the description of $w^\sharp$ in (3.4.3) to obtain that $w^\sharp$ is given by the following

diagram

$$\begin{tikzcd}
f^*(g^*(\mathscr{H})) \arrow[r, "f^*(g^*(v))"] \arrow[rr, bend left, "f^*(g^*(w))"] \arrow[dr, "f^*(v^\sharp)"'] & f^*(g^*(g_*(\mathscr{G}))) \arrow[r, "f^*(g^*(g_*(u)))"] \arrow[d, "f^*(\sigma_{\mathscr{G}})"'] & f^*(g^*(g_*(f_*(\mathscr{F})))) \arrow[d, "f^*(\sigma_{f_*(\mathscr{F})})"] \arrow[dr, "\sigma_{\mathscr{F}}"] & \\
& f^*(\mathscr{G}) \arrow[r, "f^*(u)"] \arrow[rr, bend right, "u^\sharp"'] & f^*(f_*(\mathscr{F})) \arrow[r, "\sigma_{\mathscr{F}}"] & \mathscr{F}
\end{tikzcd}$$

The central square is immediately verified to be commutative by the naturality of σ, whence the assertion.

We note that if s is a section of $\mathscr{G}$ over an open subset V of Y, $\rho_{\mathscr{G}}(s)$ is the section $s' \otimes 1$ of $f^*(\mathscr{G})$ over $f^{-1}(V)$, where s' is the section such that $s'_x = s_{f(x)}$ for any $x \in f^{-1}(V)$. We say that $\rho_{\mathscr{G}}(s)$ is the **inverse image** of s under f. Note also that if $u : \mathscr{G} \to f_*(\mathscr{F})$ is a homomorphism, it defines for each $x \in X$ a homomorphism $u_x : \mathscr{G}_{f(x)} \to \mathscr{F}_x$ over stalks, obtained by composing $(u^\sharp)_x : (f^*(\mathscr{G}))_x \to \mathscr{F}_x$ and the canonical homomorphism $s_x \mapsto s_x \otimes 1$ from $\mathscr{G}_{f(x)}$ to $(f^*(\mathscr{G}))_x = \mathscr{G}_{f(x)} \otimes_{\mathscr{B}_{f(x)}} \mathscr{A}_x$. The homomorphism u_x is also obtained by taking inductive limit of the homomorphisms $\Gamma(V, \mathscr{G}) \xrightarrow{u} \Gamma(f^{-1}(V), \mathscr{F}) \to \mathscr{F}_x$, where V runs through neighborhood of $f(x)$.

Let $\mathscr{F}_1, \mathscr{F}_2$ be $\mathscr{A}$-modules, $\mathscr{G}_1, \mathscr{G}_2$ be $\mathscr{B}$-modules, u_i $(i = 1, 2)$ be a homomorphism from $\mathscr{G}_i$ to $\mathscr{F}_i$. We denote by $u_1 \otimes u_2$ the homomorphism $u : \mathscr{G}_1 \otimes_{\mathscr{B}} \mathscr{G}_2 \to \mathscr{F}_1 \otimes_{\mathscr{A}} \mathscr{F}_2$ such that $u^\sharp = (u_1)^\sharp \otimes (u_2)^\sharp$; we verify that u is also the composition

$$\mathscr{G}_1 \otimes_{\mathscr{B}} \mathscr{G}_2 \to f_*(\mathscr{F}_1) \otimes_{\mathscr{B}} f_*(\mathscr{F}_2) \to f_*(\mathscr{F}_1 \otimes_{\mathscr{A}} \mathscr{F}_2),$$

where the first morphism is the ordinary tensor product $u_1 \otimes_{\mathscr{B}} u_2$ and the second homomorphism is the canonical homomorphism (3.2.1).

Let $(\mathscr{G}_\lambda)_{\lambda \in L}$ be an inductive system of $\mathscr{B}$-modules, and, for $\lambda \in L$, let u_λ be a homomorphism $\mathscr{G}_\lambda \to f_*(\mathscr{F})$, which form an inductive system; put $\mathscr{G} = \varinjlim \mathscr{G}_\lambda$ and $u = \varinjlim u_\lambda$. Then $(u^\lambda)^\sharp$ form an inductive system of homomorphisms $f^*(\mathscr{G}_\lambda) \to \mathscr{F}$, and the inductive limit of this system is just $u^\sharp$, since taking tensor products commutes with inductive limits.

Let $\mathscr{M}, \mathscr{N}$ be two $\mathscr{B}$-modules, V be an open subset of Y, and $U = f^{-1}(V)$. The map $v \mapsto f^*(v)$ is a homomorphism

$$\mathrm{Hom}_{\mathscr{B}|_V}(\mathscr{M}|_V, \mathscr{N}|_V) \to \mathrm{Hom}_{\mathscr{A}|_U}(f^*(\mathscr{M})|_U, f^*(\mathscr{N})|_U)$$

for the structure of $\Gamma(V, \mathscr{B})$-modules: note that $\mathrm{Hom}_{\mathscr{A}|_U}(f^*(\mathscr{M})|_U, f^*(\mathscr{N})|_U)$ is endowed with a $\Gamma(U, f^{-1}(\mathscr{B}))$-module structure, and thanks to the canonical homomorphism $\Gamma(V, \mathscr{B}) \to \Gamma(U, f^{-1}(\mathscr{B}))$ obtained from the definition of f^{-1}, this is then a $\Gamma(V, \mathscr{B})$-module. We also verify that these homomorphisms are compatible with restrictions, and therefore define a canonical homomorphism

$$\gamma : \mathscr{H}om_{\mathscr{B}}(\mathscr{M}, \mathscr{N}) \to f_*\big(\mathscr{H}om_{\mathscr{A}}(f^*(\mathscr{M}), f^*(\mathscr{N}))\big)$$

which corresponds to a homomorphism

$$\gamma^\sharp : f^*(\mathscr{H}om_{\mathscr{B}}(\mathscr{M}, \mathscr{N})) \to \mathscr{H}om_{\mathscr{A}}(f^*(\mathscr{M}), f^*(\mathscr{N})) \tag{3.4.5}$$

and this canonical homomorphisms are functorial on $\mathscr{M}$ and $\mathscr{N}$.

Suppose that $\mathscr{F}$ (resp. $\mathscr{G}$) is an $\mathscr{A}$-algebra (resp. a $\mathscr{B}$-algebra). If $u : \mathscr{G} \to f_*(\mathscr{F})$ is a homomorphisms of $\mathscr{B}$-algebras, $u^\sharp$ is a homomorphism $f^*(\mathscr{G}) \to \mathscr{F}$ of $\mathscr{A}$-algebras; this follows from the diagram

$$\begin{tikzcd} \mathscr{G} \otimes_{\mathscr{B}} \mathscr{G} \arrow[r] \arrow[d] & \mathscr{G} \arrow[d, "u"] \\ f_*(\mathscr{F} \otimes_{\mathscr{A}} \mathscr{F}) \arrow[r] & f_*(\mathscr{F}) \end{tikzcd}$$

Similarly, if $v : f^*(\mathscr{G}) \to \mathscr{F}$ is a homormorphism of $\mathscr{A}$-algebras, then $v^\flat : \mathscr{G} \to f_*(\mathscr{F})$ is a homomorphisms of $\mathscr{B}$-algebras. We then get an isomorphism of bifunctors

$$\mathrm{Hom}_{\mathscr{A}-\mathbf{alg}}(f^*(\mathscr{G}), \mathscr{F}) \xrightarrow{\sim} \mathrm{Hom}_{\mathscr{B}-\mathbf{alg}}(\mathscr{G}, f_*(\mathscr{F})).$$

We can then say that f^* is the left adjoint of the functor f^* from the category of $\mathscr{A}$-algebras to that of $\mathscr{B}$-algebras.

19.3.5 Open immersions and representable natrual transformations

The set of open immersions in the category **Rsp** is closed under composition and fiber product, so we can speak of natrual transformations $F \to G$ (where F and G are contravariant functors from **Rsp** to **Set**) which are **representable by open immersions**. The same is true when if we consider the category $\mathbf{Rsp}_{/S}$, where S is a base ringed space.

Proposition 19.3.5. *Let S be a ringed space, $F : (\mathbf{Rsp}_{/S})^\circ \to \mathbf{Set}$ a contravariant functor, and $(F_i)_{i\in I}$ be a family of subfunctors of F. Suppose that the following conditions are satisfied:*

(i) For each i, the canonical natrual transformation $u_i : F_i \to F$ are representable by an open immersion.

(ii) For any S-ringed space X, the map $U \mapsto F(U)$, where U is an open subset of X, is a sheaf of sets over X (i.e., F is a sheaf over $\mathbf{Rsp}_{/S}$).

(iii) For any S-ringed space Z and any natrual transformation $h_Z \to F$, if Z_i is the S-ringed space representating the functor $F_i \times_F h_Z$ and U_i is the image of morphism $Z_i \to Z$, then (U_i) form an open covering of Z.

(iv) For each i, the functor F_i is representable by an S-ringed space X_i.

Then the functor F is representable by an S-ringed space X, and the images of X_i under the morphism $X_i \to X$ (which is open by condition (i)) form an open covering of X.

19.4 Quasi-coherent sheaves and coherent sheaves

19.4.1 Quasi-coherent sheaves

In this subsection we introduce an abstract notion of quasi-coherent $\mathscr{O}_X$-module. This notion is very useful in algebraic geometry, since quasi-coherent modules on a scheme have a good description on any affine open. However, in the general setting of locally ringed spaces this notion is not well behaved at all. The category of quasi-coherent sheaves is not abelian in general, infinite direct sums of quasi-coherent sheaves aren't quasi-coherent, etc, etc.

Let $(X, \mathscr{O}_X)$ be a ringed space. Let $\mathscr{F}$ be a sheaf of $\mathscr{O}_X$-modules. We say that $\mathscr{F}$ is a **quasi-coherent sheaf** of $\mathscr{O}_X$-modules if for each $x \in X$, there exists an open neighbourhood U of x such that $\mathscr{F}|_U$ is isomorphic to the cokernel of a homomorphism of the form $\mathscr{O}_X^{\oplus J}|_U \to \mathscr{O}_X^{\oplus I}|_U$, where I and J are arbitrary index sets. It is clear that $\mathscr{O}_X$ itself is a quasi-coherent $\mathscr{O}_X$-module, and a finite direct sum of quasi-coherent modules is quasi-coherent. The category of quasi-coherent $\mathscr{O}_X$-modules is denoted $\mathbf{QCoh}(\mathscr{O}_X)$. We say an $\mathscr{O}_X$-lagebra $\mathscr{A}$ is quasi-coherent if it is a quasi-coherent $\mathscr{O}_X$-module.

The definition of quasi-coherence amounts to saying that locally the sheaf $\mathscr{F}$ admits a *presentation* by the structural sheaf $\mathscr{O}_X$. This definition is inspired by following ideal: for any module M over a ring A, M admits a presentation of the form

$$A^{\oplus J} \longrightarrow A^{\oplus I} \longrightarrow M \longrightarrow 0$$

where I and J are arbitrary index sets (and in particular may not be finite). Therefore, quasi-coherent sheaves can be seen as a "real module" over the ringed space $(X, \mathscr{O}_X)$, and this idea really makes sense in the realm of algebraic geometry.

Proposition 19.4.1. *Let $(f, f^\#) : (X, \mathscr{O}_X) \to (Y, \mathscr{O}_Y)$ be a morphism of ringed spaces. Then the pullback $f^*(\mathscr{G})$ of a quasi-coherent $\mathscr{O}_Y$-module $\mathscr{G}$ is quasi-coherent.*

Proof. Since the question is local, we may assume that $\mathscr{G}$ has a global presentation by $\mathscr{O}_Y$. We have seen that f^* commutes with all colimits, and is right exact, so if we have an exact sequence

$$\mathscr{O}_Y^{\oplus J} \longrightarrow \mathscr{O}_Y^{\oplus I} \longrightarrow \mathscr{G} \longrightarrow 0$$

then upon applying f^* we obtain the exact sequence

$$\mathscr{O}_X^{\oplus J} \longrightarrow \mathscr{O}_X^{\oplus I} \longrightarrow f^*(\mathscr{G}) \longrightarrow 0$$

This implies the assertion. □

Proposition 19.4.2. *Let $(X, \mathscr{O}_X)$ be ringed space. Let $\rho : A \to \Gamma(X, \mathscr{O}_X)$ be a ring homomorphism from a ring A into the ring of global sections on X and M be an A-module. Then the following three constructions give canonically isomorphic $\mathscr{O}_X$-modules:*

(i) Let $(\pi, \pi^\#) : (X, \mathscr{O}_X) \to (\{*\}, A)$ be the morphism of ringed spaces where $\pi : X \to \{*\}$ is the unique map and $\pi^\#$ is the given homomorphism $\rho : A \to \Gamma(X, \mathscr{O}_X)$. Set $\mathscr{F}_1 = \pi^*(M)$.

(ii) Choose a presentation $A^{\oplus J} \to A^{\oplus I} \to M \to 0$ and set

$$\mathscr{F}_2 = \operatorname{coker}(\mathscr{O}_X^{\oplus J} \to \mathscr{O}_X^{\oplus I})$$

where the homomorphism is induced by ρ and the matrix coefficients of the homomorphism in the presentation of M.

(iii) Let $\mathscr{F}_3$ be the sheaf associated to the presheaf $U \mapsto \Gamma(U, \mathscr{O}_X) \otimes_A M$, where the homomorphism $A \to \Gamma(X, \mathscr{O}_X)$ is the composition of ρ with the restriction map $\Gamma(X, \mathscr{O}_X) \to \Gamma(U, \mathscr{O}_X)$.

This construction has the following properties:

(a) The resulting $\mathscr{O}_X$-modules $\mathscr{F}_M = \mathscr{F}_1 = \mathscr{F}_2 = \mathscr{F}_3$ is quasi-coherent.

(b) The construction gives a functor from the category of A-modules to the category of quasi-coherent sheaves on X which commutes with arbitrary colimits.

(c) For any point $x \in X$ we have $\mathscr{F}_{M,x} = \mathscr{O}_{X,x} \otimes_A M$ which is functorial in M.

(d) For any $\mathscr{O}_X$-module $\mathscr{G}$ we have

$$\operatorname{Hom}_{\mathscr{O}_X}(\mathscr{F}_M, \mathscr{G}) = \operatorname{Hom}_A(M, \Gamma(X, \mathscr{G}))$$

where the A-module structure on $\Gamma(X, \mathscr{G})$ is induced from the $\Gamma(X, \mathscr{O}_X)$-module structure via α.

Proof. The isomorphism between $\mathscr{F}_1$ and $\mathscr{F}_3$ comes from the fact that π^* is defined as the sheafification of the presheaf in (iii). The isomorphism between the constructions in (ii) and (i) comes from the fact that the functor π^* is right exact, so the sequence

$$\pi^*(A^{\oplus I}) \longrightarrow \pi^*(A^{\oplus J}) \longrightarrow \pi^*(M) \to 0$$

is exact, that π^* commutes with arbitrary direct sums, and the fact that $\pi^*(A) = \mathscr{O}_X$.

Now assertion (a) is clear from construction (ii), so is (b) since π^* has these properties. Assertion (c) follows from the description of stalks of pullback sheaves, and (d) follows from adjointness of π^* and π_*. □

In the situation of Proposition 19.4.2 we say $\mathscr{F}_M$ is the **sheaf associated to the module M and the ring map ρ**. If $A = \Gamma(X, \mathscr{O}_X)$ and $\rho = 1_A$, we simply say that $\mathscr{F}_M$ is the sheaf associated to the A-module M.

Proposition 19.4.3. *Let $(X, \mathscr{O}_X)$ be a ringed space and $A = \Gamma(X, \mathscr{O}_X)$. Let M be an A-module and $\mathscr{F}_M$ be the quasi-coherent sheaf of $\mathscr{O}_X$-modules associated to M. If $(f, f^\#) : (Y, \mathscr{O}_Y) \to (X, \mathscr{O}_X)$ is a morphism of ringed spaces, then $f^*(\mathscr{F}_M)$ is the sheaf associated to the $\Gamma(Y, \mathscr{O}_Y)$-module $\Gamma(Y, \mathscr{O}_Y) \otimes_A M$.*

Proof. In view of the following diagram of ringed spaces

$$\begin{tikzcd}
(Y, \mathscr{O}_Y) \arrow[r, "\pi"] \arrow[d, "f"'] & (\{*\}, \Gamma(Y, \mathscr{O}_Y)) \arrow[d, "\text{induced by } f^\#"] \\
(X, \mathscr{O}_X) \arrow[r, "\pi"] & (\{*\}, \Gamma(X, \mathscr{O}_X))
\end{tikzcd}$$

the assertion follows from the first description of $\mathscr{F}_M$ in Proposition 19.4.2 as $\pi^*(M)$. □

To conclude this part, we prove an important result which will be used when we consider quasi-coherent sheaf on affine schemes. We state it in a general manner.

Proposition 19.4.4. *Let $(X, \mathcal{O}_X)$ be a ringed space and x be a point of X. suppose that x has a fundamental system of quasi-compact neighbourhoods, then for any quasi-coherent $\mathcal{O}_X$-module $\mathcal{F}$, there exists an open neighbourhood U of x such that $\mathcal{F}|_U$ is isomorphic to the sheaf of modules $\mathcal{F}_M$ on $(U, \mathcal{O}_U)$ associated to a $\Gamma(U, \mathcal{O}_U)$-module M.*

Proof. Since $\mathcal{F}$ is quasi-coherent, we may replace X by an open neighbourhood of x and assume that $\mathcal{F}$ is isomorphic to the cokernel of a map $\mathcal{O}_X^{\oplus J} \to \mathcal{O}_X^{\oplus I}$. The problem is that this map may not be given by a matrix, because the global sections of a direct sum is in general different from the direct sum of the global sections.

Let U be a quasi-compact neighbourhood of x. We proceed as in the proof of Proposition 19.2.45. For each $j \in J$ denote $s_j \in \Gamma(X, \bigoplus_{i\in I} \mathcal{O}_X)$ the image of the section 1 in the summand $\mathcal{O}_X$ corresponding to j. There exists a finite collection of opens $U_{jk}, k \in K_j$ such that $U = \bigcup_{k\in K_j} U_{jk}$ and such that each restriction $s_j|_{U_{jk}}$ is a finite sum $\sum_{i\in I_{jk}} f_{jki}$ with $I_{jk} \subseteq I$. Let $I_j = \bigcup_{k\in K_j} I_{jk}$. This is a finite set since there are finitely many U_{jk} and each I_{jk} is finite. Since $U = \bigcup_{k\in K_j} U_{jk}$ the section $s_j|_U$ is a section of the finite direct sum $\bigoplus_{i\in I_j} \mathcal{O}_X$. Then by Proposition 19.2.42 we see that actually $s_j|_U$ is a sum $\sum_{i\in I_j} f_{ij}$ with $f_{ij} \in \mathcal{O}_X(U) = \Gamma(U, \mathcal{O}_U)$. At this point we can define a module M as the cokernel of the map

$$\bigoplus_{j\in J} \Gamma(U, \mathcal{O}_U) \to \bigoplus_{i\in I} \Gamma(U, \mathcal{O}_U).$$

with matrix given by the (f_{ij}). By construction (ii) of Proposition 19.4.2 we see that $\mathcal{F}_M$ has the same presentation as $\mathcal{F}|_U$ and therefore $\mathcal{F}_M \cong \mathcal{F}|_U$. □

19.4.2 Sheaves of finite type

Let $(X, \mathcal{O}_X)$ be a ringed space and $\mathcal{F}$ be an $\mathcal{O}_X$-modules. We say that $\mathcal{F}$ is **of finite type** if for every point $x \in X$ there exists an open neighbourhood U of x such that $\mathcal{F}|_U$ is generated by a finite family of sections over U, whence isomorphic to a quotient sheaf of a sheaf of the form $\mathcal{O}_X^n|_U$. It is clear that any quotient of a sheaf of finite type is of finite type, and a finite direct sum of sheaves of finite type is of finite type.

Proposition 19.4.5. *Let $(f, f^\#) : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ be a morphism of ringed spaces. The pullback $f^*\mathcal{G}$ of a finite type $\mathcal{O}_Y$-module is a finite type $\mathcal{O}_X$-module.*

Proof. Since the question is local, we may assume $\mathcal{G}$ is globally generated by finitely many sections. We have seen that f^* commutes with all colimits, and is right exact, so if we have a surjection $\bigoplus_{i=1}^n \mathcal{O}_Y \to \mathcal{G} \to 0$, then by applying f^* we obtain the surjection $\bigoplus_{i=1}^n \mathcal{O}_X \to f^*\mathcal{G} \to 0$. □

Proposition 19.4.6. *Let $\mathcal{F}$ be an $\mathcal{O}_X$-module of finite type.*

(i) If $(s_i)_{1\le i\le n}$ are sections of $\mathcal{F}$ over an open neighborhood U of a point x and if the $s_{i,x}$ generate $\mathcal{F}$, then there exists an open neighborhood $V \subseteq U$ of x such that the $s_{i,y}$ generate $\mathcal{F}_y$ for any $y \in V$.

(ii) If $\varphi : \mathcal{F} \to \mathcal{G}$ is a homomorphism such that $\varphi_x = 0$, there exists an open neighborhood U of x such that $\varphi|_U = 0$.

(iii) If $\psi : \mathscr{G} \to \mathscr{F}$ is a homomorphism such that ψ_x is surjective, then there exists an open neighborhood V of x such that $\psi|_V$ is surjective.

(iv) The support of $\mathscr{F}$ is closed.

Proof. We first prove (i), so let $(t_j)_{1\le j\le m}$ be a family of sections of $\mathscr{F}$ over an open neighborhood $U' \subseteq U$ of x generating $\mathscr{F}|_{U'}$. Since $(s_{i,x})$ generates $\mathscr{F}_x$, there exists sections a_{ij} of $\mathscr{O}_X$ over an open neighborhood $U'' \subseteq U$ of x such that $t_{j,x} = \sum_{i=1}^n a_{ij,x}s_{i,x}$ for each j. We then conclude that there is an open neighborhood $V \subseteq U''$ of x such that for each $y \in V$, we have $t_{j,y} = \sum_{i=1}^n a_{ij,y}s_{i,y}$, so $(s_{i,y})$ generates $\mathscr{F}_y$ for $y \in V$.

Assertion (iv) follows from (i) by taking $n = 1$ and $s_1 = 0$; also, (iii) follows from (iv) by considering $\operatorname{coker}\psi$, which is of finite type. Finally, (ii) follows from (iv) by considering $\operatorname{im}\varphi$, which is also of finite type. □

Corollary 19.4.7. *Let $(X, \mathscr{O}_X)$ be a locally ringed space and $\mathscr{F}$ be an $\mathscr{O}_X$-module of finite type. Then $\operatorname{supp}(\mathscr{F})$ is the set of $x \in X$ such that $\mathscr{F}_x/\mathfrak{m}_x\mathscr{F}_x \neq 0$.*

Proof. In fact, $\mathscr{F}_x$ is a finitely generated $\mathscr{O}_{X,x}$, so $\mathscr{F}_x = 0$ if and only if $\mathfrak{m}_x\mathscr{F}_x = \mathscr{F}_x$ by Nakayama's lemma. □

Corollary 19.4.8. *Let $(X, \mathscr{O}_X)$ be a locally ringed space and $\mathscr{F}, \mathscr{G}$ be $\mathscr{O}_X$-modules of finite type. Then*

$$\operatorname{supp}(\mathscr{F} \otimes_{\mathscr{O}_X} \mathscr{G}) = \operatorname{supp}(\mathscr{F}) \cap \operatorname{supp}(\mathscr{G}).$$

Proof. As the tensor product of two $\kappa(x)$-vector spaces is nonzero if both of them are nonzero, this follows from Corollary 19.4.7. □

Corollary 19.4.9. *Let $f : X \to Y$ be a morphism of locally ringed spaces. For any $\mathscr{O}_Y$-module $\mathscr{G}$ of finite type, we have*

$$\operatorname{supp}(f^*(\mathscr{G})) = f^{-1}(\operatorname{supp}(\mathscr{G})).$$

Proof. This follows from Corollary 19.4.7 and **??**. □

Proposition 19.4.10. *Suppose that X is quasi-compact and let $\mathscr{F}, \mathscr{G}$ be two $\mathscr{O}_X$-modules such that $\mathscr{G}$ is of finite type and $\mathscr{F}$ is the filtered limit $(\mathscr{F}_\lambda)$ of $\mathscr{O}_X$-modules. Let $\varphi : \mathscr{F} \to \mathscr{G}$ be a surjective homomorphism, then there exists an index λ such that the homomorphism $\mathscr{F}_\lambda \to \mathscr{G}$ is surjective.*

Proof. For any $x \in X$, there exists a finite system of sections s_i of $\mathscr{G}$ over an open neighborhood $U(x)$ of x such that $s_{i,y}$ generates $\mathscr{G}_y$ for any $y \in U(x)$. Then there is an open neighborhood $V(x) \subseteq U(x)$ of x and sections t_i of $\mathscr{F}$ over $V(x)$ such that $s_i|_{V(x)} = \varphi(t_i)$ for each i. We can then suppose that the t_i are the images of sections of a single sheaf $\mathscr{F}_{\lambda(x)}$ over $V(x)$. Since X is quasi-compact, it can be covered by finitely many $V(x_k)$, and let λ be the supremum of the $\lambda(x_k)$ the assertion then follows. □

Corollary 19.4.11. *Suppose that X is quasi-compact and let $\mathscr{F}$ be an $\mathscr{O}_X$-module of finite type that is generated by global sections. Then $\mathscr{F}$ is generated by finitely many global sections.*

Proof. It suffices to cover X be finitely many open neighborhoods U_k such that for each k, there exists finitely many sections s_{ik} of $\mathscr{F}$ over X whose restrictions to U_k generate $\mathscr{F}|_{U_k}$. It is clear that the s_{ik} then generate $\mathscr{F}$. □

Proposition 19.4.12. *Let X be a ringed space. Let*

$$0 \longrightarrow \mathscr{F} \xrightarrow{\varphi} \mathscr{G} \xrightarrow{\psi} \mathscr{H} \longrightarrow 0$$

be a short exact sequence of $\mathscr{O}_X$-modules. If $\mathscr{F}$ and $\mathscr{H}$ are of finite type, so is $\mathscr{G}$.

Proof. Since the question is local, we may assume that $\mathscr{F}$ (resp. $\mathscr{H}$) is generated by finitely many global sections $(s_i)_{1\le i\le n}$ (resp. $(t_j)_{1\le j\le m}$), and there are sections $(t'_j)_{1\le j\le m}$ of $\mathscr{G}$ over X such that $t_j = \psi(t'_j)$ for each j. It is then clear that $\mathscr{G}$ is generated by the sections $\varphi(s_i)$ and t'_j. □

Let $(X, \mathscr{O}_X)$ be a ringed space. Let $\mathscr{F}$ be a sheaf of $\mathscr{O}_X$-modules. We say that $\mathscr{F}$ is **of finite presentation** if for every point $x \in X$ there exists an open neighbourhood $x \in U \subseteq X$, and $n, m \in \mathbb{N}$ such that $\mathscr{F}|_U$ is isomorphic to the cokernel of a homomorphism $\bigoplus_{j=1}^m \mathscr{O}_U \to \bigoplus_{j=1}^n \mathscr{O}_U$. This means that X is covered by open sets U such that $\mathscr{F}|_U$ has a presentation of the form

$$\bigoplus_{j=1}^m \mathscr{O}_U \longrightarrow \bigoplus_{j=1}^n \mathscr{O}_U \longrightarrow \mathscr{F}|_U \longrightarrow 0$$

As in the case of $\mathscr{O}_X$-modules, the pullback of a $\mathscr{O}_X$-module of finite presentation is of finite presentation. We also note that any $\mathscr{O}_X$-module of finite presentation is in particular quasi-coherent.

Proposition 19.4.13. *Let $(X, \mathscr{O}_X)$ be a ringed space. Let $\mathscr{F}$ be a $\mathscr{O}_X$-module of finite presentation.*

(a) If $\psi : \mathscr{O}_X^{\oplus r} \to \mathscr{F}$ is a surjective homomorphism, then $\ker \psi$ *is of finite type.*

(b) If $\varphi : \mathscr{G} \to \mathscr{F}$ is a surjective homomorphism with $\mathscr{G}$ of finite type, then $\ker \theta$ *is of finite type.*

Proof. □

Proposition 19.4.14. *Let $(X, \mathscr{O}_X)$ be a ringed space and $\mathscr{F}$ be an $\mathscr{O}_X$-module of finite presentation. Then for any $\mathscr{O}_X$-module $\mathscr{H}$, the canonical homomorphism*

$$(\mathscr{H}om_{\mathscr{O}_X}(\mathscr{F}, \mathscr{H}))_x \to \mathrm{Hom}_{\mathscr{O}_{X,x}}(\mathscr{F}_x, \mathscr{G}_x)$$

is bijective.

Proof. □

Proposition 19.4.15. *Let $(X, \mathscr{O}_X)$ be a ringed space and $\mathscr{F}, \mathscr{G}$ be finitely presented $\mathscr{O}_X$-module. If for a point $x \in X$, $\mathscr{F}_x$ and $\mathscr{G}_x$ are isomorphic $\mathscr{O}_{X,x}$-modules, then there exists an open neighbourhood U of x such that $\mathscr{F}|_U \cong \mathscr{G}|_U$.*

Proof. If $\varphi : \mathscr{F}_x \to \mathscr{G}_x$ and $\psi : \mathscr{G}_x \to \mathscr{F}_x$ are the isomorphisms, there exists, by Proposition 19.4.14, an open neighborhood V of x and a section u (resp. v) of $\mathscr{H}om_{\mathscr{O}_X}(\mathscr{F}, \mathscr{G})$ (resp. $\mathscr{H}om_{\mathscr{O}_X}(\mathscr{G} \circ \mathscr{F})$) over V such that $u_x = \varphi$ (resp. $v_x = \psi$). As $(u \circ v)_x$ and $(v \circ u)_x$ are the identities, by Proposition 19.4.14 again there exists an open neighborhood $U \subseteq V$ of x such that $(u \circ v)|_U$ and $(v \circ u)|_U$ are idnetities, whence the proposition. □

19.4.3 Coherent sheaves

Let $(X, \mathcal{O}_X)$ be a ringed space. Let $\mathcal{F}$ be a sheaf of $\mathcal{O}_X$-modules. We say that $\mathcal{F}$ is a **coherent** $\mathcal{O}_X$-module if $\mathcal{F}$ is of finite type and for every open $U \subseteq X$ and every finite collection $s_1, \dots, s_n$ of sections of $\mathcal{F}$ over U, the kernel of the associated map $\bigoplus_{i=1}^n \mathcal{O}_U \to \mathcal{F}|_U$ is of finite type. The category of coherent $\mathcal{O}_X$-modules is denoted $\mathbf{Coh}(\mathcal{O}_X)$. This is a more reasonable object than the category of quasi-coherent sheaves, in the sense that it is at least an abelian subcategory of $\mathbf{Mod}(\mathcal{O}_X)$ no matter what X is. However, the pullback of a coherent module is almost never coherent in the general setting of ringed spaces.

Proposition 19.4.16. *Let $(X, \mathcal{O}_X)$ be a ringed space. Any coherent $\mathcal{O}_X$-module is of finite presentation and hence quasi-coherent.*

Proof. Let $\mathcal{F}$ be a coherent sheaf on X and let x be a point of X. We may find an open neighbourhood U and sections $(s_i)_{1 \le i \le n}$ of $\mathcal{F}$ over U such that the associated homomorphism $\varphi : \bigoplus_{i=1}^n \mathcal{O}_U \to \mathcal{F}|_U$ is surjective. Since $\ker \varphi$ is also of finite type, we may find an open neighbourhood $x \in V \subseteq U$ and sections $(t_j)_{1 \le j \le m}$ of $\bigoplus_{i=1}^m \mathcal{O}_V$ which generate the kernel of $\varphi|_V$. Then over V we get the presentation

$$\bigoplus_{j=1}^m \mathcal{O}_V \longrightarrow \bigoplus_{i=1}^n \mathcal{O}_V \longrightarrow \mathcal{F}|_V \longrightarrow 0$$

which shows that $\mathcal{F}$ is of finite presentation. □

Example 19.4.17. Suppose that X is a point. In this case the definition above gives a notion for modules over rings. What does the definition of coherent mean? It is closely related to the notion of Noetherian, but it is not the same: namely, the ring $A = \mathbb{C}[x_1, x_2, x_3, \dots]$ is coherent as a module over itself but not Noetherian as a module over itself.

Proposition 19.4.18. *Let $(X, \mathcal{O}_X)$ be a ringed space.*

(a) Let $\varphi : \mathcal{F} \to \mathcal{G}$ be a homomorphism from an $\mathcal{O}_X$-module $\mathcal{F}$ of finite type to a coherent $\mathcal{O}_X$-module $\mathcal{G}$. Then $\ker \varphi$ is of finite type.

(b) Let $\varphi : \mathcal{F} \to \mathcal{G}$ be a homomorphism of coherent $\mathcal{O}_X$-modules. Then $\ker \varphi$ and $\operatorname{coker} \varphi$ are coherent.

(c) Given a short exact sequence of $\mathcal{O}_X$-modules $0 \to \mathcal{F}_1 \to \mathcal{F}_2 \to \mathcal{F}_3 \to 0$ if two out of three are coherent so is the third.

(d) The category of coherent $\mathcal{O}_X$-modules is abelian and the inclusion functor $\mathbf{Coh}(\mathcal{O}_X) \to \mathbf{Mod}(\mathcal{O}_X)$ is exact.

Proof. Let $\varphi : \mathcal{F} \to \mathcal{G}$ be a homomorphism where $\mathcal{F}$ is of finite type and $\mathcal{G}$ is coherent. Let us show that $\ker \varphi$ is of finite type. Pick $x \in X$ and choose an open neighbourhood U of x in X such that $\mathcal{F}|_U$ is generated by $s_1, \dots, s_n$. By definition the kernel $\mathcal{K}$ of the induced map $\bigoplus_{i=1}^n \mathcal{O}_U \to \mathcal{G}, e_i \mapsto \varphi(s_i)$ is of finite type. Hence $\ker \varphi$ which is the image of the composition $\mathcal{K} \to \bigoplus_{i=1}^n \mathcal{O}_U \to \mathcal{F}$ is of finite type.

Now consider the case of assertion (b). By assertion (a) the kernel of φ is of finite type and hence is coherent as a subsheaf of $\mathcal{F}$. With the same hypotheses let us show that $\operatorname{coker} \varphi$ is coherent. Since $\mathcal{G}$ is of finite type so is $\operatorname{coker} \varphi$. Let $U \subseteq X$ be open and let $\bar{s}_i \in \operatorname{coker} \varphi(U), 1 \le$

$i \leq n$ be sections. We have to show that the kernel of the associated morphism $\overline{\psi} : \bigoplus_{i=1}^n \mathcal{O}_U \to \operatorname{coker} \varphi$ has finite type. There exists an open covering of U such that on each open all the sections $\overline{s}_i$ lift to sections s_i of $\mathcal{G}$. Hence we may assume this is the case over U. Thus $\overline{\psi}$ lifts to $\psi : \bigoplus_{i=1}^n \mathcal{O}_U \to \mathcal{G}$. Consider the following diagram

$$\begin{tikzcd}
0 \arrow[r] & \ker \psi \arrow[r] \arrow[d] & \bigoplus_{i=1}^n \mathcal{O}_U \arrow[r] \arrow[d, equal] & \mathcal{G} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \ker \overline{\psi} \arrow[r] & \bigoplus_{i=1}^n \mathcal{O}_U \arrow[r] & \operatorname{coker} \psi \arrow[r] & 0
\end{tikzcd}$$

By the snake lemma we have $\operatorname{im} \varphi \cong \operatorname{coker}(\ker \psi \to \ker \overline{\psi})$, thus there is a short exact sequence $0 \to \ker \psi \to \ker \overline{\psi} \to \operatorname{im} \varphi \to 0$. Hence by Proposition 19.4.12 we see that $\ker \overline{\psi}$ is of finite type.

Let $0 \to \mathcal{F}_1 \to \mathcal{F}_2 \to \mathcal{F}_3 \to 0$ be a short exact sequence of $\mathcal{O}_X$-modules. By part (b) it suffices to prove that if $\mathcal{F}_1$ and $\mathcal{F}_3$ are coherent so is $\mathcal{F}_2$. By Proposition 19.4.12 we see that $\mathcal{F}_2$ has finite type. Let $s_1, \ldots, s_n$ be finitely many local sections of $\mathcal{F}_2$ defined over a common open U of X. We have to show that the module of relations $\mathcal{K}$ between them is of finite type. Consider the following commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & 0 \arrow[r] \arrow[d] & \bigoplus_{i=1}^n \mathcal{O}_U \arrow[r] \arrow[d] & \bigoplus_{i=1}^n \mathcal{O}_U \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathcal{F}_1 \arrow[r] & \mathcal{F}_2 \arrow[r] & \mathcal{F}_3 \arrow[r] & 0
\end{tikzcd}$$

with obvious notation. By the snake lemma we get a short exact sequence $0 \to \mathcal{K} \to \mathcal{K}_3 \to \mathcal{F}_1$ where $\mathcal{K}_3$ is the module of relations among the images of the sections s_i in $\mathcal{F}_3$. Since $\mathcal{F}_3$ is coherent we see that $\mathcal{K}_3$ is finite type. Since $\mathcal{F}_1$ is coherent we see that the image $\mathcal{I}$ of $\mathcal{K}_3 \to \mathcal{F}_1$ is coherent. Hence $\mathcal{K}$ is the kernel of the map $\mathcal{K} \to \mathcal{I}$ between a finite type sheaf and a coherent sheaves and hence finite type by (b). □

Corollary 19.4.19. *Let* $\mathcal{F}_1 \xrightarrow{u} \mathcal{F}_2 \xrightarrow{v} \mathcal{F}_3 \xrightarrow{w} \mathcal{F}_4 \xrightarrow{t} \mathcal{F}_5$ *be an exact sequence of* $\mathcal{O}_X$*-modules. If* $\mathcal{F}_1, \mathcal{F}_2, \mathcal{F}_4$ *and* $\mathcal{F}_5$ *are coherent, then* $\mathcal{F}_3$ *is coherent.*

Proof. In fact, $\operatorname{coker} u = \mathcal{F}_2/\ker v$ and $\operatorname{im} w = \ker t$ are coherent, and it suffices to consider the exact sequence

$$0 \longrightarrow \operatorname{coker} u \longrightarrow \mathcal{F}_3 \longrightarrow \operatorname{im} w \longrightarrow 0$$

and apply Proposition 19.4.18. □

Corollary 19.4.20. *Let* $\mathcal{F}$ *and* $\mathcal{G}$ *be two coherent subsheaves of a coherent sheaf* $\mathcal{K}$*. The sheaves* $\mathcal{F} + \mathcal{G}$ *and* $\mathcal{F}/\mathcal{G}$ *are coherent.*

Proof. The sheaf $\mathcal{F} + \mathcal{G}$ is a subsheaf of $\mathcal{K}$ of fintie type, so it is coherent by definition. As for $\mathcal{F} \cap \mathcal{G}$, it is the kernel of $\mathcal{F} \to \mathcal{K}/\mathcal{G}$, so is coherent. □

Corollary 19.4.21. *If* $\mathcal{F}$ *and* $\mathcal{G}$ *are coherent* $\mathcal{O}_X$*-modules, so are* $\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G}$ *and* $\mathcal{H}om_{\mathcal{O}_X}(\mathcal{F}, \mathcal{G})$.

Proof. Since the question is local, we can assume that $\mathcal{F}$ is the cokernel of a homomorphism $\mathcal{O}_X^n \to \mathcal{O}_X^m$. Then $\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G}$ is isomorphic to the cokernel of the homomorphism $\mathcal{O}_X^n \otimes_{\mathcal{O}_X} \mathcal{G} \to$

$\mathcal{O}_X^m \otimes_{\mathcal{O}_X} \mathcal{G}$, which is identified with the cokernel of $\mathcal{G}^n \to \mathcal{G}^m$. Since $\mathcal{G}$ is coherent, we then see $\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G}$ is also coherent.

Similarly, in view of Proposition 19.4.14, we have an exact sequence □

Corollary 19.4.22. *Let $\mathcal{F}$ be a coherent $\mathcal{O}_X$-module and $\mathcal{I}$ be an coherent ideal of $\mathcal{O}_X$. Then the $\mathcal{O}_X$-module $\mathcal{I}\mathcal{F}$ is coherent.*

Proof. The image of the canonical homomorphism $\mathcal{I} \otimes_{\mathcal{O}_X} \mathcal{F} \to \mathcal{F}$ is $\mathcal{I}\mathcal{F}$, so this follows from Corollary 19.4.21. □

Corollary 19.4.23. *Let X be a ringed space and $\varphi : \mathcal{F} \to \mathcal{G}$ be a homomorphism of $\mathcal{O}_X$-modules. Assume $\mathcal{F}$ of finite type, $\mathcal{G}$ is coherent and the homomorphism $\varphi : \mathcal{F}_x \to \mathcal{G}_x$ is injective for a point $x \in X$. Then there exists an open neighbourhood $x \in U \subseteq X$ such that $\varphi|_U$ is injective.*

Proof. Denote by $\mathcal{K} \subseteq \mathcal{F}$ the kernel of φ. By Proposition 19.4.18 we see that $\mathcal{K}$ is a finite type $\mathcal{O}_X$-module. Our assumption is that $\mathcal{K}_x = 0$, so by Proposition 19.4.6(iv) there exists an open neighbourhood U of x such that $\mathcal{K}|_U = 0$. □

We say an $\mathcal{O}_X$-algebra $\mathcal{A}$ is **coherent** if $\mathcal{A}$ is a coherent $\mathcal{O}_X$-module. In particular, $\mathcal{O}_X$ is a coherent $\mathcal{O}_X$-algebra if, for any open subset $U \subseteq X$ and any homomorphism $\mathcal{O}_X^n|_U \to \mathcal{O}_X|U$ of $\mathcal{O}_U$-modules, the kernel of this homomorphism is of finite type. We then say that $\mathcal{O}_X$ is a coherent sheaf of rings. If $\mathcal{O}_X$ is a coherent sheaf of rings, any $\mathcal{O}_X$-module of finite presentation is coherent in view of Proposition 19.4.18.

Example 19.4.24. The annihilator of a $\mathcal{O}_X$-module $\mathcal{F}$ is the kernel $\mathcal{I}$ of the homomorphism $\mathcal{O}_X \to \mathcal{H}om_{\mathcal{O}_X}(\mathcal{F}, \mathcal{F})$ which sends a section $s \in \Gamma(U, \mathcal{O}_X)$ to the multiplication by s in $\mathrm{Hom}(\mathcal{F}|_U, \mathcal{F}|_U)$. If $\mathcal{O}_X$ is a coherent sheaf of rings and if $\mathcal{F}$ is a coherent $\mathcal{O}_X$-module, $\mathcal{I}$ is coherent by Proposition 19.4.18, and it follows from Proposition 19.4.14 that for each $x \in X$, $\mathcal{I}_x$ is the annihilator of the $\mathcal{O}_{X,x}$-module $\mathcal{F}_x$.

Proposition 19.4.25. *Suppose that $\mathcal{O}_X$ is a coherent sheaf of rings and let $\mathcal{I}$ be a coherent ideal of $\mathcal{I}$. For an $(\mathcal{O}_X/\mathcal{I})$-module $\mathcal{F}$ to be coherent, it is necessary and sufficient that as an $\mathcal{O}_X$-module, $\mathcal{F}$ is coherent. In particular, $\mathcal{O}_X/\mathcal{I}$ is a coherent sheaf of rings.*

Proof. We note that $\mathcal{O}_X/\mathcal{I}$ is a coherent $\mathcal{O}_X$-module. If $\mathcal{F}$ is a coherent $(\mathcal{O}_X/\mathcal{I})$, any point of X admits an open neighborhood U such that $\mathcal{F}|_U$ is the cokernel of a homomorphism $(\mathcal{O}_X/\mathcal{I})^m|_U \to (\mathcal{O}_X/\mathcal{I})^n|_U$, so $\mathcal{F}$ is a coherent $\mathcal{O}_X$-module.

Conversely, suppose that $\mathcal{F}$, as an $\mathcal{O}_X$-module, is coherent. First, since $\mathcal{F}$ is an $\mathcal{O}_X$-module of finite type, it is an $(\mathcal{O}_X/\mathcal{I})$-module of finite type. On ther other hand, let U be an open subset of X and $u : (\mathcal{O}_X/\mathcal{I})^n|_U \to \mathcal{F}|_U$ is an $(\mathcal{O}_X/\mathcal{I})$-homomorphism; by composing with the canonical homomorphism $v : \mathcal{O}_X^n|_U \to (\mathcal{O}_X/\mathcal{I})^n|_U$, we obtain a homomorphism $u \circ v : \mathcal{O}_X^n|_U \to \mathcal{F}|_U$, and $\ker(u \circ v)$ is by hypothesis of finite type. But since v is surjective, $\ker u$ is the image of $\ker(u \circ v)$ by v, so is of finite type. □

Proposition 19.4.26. *Let $f : X \to Y$ be a morphism of ringed spaces and suppose that $\mathcal{O}_X$ is a coherent rings. Then for any coherent $\mathcal{O}_Y$-module $\mathcal{G}$, $f^*(\mathcal{G})$ is a coherent $\mathcal{O}_X$-module.*

Proof. Let V be an open subset of Y such that $\mathcal{G}|_V$ is the cokernel of a homomorphism $v : \mathcal{O}_Y^n|_V \to \mathcal{O}_Y^n|_V$. As f_U^* is right exact, we have $f^*(\mathcal{G})|_U = f_U^*(\mathcal{G}|_V)$ (where $U = f^{-1}(V)$) and the cokernel of the homomorphism $f_U^*(v) : \mathcal{O}_X^m|_U \to \mathcal{O}_X^n|_U$ is coherent by Proposition 19.4.18. □

19.4.4 Locally free sheaves

Let $(X, \mathcal{O}_X)$ be a ringed space. We say an $\mathcal{O}_X$-module $\mathcal{F}$ is **locally free** if, for any $x \in X$, there exists an open neighborhood U of x such that $\mathcal{F}|_U$ is isomorphic to an $(\mathcal{O}_X|_U)$-module of the form $\mathcal{O}_X^{\oplus I}|_U$. If for any open subset U the set I is finite, we say that $\mathcal{F}$ is **of finite rank**. If for any open subset U, the set I has n elements, we say that $\mathcal{F}$ is **of rank n**. If $\mathcal{F}$ is a locally free $\mathcal{O}_X$-module of finite rank, for any point $x \in X$, $\mathcal{F}_x$ is a free $\mathcal{O}_X$-module of finite rank $n(x)$, and there exists an open neighborhood U of x such that $\mathcal{F}|_U$ is of rank $n(x)$. If X is connected, we then see $n(x)$ is constant.

It is clear that any locally finite sheaf is quasi-coherent, and if $\mathcal{O}_X$ is a coherent sheaf of rings, any locally free $\mathcal{O}_X$-module of finite rank is coherent. If $\mathcal{E}$ is locally free, $\mathcal{E} \otimes_{\mathcal{O}_X} \mathcal{F}$ is an exact functor on the category of $\mathcal{O}_X$-modules.

We will mostly consider locally free $\mathcal{O}_X$-modules of finite rank, so when we mention the notation of a locally free $\mathcal{O}_X$-modules, it should be understood that we mean locally free $\mathcal{O}_X$-modules of finite rank.

Example 19.4.27. Let $\mathcal{F}$ be an $\mathcal{O}_X$-module of finite presentation. Then if for a point $x \in X$, $\mathcal{F}_x$ is a free module of rank n, there exists an open neighborhood U of x such that $\mathcal{F}|_U$ is locally free of rank n (Proposition 19.4.15).

Proposition 19.4.28. *Let $\mathcal{E}, \mathcal{F}$ be $\mathcal{O}_X$-modules and consider the canonical functorial homomorphism*

$$\mathcal{E}^* \otimes_{\mathcal{O}_X} \mathcal{F} = \mathcal{H}om_{\mathcal{O}_X}(\mathcal{E}, \mathcal{O}_X) \otimes_{\mathcal{O}_X} \mathcal{F} \to \mathcal{H}om_{\mathcal{O}_X}(\mathcal{E}, \mathcal{F})$$

If $\mathcal{F}$ or $\mathcal{E}$ is locally free of finite rank, then this homomorphism is bijective.

Proof. The homomorphism is defined by the following: for any open subset U and a couple (u, t), where $u \in \Gamma(U, \mathcal{E}) = \mathrm{Hom}(\mathcal{E}|_U, \mathcal{O}_X|_U)$ and $t \in \Gamma(U, \mathcal{F})$, we associate the element of $\mathrm{Hom}(\mathcal{E}|_U, \mathcal{F}|_U)$ whose stalk at each point $x \in U$ send $s_x \in \mathcal{E}_x$ to the element $u_x(s_x)t_s \in \mathcal{F}_x$. Since the question is local, we may assume that $\mathcal{E} = \mathcal{O}_X^n$ or $\mathcal{F} = \mathcal{O}_X^n$. As for any $\mathcal{O}_X$-module $\mathcal{G}$, $\mathcal{H}om_{\mathcal{O}_X}(\mathcal{O}_X^n, \mathcal{G})$ is canonically isomorphic to $\mathcal{G}^n$ and $\mathcal{H}om_{\mathcal{O}_X}(\mathcal{G}, \mathcal{O}_X^n)$ is isomorphic to $(\mathcal{G}^n)^*$, we are reduced to the case $\mathcal{E} = \mathcal{F} = \mathcal{O}_X$, and the claim is then immediate. □

If $\mathcal{L}$ is locally free of rank 1, so is its dual $\mathcal{L}^* = \mathcal{H}om_{\mathcal{O}_X}(\mathcal{L}, \mathcal{O}_X)$, because this is ture for $\mathcal{L} = \mathcal{O}_X$ and the question is local. Moreover, we have a canonical isomorphism

$$\mathcal{H}om_{\mathcal{O}_X}(\mathcal{L}, \mathcal{O}_X) \otimes_{\mathcal{O}_X} \mathcal{L} \cong \mathcal{O}_X.$$

In fact, it suffices to prove that the canonical homomorphism $\mathcal{O}_X \to \mathcal{H}om_{\mathcal{O}_X}(\mathcal{L}, \mathcal{L})$ is bijective, and for this we may assume that $\mathcal{L} = \mathcal{O}_X$, and then the claim is immediate. Due to this, we put $\mathcal{L}^{-1} = \mathcal{H}om_{\mathcal{O}_X}(\mathcal{L}, \mathcal{O}_X)$, and $\mathcal{L}^{-1}$ is called the inverse of $\mathcal{L}$.

If $\mathcal{L}$ and $\mathcal{L}'$ are two $\mathcal{O}_X$-modules locally free of rank 1, so is their tensor product $\mathcal{L} \otimes_{\mathcal{O}_X} \mathcal{L}'$, since locally we have $\mathcal{O}_X \otimes_{\mathcal{O}_X} \mathcal{O}_X \cong \mathcal{O}_X$. For any integer $n \geq 1$, we denote by $\mathcal{L}^{\otimes n}$ the n-fold tensor product $\mathcal{L}$, which is also a locally free $\mathcal{O}_X$-module of rank 1; by convention, we set $\mathcal{L}^{\otimes 0} = \mathcal{O}_X$ and $\mathcal{L}^{\otimes(-n)} = (\mathcal{L}^{-1})^{\otimes n}$. Then there exists a canonical isomorphism

$$\mathcal{L}^{\otimes m} \otimes_{\mathcal{O}_X} \mathcal{L}^{\otimes n} \cong \mathcal{L}^{\otimes(n+m)}$$

Proposition 19.4.29. *Let $f : Y \to X$ be a morphism of ringed spaces. If $\mathscr{E}$ is a locally free $\mathscr{O}_X$-module (resp. locally free $\mathscr{O}_X$-module of rank n), then $f^*(\mathscr{E})$ is a locally free $\mathscr{O}_Y$-module (resp. locally free $\mathscr{O}_Y$-module of rank n). Moreover, we have a canonical isomorphism $f^*(\mathscr{E}^*) = (f^*(\mathscr{E}))^*$.*

Proof. The first assertion from the fact that f^* commutes with direct sums and $f^*(\mathscr{O}_X) = \mathscr{O}_Y$, the second assertin can be checked for the case $\mathscr{E} = \mathscr{O}_X$, since the question is local. □

Let $\mathscr{L}$ be a locally free $\mathscr{O}_X$-module of rank 1. We denote by $\Gamma_*(X, \mathscr{L})$ or simple $\Gamma_*(\mathscr{L})$ the abelian group of the direct sum $\bigoplus_{n\in\mathbb{Z}} \Gamma(X, \mathscr{L}^{\otimes n})$. We endow it a graded ring structure by defining the product of a couple (s_n, s_m), where $s_n \in \Gamma(X, \mathscr{L}^{\otimes n})$ and $s_m \in \Gamma(X, \mathscr{L}^{\otimes m})$, the section of $\mathscr{L}^{\otimes(n+m)}$ over X corresponding to the section $s_n \otimes s_m$ of $\mathscr{L}^{\otimes n} \otimes_{\mathscr{O}_X} \mathscr{L}^{\otimes m}$. The associative of this multiplication is immediately verified, and it is clear that $\Gamma_*(X, \mathscr{L})$ is a covariant functor on $\mathscr{L}$ with values in the category of graded rings of type $\mathbb{Z}$.

If now $\mathscr{F}$ is an $\mathscr{O}_X$-module, we set

$$\Gamma_*(\mathscr{L}, \mathscr{F}) = \bigoplus_{n\in\mathbb{Z}} \Gamma(X, \mathscr{F} \otimes_{\mathscr{O}_X} \mathscr{L}^{\otimes n}).$$

We endow this abelian group a graded $\Gamma_*(\mathscr{L})$-module structure by the following: for any couple (s_n, u_m), where $s_n \in \Gamma(X, \mathscr{L}^{\otimes n})$ and $u_m \in \Gamma(X, \mathscr{F} \otimes \mathscr{L}^{\otimes n})$, we associate the section of $\mathscr{F} \otimes \mathscr{L}^{\otimes(n+m)}$ that corresponds to $s_n \otimes u_m$; the verification that this defines a module structure is immediate. For fixed X and $\mathscr{L}$, we see $\Gamma_*(\mathscr{L}, \mathscr{F})$ is a covariant functor on $\mathscr{F}$ with values in the category of graded $\Gamma_*(\mathscr{L})$-modules. For X and $\mathscr{F}$ fixed, this is a covariant functor on $\mathscr{L}$ iwth values in the category of abelian groups.

Let $f : Y \to X$ be a morphism of ringed spaces. The canonical homomorphism $\rho : \mathscr{L}^{\otimes n} \to f_*(f^*(\mathscr{L}^{\otimes n}))$ defines a homomorphism $\Gamma(X, \mathscr{L}^{\otimes n}) \to \Gamma(Y, f^*(\mathscr{L}^{\otimes n}))$ of abelian groups, and as $f^*(\mathscr{L}^{\otimes n}) = (f^*(\mathscr{L}))^{\otimes n}$, it gives a homomorphism $\Gamma_*(\mathscr{L}) \to \Gamma_*(f^*(\mathscr{L}))$ of graded rings. Similarly, the canonical homomorphism $\mathscr{F} \otimes \mathscr{L}^{\otimes n} \to f_*(f^*(\mathscr{F} \otimes \mathscr{L}^{\otimes n}))$ defines a homomorphism $\Gamma(X, \mathscr{F} \otimes \mathscr{L}^{\otimes n}) \to \Gamma(Y, f^*(\mathscr{F} \otimes \mathscr{L}^{\otimes n}))$ and as

$$f^*(\mathscr{F} \times \mathscr{L}^{\otimes n}) = f^*(\mathscr{F}) \otimes (f^*(\mathscr{L}))^{\otimes n}$$

these homomorphisms give rise to a bi-homomorphism $\Gamma_*(\mathscr{L}, \mathscr{F}) \to \Gamma_*(f^*(\mathscr{L}), f^*(\mathscr{F}))$ of graded modules.

Proposition 19.4.30. *Let $f : X \to Y$ be a morphism of ringed spaces, $\mathscr{F}$ be an $\mathscr{O}_X$-module, and $\mathscr{E}$ be a locally free $\mathscr{O}_Y$-module of finite rank. Then there exists a canonical isomorphism*

$$f_*(\mathscr{F}) \otimes_{\mathscr{O}_Y} \mathscr{E} \cong f_*(\mathscr{F} \otimes_{\mathscr{O}_X} f^*(\mathscr{E})).$$

Proof. For any $\mathscr{O}_Y$-module $\mathscr{E}$, we have canonical homomorphisms

$$f_*(\mathscr{F}) \otimes_{\mathscr{O}_Y} \mathscr{E} \xrightarrow{1\otimes\rho_{\mathscr{E}}} f_*(\mathscr{E}) \otimes_{\mathscr{O}_Y} f_*(f^*(\mathscr{E})) \xrightarrow{\alpha} f_*(\mathscr{F} \otimes_{\mathscr{O}_X} f^*(\mathscr{E}))$$

Since $\mathscr{E}$ is locally free and the question is local on Y, we may assume that $\mathscr{E} = \mathscr{O}_Y^n$; as f_* and f^* commutes with finite direct sums, we can also suppose that $n = 1$, and in this case, the proposition follows directly from the definition and the relation $f^*(\mathscr{O}_Y) = \mathscr{O}_X$. □

Proposition 19.4.31. *Let $f : X \to Y$ be a morphism of ringed spaces, $\mathscr{F}, \mathscr{G}$ be two $\mathscr{O}_Y$-modules, and suppose that $\mathscr{F}$ is locally free of finite rank. Then the canonical homomorphism*

$$f^*(\mathscr{H}om_{\mathscr{O}_Y}(\mathscr{F}, \mathscr{G})) \to \mathscr{H}om_{\mathscr{O}_X}(f^*(\mathscr{F}), f^*(\mathscr{G}))$$

is an isomorphism.

Proof. Since the question is local on Y, we can assume that $\mathscr{F} = \mathscr{O}_Y^n$; then $\mathscr{H}om_{\mathscr{O}_Y}(\mathscr{O}_Y, \mathscr{G})$ is identified with $\mathscr{G}^n$, $f^*(\mathscr{F})$ is identified with $\mathscr{O}_X^n$, and $\mathscr{H}om_{\mathscr{O}_X}(f^*(\mathscr{F}), f^*(\mathscr{G}))$ is identified with $(f^*(\mathscr{G}))^n$, whence the assertion. □

Remark 19.4.1. Let X be a ringed space. For any integer $n > 0$, we prove that there is a *set* $\mathfrak{M}_n$ (denoted also by $\mathfrak{M}_n(X)$) of locally free $\mathscr{O}_X$-module of rank n such that any locally free $\mathscr{O}_X$-module of rank n is isomorphic to an element of $\mathfrak{M}_n$. For this, we consider the set $\mathfrak{R}_n$ of couples $(\mathfrak{U}, \Theta)$, where $\mathfrak{U}$ is an open covering of X and Θ is a family $(\theta_{UV})_{(U,V)\in\mathfrak{U}\times\mathfrak{U}}$, where θ_{UV} is an automorphism of $\mathscr{O}_X^n|_{(U\cap V)}$, θ_{UU} is the identity automorphism of $\mathscr{O}_U^n$, and the family (θ_{UV}) satisfies the cocycle conditions. Then any element $(\mathfrak{U}, \Theta)$ of $\mathfrak{R}_n$ corresponds to a well-defined locally free $\mathscr{O}_X$-module of rank n. If we denote by $\mathfrak{L}_n$ the set of these $\mathscr{O}_X$-modules, then any locally free $\mathscr{O}_X$-module of rank n is isomorphic to one of the elements in $\mathfrak{L}_n$; it then suffices to choose for $\mathfrak{M}_n$ a system of representatives of $\mathfrak{L}_n$ for the equivalence condition: $\mathscr{E}$ and $\mathscr{E}'$ are equivalent if they are isomorphic. For any locally free $\mathscr{O}_X$-module $\mathscr{E}$ of rank n, we denote by $\mathrm{cl}(\mathscr{E})$ the uique element of $\mathfrak{M}_n$ which is isomorphic to $\mathscr{E}$.

We can define a composition law on the set $\mathfrak{M}_1$ by associating two elements $\mathscr{L}, \mathscr{L}'$ of $\mathfrak{M}_1(X)$ the element $\mathrm{cl}(\mathscr{L}\otimes\mathscr{L}')$. It is clear that this law is associative and commutative and with identity element $\mathrm{cl}(\mathscr{O}_X)$. Moreover for any $\mathscr{L} \in \mathfrak{M}_1(X)$, $\mathrm{cl}(\mathscr{L}^{-1})$ is the inverse of $\mathscr{L}$ for this composition law. We then define a commutative group structure on $\mathfrak{M}_1(X)$, and this group is called the **Picard group** of the ringed space X and denoted by $\mathrm{Pic}(X)$. We also note that there exists a canonical isomorphism

$$\varphi_X : H^1(X, \mathscr{O}_X^\times) \xrightarrow{\sim} \mathrm{Pic}(X).$$

For this, we note that for any open subset U of X the multiplicative group $\Gamma(U, \mathscr{O}_X^\times)$ is canonically identified with the grop of automorphisms of $\mathscr{O}_U$-module $\mathscr{O}_U$, which send each section ε of $\mathscr{O}_X^\times$ over U to the automorphism $u : \mathscr{O}_U \to \mathscr{O}_U$ such that $u_x(s_x) = \varepsilon_x s_x$ for any $x \in U$ and any $s_x \in \mathscr{O}_{X,x}$. Let $\mathfrak{U} = (U_\lambda)$ be an open covering of X; the datum that, given any couple (λ, μ) of indices, an automorphism θ_λ of $\mathscr{O}_X|_{U_\lambda\cap U_\mu}$ which satisfy the cocycle conditions, is then equivalent to giving a 1-cochain of the covering $\mathfrak{U}$, with values in $\mathscr{O}_X^\times$. Similarly, the datum that, given an index λ, an automorphism ω_λ of $\mathscr{O}_{U_\lambda}$, is equivalent to giving a 0-cochain of $\mathfrak{U}$ with values in $\mathscr{O}_X^\times$, and the coboundary of this cochain corresponds to the automorphisms $(\omega_\lambda|_{U_\lambda\cap U_\mu}) \circ (\omega_\mu|_{U_\lambda\cap U_\mu})^{-1}$. We then corresponds any 1-cocycle $(\theta_{\lambda\mu})$ of $\mathfrak{U}$ with values in $\mathscr{O}_X^\times$, the element $\mathrm{cl}(X)$ of $\mathrm{Pic}(X)$, where $\mathscr{L}$ is the locally free $\mathscr{O}_X$-module of rank 1 defined by the family $\theta = (\theta_{\lambda\mu})$; two cohomologous cocycles then correspond to the same element of $\mathrm{Pic}(X)$, so we obtain a map $\varphi_{\mathfrak{U}} : H^1(\mathfrak{U}, \mathscr{O}_X^\times) \to \mathrm{Pic}(X)$. Moreover, if $\mathfrak{V}$ is a second open covering of X, which

is a refinement of $\mathfrak{U}$, the diagram

$$\begin{tikzcd} H^1(\mathfrak{U}, \mathscr{O}_X^\times) \arrow[dr, "\varphi_{\mathfrak{U}}"] \arrow[dd] & \\ & \mathrm{Pic}(X) \\ H^1(\mathfrak{V}, \mathscr{O}_X^\times) \arrow[ur, "\varphi_{\mathfrak{V}}"] & \end{tikzcd}$$

where the vertical arrow is the canonical homomorphism, is commutative. By passing to limit, we then obtain a map $\varphi_X : H^1(X, \mathscr{O}_X^\times) \to \mathrm{Pic}(X)$, where the Čech cohomology group $\check{H}^1(X, \mathscr{O}_X^\times)$ is canonically identified with $H^1(X, \mathscr{O}_X^\times)$. The map φ_X is clearly surjective, since any locally free sheaf of rank 1 is defined by a 1-cocycle. It is injective, because it suffices to show that the maps $\varphi_{\mathfrak{U}}$ are injective, and this follows from the definition of $H^1(\mathfrak{U}, \mathscr{O}_X^\times)$. It remains to prove that $\varphi_{\mathfrak{U}}$ is a homomorphism of groups. Let $\mathscr{L}, \mathscr{L}'$ be two locally free $\mathscr{O}_X$-modules of rank 1 such that, for any λ, $\mathscr{L}|_{U_\lambda}$ and $\mathscr{L}'|_{U_\lambda}$ are isomorphic to $\mathscr{O}_{U_\lambda}$. There then exists for each λ an element a_λ (resp. a'_λ) of $\Gamma(U_\lambda, \mathscr{L})$ (resp. $\Gamma(U_\lambda, \mathscr{L}')$) such that the elements of $\Gamma(U_\lambda, \mathscr{L})$ (resp. $\Gamma(U_\lambda, \mathscr{L}')$) are of the form $s_\lambda \cdot a_\lambda$ (resp. $s_\lambda \cdot a'_\lambda$) where s_λ runs through $\Gamma(U_\lambda, \mathscr{O}_X)$. The corresponding cocycles $(\varepsilon_{\lambda\mu})$, $(\varepsilon'_{\lambda\mu})$ are such that the relation $s_\lambda \cdot a_\lambda = s_\mu \cdot a_\mu$ (resp. $s_\lambda \cdot a'_\lambda = s_\mu \cdot a'_\mu$) over $U_\lambda \cap U_\mu$ is equivalent to $s_\lambda = \varepsilon_{\lambda\mu} s_\mu$ (resp. $s_\lambda = \varepsilon'_{\lambda\mu} s_\mu$) over $U_\lambda \cap U_\mu$. As the sections of $\mathscr{L} \otimes \mathscr{L}'$ over U_λ are the finite sums of $s_\lambda s'_\lambda \cdot (a_\lambda \otimes a'_\lambda)$ where s_λ, s'_λ runs through $\Gamma(U_\lambda, \mathscr{O}_X)$, it is clear that the cocycle $(\varepsilon_{\lambda\mu}\varepsilon'_{\lambda\mu})$ corresponds to $\mathscr{L} \otimes \mathscr{L}'$, which completes the proof.

Let $f : X' \to X$ be a morphism of ringed spaces. If $\mathscr{L}_1$, $\mathscr{L}_2$ are two locally free $\mathscr{O}_X$-modules of rank 1 and are isomorphic, the $\mathscr{O}_{X'}$-modules $f^*(\mathscr{L}_1)$ and $f^*(\mathscr{L}_2)$ are isomorphic. On the other hand, for any $\mathscr{O}_X$-modules $\mathscr{F}, \mathscr{G}$, we have $f^*(\mathscr{F} \otimes \mathscr{G}) = f^*(\mathscr{F}) \otimes f^*(\mathscr{G})$. We then conclude that the morphism f defines a canonical homomorphism of abelian groups

$$\mathrm{Pic}(f) : \mathrm{Pic}(X) \to \mathrm{Pic}(X').$$

On the other hand, we have a canonical homomorphism

$$H^1(f) : H^1(X, \mathscr{O}_X^\times) \to H^1(X', \mathscr{O}_{X'}^\times)$$

corresponds the restriction of the homomorphism $f^\# : \mathscr{O}_X \to f_*(\mathscr{O}_{X'})$ to $\mathscr{O}_X^\times$. We claim that the diagram

$$\begin{tikzcd} H^1(X, \mathscr{O}_X^\times) \arrow[r, "H^1(f)"] \arrow[d, "\varphi_X", "\sim"'] & H^1(X', \mathscr{O}_{X'}^\times) \arrow[d, "\sim"', "\varphi_{X'}"] \\ \mathrm{Pic}(X) \arrow[r, "\mathrm{Pic}(f)"] & \mathrm{Pic}(X') \end{tikzcd}$$

is commutative. In fact, if $\mathscr{L}$ is given by the cocycle $(\varepsilon_{\lambda\mu})$ of an open covering (U_λ) of X, it suffices to prove that $f^*(\mathscr{L})$ is defined by a cocycle whose class is cohomologous to the image of $(\varepsilon_{\lambda\mu})$ under $H^1(f)$. But if $\theta_{\lambda\mu}$ is the automorphism of $\mathscr{O}_X|_{U_\lambda \cap U_\mu}$ corresponding to $\varepsilon_{\lambda\mu}$, it is clear that $f^*(\mathscr{L})$ is obtained by glueing $\mathscr{O}_{X'}|_{\psi^{-1}(U_\lambda)}$ with the automorphisms $g^*(\theta_{\lambda\mu})$, and it sufficies to verify that this corresponds to the cocycle $(f^\#(\varepsilon_{\lambda\mu}))$; this follows also from the definition by identify $\varepsilon_{\lambda\mu}$ with its image under $\rho_{\mathscr{O}_X}$, which is a section of $\psi^{-1}(\mathscr{O}_X)$ over $\psi^{-1}(U_\lambda \cap U_\mu)$.

We now consider locally free sheaves over *locally* ringed spaces. The point of locality is that we can consider sections of a locally free sheaf as functions over X. More precisely, if $s \in \Gamma(U, \mathscr{E})$ for some locally free $\mathscr{O}_X$-module $\mathscr{E}$ of rank r, then for $x \in U$ we can define $s(x)$ to be the image of s_x in $\mathscr{E}_x/\mathfrak{m}_x\mathscr{E}_x$ (this is called the *value* of s at x, written as $s(x)$, do not confuse it with the *stalk* s_x at x). Since $\mathscr{E}_x \cong \mathscr{O}_{X,x}^r$, we can then think s as a function on x with r components. As we shall see, this is the common situation when we talk about schemes.

Proposition 19.4.32. *Let X be a locally ringed space and $\mathscr{E}$ be a locally free $\mathscr{O}_X$-module of finite rank. Then for any section s of $\mathscr{E}$ over X, the set X_s of $x \in X$ such that $s(x) \neq 0$ is open in X and s is invertible over X_s.*

Proof. Since the question is local, we can assume that $\mathscr{E} = \mathscr{O}_X^n$. If $(s_j)_{1\leq j\leq n}$ is the projection of s to the n-th component, we see $s(x) \neq 0$ if and only if $s_j(x) \neq 0$ for some j, so X_s is the union of the X_{s_j}, and we are reduced to the case $n = 1$. But for $s \in \Gamma(X, \mathscr{O}_X)$, to say that $s(x) \neq 0$ amounts to that $s_x \notin \mathfrak{m}_x$, hence s_x is inveritble in $\mathscr{O}_{X,x}$. By then there then existes an open neighborhood U of x in X such that $s|_U$ is invertible in $\Gamma(U, \mathscr{O}_X)$, and therefore $s(y) \neq 0$ for any $y \in U$. □

Corollary 19.4.33. *Let X be a locally ringed space and $\mathscr{E}$ be a locally free $\mathscr{O}_X$-module of finite rank. Let $s_1, \ldots, s_p$ be sections of $\mathscr{E}$ over X. Then the set of $x \in X$ such that $s_1(x), \ldots, s_p(x)$ are lineraly independent over $\mathscr{E}_x/\mathfrak{m}_x\mathscr{E}_x$ is open in X.*

Proof. We know that $\bigwedge^p \mathscr{E}$ is a locally free $\mathscr{O}_X$-module of rank $\binom{n}{p}$. Moreover, for any $x \in X$, the stalk $(\bigwedge^p \mathscr{E})_x/\mathfrak{m}_x(\bigwedge^p \mathscr{E})_x$ is identified with $\bigwedge^p(\mathscr{E}_x/\mathfrak{m}_x\mathscr{E}_x)$. If $s = s_1 \wedge \cdots \wedge s_p$, then $s(x)$ is identified with $s_1(x) \wedge \cdots \wedge s_p(x)$, and $s(x) \neq 0$ if and only if $s_1(x), \ldots, s_p(x)$ are linearly independent, whence the assertion by Proposition 19.4.32. □

Corollary 19.4.34. *Let X be a locally ringed space, $\mathscr{E}$ be a locally free $\mathscr{O}_X$-module of rank n, and $s_1, \ldots, s_n$ be sections of $\mathscr{E}$ over X such that, for any $x \in X$, $s_1(x), \ldots, s_n(x)$ are lineraly independent. Then the homomorphism $u : \mathscr{O}_X^n \to \mathscr{E}$ defined by the sections s_i is bijective.*

Proof. Again we can assume that $\mathscr{E} = \mathscr{O}_X^n$ and canonically identity $\bigwedge^n \mathscr{E}$ with $\mathscr{O}_X$. The section $s = s_1 \wedge \cdots \wedge s_n$ is then a section of $\mathscr{O}_X$ over X such that $s(x) \neq 0$ for all $x \in X$, and thus invertible in $\Gamma(X, \mathscr{O}_X)$. We can then define a homomorphism inverse to u by Cramer's rule. □

Proposition 19.4.35. *Let X be a locally ringed space, $\mathscr{F}$ be an $\mathscr{O}_X$-module of finite type, $\mathscr{E}$ a locally free $\mathscr{O}_X$-module of finite rank, and $u : \mathscr{F} \to \mathscr{E}$ be a homomorphism, and x be a point of X. Then the following conditions are equivalent:*

(i) The homomorphism u_x is left invertible (which means u_x is injective and its image in $\mathscr{E}_x$ is a direct factor).

(ii) The homomorphism $u_x \otimes 1 : \mathscr{F}_x/\mathfrak{m}_x\mathscr{F}_x \to \mathscr{E}_x/\mathfrak{m}_x\mathscr{E}_x$ of vector spaces induced by u_x is injective.

(iii) There exists an open neighborhood U of x such that $u|_U : \mathscr{F}|_U \to \mathscr{E}|_U$ is left invertible, the image $u(\mathscr{F})|_U$ is a locally free $\mathscr{O}_U$-module isomorphic to $\mathscr{F}|_U$, which admits a locally free complement in $\mathscr{E}|_U$.

Moreover, the set of $x \in X$ satisfying these equivalent conditions are open.

Proof. The equivalence of (i) and (ii) is a general result in algebras, and it is clear that (iii) implies (i). We now prove that (i) implies (iii); there exists by hypothesis a homomorphism $w : \mathscr{E}_x \to \mathscr{F}_x$ such that $w \circ u_x$ is the identify automorphism on $\mathscr{F}_x$. As $\mathscr{E}$ is locally free of finite rank, hence of finite presentation, it follows from Proposition 19.4.14 that there exists an open neigbourhood U of x and a homomorphism $v : \mathscr{E}|_U \to \mathscr{F}|_U$ such that $w = v_x$, hence $(v \circ (u|_U))_x = v_x \circ u_x$ is the identity automorphism. We then conclude that, by restricting U, we can suppose that $v \circ (u|_U)$ is the identity on $\mathscr{F}|_U$, which means $u|_U$ is left invertible. We then know that $p = (u|_U) \circ v$ is a projection from $\mathscr{E}|_U$ to $u(\mathscr{F})|_U$, and that $u|_U$ is an isomorphism from $\mathscr{F}|_U$ to $u(\mathscr{F})|_U$. We claim that (aftering shrinking U if necessary), $u(\mathscr{E})_U$ and $\ker p$ are locally free $\mathscr{O}_U$-modules (supplementary in $\mathscr{F}|_U$). In fact, $p_x : \mathscr{F}_x \to (u(\mathscr{F}))_x$ is a projection, hence so is $p_x \otimes 1 : \mathscr{E}_x/\mathfrak{m}_x\mathscr{E}_x \to (u(\mathscr{F}))_x/\mathfrak{m}_x(u(\mathscr{F}))_x$. There exists sections s_j $(1 \leq j \leq n)$ of $\mathscr{F}$ over U such that the first m sections s_j $(1 \leq j \leq m)$ are sections of $u(\mathscr{F})$, and the later $n - m$ are sections of $\ker p$, and that the $s_j(x)$ $(1 \leq j \leq n)$ form a base for $\mathscr{F}_x/\mathfrak{m}_x\mathscr{F}_x$. In view of Corollary 19.4.34, by shrinking U, we can suppose that the $\mathscr{O}_X$-module $\mathscr{M}$ generated by s_j for $1 \leq j \leq n$ and the $\mathscr{O}_X$-module $\mathscr{N}$ generated by the s_j for $m + 1 \leq j \leq n$ are free and supplementary in $\mathscr{E}|_U$. We have evidently $\mathscr{M} \subseteq u(\mathscr{F})|_U$ and $\mathscr{N} \subseteq \ker p$; on the other hand, if $i : \mathscr{M} \to u(\mathscr{F})|_U$ and $j : \mathscr{N} \to \ker p$ are the canonical injections, then the choice of s_j implies that i_x and j_x are bijections. As $u(\mathscr{F})|_U$ and $\ker p$ are $\mathscr{O}_U$-modules of finite type (the second being the image of $\mathscr{E}|_U$ under $1 - p$), we conclude from Proposition 19.4.6 (by shrinking U if necessary) that $\mathscr{M} = u(\mathscr{E})|_U$ and $\mathscr{N} = \ker p$. □

Corollary 19.4.36. *With the hypotheses in Proposition 19.4.35, the following conditions are equivalent:*

(i) For any morphism $g : X' \to X$ of locally ringed spaces, the homomorphism $g^*(u) : g^*(\mathscr{F}) \to g^*(\mathscr{E})$ is injective.

(ii) For any $x \in X$, the homomorphism $u_x \otimes 1 : \mathscr{F}_x/\mathfrak{m}_x\mathscr{F}_x \to \mathscr{E}_x/\mathfrak{m}_x\mathscr{E}_x$ is injective.

(iii) For any $x \in X$, there exists an open neighborhood U of x such that $u|_U : \mathscr{F}|_U \to \mathscr{E}|_U$ is left invertible.

Moreover, if the conditions are satisfied, $\mathscr{F}$ is a locally free $\mathscr{O}_X$-module of finite rank.

Proof. The equivalence of (ii) and (iii) follows from Proposition 19.4.35, so does the last one. The fact that (iii) implies (i) follows from follows from the fact that we can reduce ourselves to the case where $\mathscr{E} = \mathscr{O}_X^n$ and $\mathscr{F} = \mathscr{O}_X^m$ and that g^* is left exact, since the question is local on X. Finally, we show that (ii) is a particular case of (i): it suffices to consider the locally ringed space X' reduced to a point x, with sheaf of rings $\kappa(x)$ (that is, $\mathrm{Spec}(\kappa(x))$). We let $g : X' \to X$ be the canonical morphism which maps x to x and $g^\# : \mathscr{O}_X \to \kappa(x)$ is the cannical homomorphism $\Gamma(U, \mathscr{O}_X) \to \mathscr{O}_{X,x} \to \kappa(x)$ for any open neigbourhood U of x. It is then easily verified that $g^*(u)$ is the homomorphism $u_x \otimes 1$. □

Remark 19.4.2. If u satisfies the conditions of Corollary 19.4.36, then we say that it is **universally injective**.

Corollary 19.4.37. *Let X be a locally ringed space, $\mathscr{F}, \mathscr{E}$ be two locally free $\mathscr{O}_X$-modules of finite rank, $u : \mathscr{F} \to \mathscr{E}$ be a homomorphism, and x be a point of X. The following conditions are equivalent:*

(i) The homomorphism $u_x \otimes 1 : \mathscr{F}_x/\mathfrak{m}_x\mathscr{F}_x \to \mathscr{E}_x/\mathfrak{m}_x\mathscr{E}_x$ is surjective.

(ii) The homomorphism u_x is surjective.

(iii) The homomorphism $\bigwedge^m u_x : \bigwedge^m \mathscr{F}_x \to \bigwedge^m \mathscr{E}_x$ (where m is the rank of $\mathscr{F}_x$) is surjective.

(iv) The homomorphism $u_x^t : \mathscr{E}_x^* \to \mathscr{F}_x^*$ is left invertible.

Moreover, the set S of $x \in X$ satisfying these conditions is open in X, $\ker(u)|_S$ is a locally free $\mathscr{O}_S$-module and any $x \in S$ admits an open neighborhood $U \subseteq S$ such that $\ker(u)|_U$ admits in $\mathscr{F}|_U$ a locally free complement (isomorphic to $\mathscr{E}|_U$).

Proof. The equivalence of (i) and (ii) follows from Nakayama's Lemma. Similarly, (iii) is equivalent to that

$$(\bigwedge^m u_x) \otimes 1 : (\bigwedge^m \mathscr{F}_x)/\mathfrak{m}_x(\bigwedge^m \mathscr{F}_x) \to (\bigwedge^m \mathscr{E}_x)/\mathfrak{m}_x(\bigwedge^m \mathscr{E}_x)$$

is surjective; but $(\bigwedge^m u_x) \otimes 1$ is identified with

$$\bigwedge^m (u_x \otimes 1) : \bigwedge^m (\mathscr{F}_x/\mathfrak{m}_x\mathscr{F}_x) \to \bigwedge^m (\mathscr{E}_x/\mathfrak{m}_x\mathscr{E}_x),$$

and as $\mathscr{E}_x/\mathfrak{m}_x\mathscr{E}_x$ is a vector space of dimension m over $\kappa(x)$, $\bigwedge^m (u_x \otimes 1)$ is surjective if $u_x \otimes 1$ is surjective, and is zero in the contrary case, whence the equivalence of (i) and (iii). On the other hand, as $(\mathscr{F}^*)^* = \mathscr{F}$, $(\mathscr{E}^*)^* = \mathscr{E}$ and $(u^t)^t = u$, it is the same to say that $u_x \otimes 1$ is surjective and that $(u_x \otimes 1)^t = (u_x)^t \otimes 1 : \mathscr{E}_x^*/\mathfrak{m}_x\mathscr{E}_x^* \to \mathscr{F}_x^*/\mathfrak{m}_x\mathscr{F}_x^*$ is injective, whence the equivalence of (i) and (iv) in view of Proposition 19.4.35. The fact that S is open follows from Proposition 19.4.35. We can then reduce to the case where $S = X$, and the other assertions of the statement are deduced by transposing the conclusions of Proposition 19.4.35 applied to u^t. □

Corollary 19.4.38. *With the notations of Corollary 19.4.37, suppose moreover that $\mathscr{F}$ and $\mathscr{E}$ have the same rank at each point. Then, for any $x \in X$, the following conditions are equivalent:*

(i) u_x is left invertible;

(ii) u_x is surjective;

(iii) u_x is bijective.

Moreover, the set of $x \in x$ satisfying these conditions is open in X.

Corollary 19.4.39. *With the notations of Corollary 19.4.37, let $f : X' \to X$ be a morphism of locally ringed spaces and put $\mathscr{F}' = f^*(\mathscr{F})$, $\mathscr{E}' = f^*(\mathscr{E})$, which are locally free $\mathscr{O}_{X'}$-modules of finite rank. Let $u' = f^*(u) : \mathscr{F}' \to \mathscr{E}'$. Then for a point $x' \in X'$, $u'_{x'}$ is surjective (resp. left invertible) if and only if at the point $x = f(x')$, u_x is surjective (resp. left invertible).*

Proof. In fact, we have $\mathscr{F}'_{x'} = \mathscr{F}_x \otimes_{\mathscr{O}_{X,x}} \mathscr{O}_{X',x'}$, $\mathscr{E}'_{x'} = \mathscr{F}_x \otimes_{\mathscr{O}_{X,x}} \mathscr{O}_{X',x'}$, and $u'_{x'}$ is deduced from u_x be base changing $\mathscr{O}_{X,x}$ to $\mathscr{O}_{X',x'}$. If k and k' are the residue fields of x and x', we then have $\mathscr{F}'_{x'} \otimes k' = (\mathscr{F}_x \otimes k) \otimes_k k'$, $\mathscr{F}'_{x'} \otimes k' = (\mathscr{F}_x \otimes k) \otimes_k k'$, and the homomorphism $u'_{x'} \otimes 1 : \mathscr{F}'_{x'} \otimes k' \to \mathscr{E}'_{x'} \otimes k'$ is then deduced from $u_x \otimes 1_k : \mathscr{F}_x \otimes k \to \mathscr{E}_x \otimes k$ by base changing from k to k'. The conclusion then follows from the fact that this base change is faithfully flat, the Nakayama lemma, and Proposition 19.4.35. □

Proposition 19.4.40. *Let X be a locally ringed space, $\mathscr{L}$ be an $\mathscr{O}_X$-module of finite type. For that $\mathscr{L}$ to be locally free of rank 1, it is necessary and sufficient that there exists an $\mathscr{O}_X$-module $\mathscr{F}$ such that $\mathscr{L} \otimes_{\mathscr{O}_X} \mathscr{F}$ is isomorphic to $\mathscr{O}_X$. Moreover, any $\mathscr{O}_X$-module with this property is isomorphic to $\mathscr{L}^{-1}$.*

Proof. We have seen that if $\mathscr{L}$ is locally of rank 1 then $\mathscr{L}^{-1} \otimes_{\mathscr{O}_X} \mathscr{L} \cong \mathscr{O}_X$. Moreover, in this case $\mathscr{L}^{-1}$ is isomorphic to $\mathscr{L}^{-1} \otimes_{\mathscr{O}X} \mathscr{O}_X$, hence to $\mathscr{L}^{-1} \otimes_{\mathscr{O}_X} (\mathscr{L} \otimes_{\mathscr{O}_X} \mathscr{F})$ and therefore to $\mathscr{F}$. It then remains to prove that if $\mathscr{L} \otimes_{\mathscr{O}_X} \mathscr{F}$ is isomorphic to $\mathscr{O}_X$ then $\mathscr{L}$ is locally free of rank 1. Let $x \in X$ and put $A = \mathscr{O}_{X,x}$ (which is a local ring with maximal ideal $\mathfrak{m}$), $M = \mathscr{L}_x$, $N = \mathscr{F}_x$. The hypothesis implies that $M \otimes_A N$ is isomorphic to A, and as $(A/\mathfrak{m}) \otimes_A (M \otimes_A N)$ is identified with $(M/\mathfrak{m}M) \otimes_{A/\mathfrak{m}} (N/\mathfrak{m}N)$, this tensor product is isomorphic to $A/\mathfrak{m}$ over the field $A/\mathfrak{m}$, which shows that $M/\mathfrak{m}M$ and $N/\mathfrak{m}N$ are of dimension 1 over $A/\mathfrak{m}$. For any element $z \in M$ not belonging to $\mathfrak{m}M$, we then have $M = Az + \mathfrak{m}M$, which implies $M = Az$ by Nakayama's Lemma. Also, the annihilator of z also annihilates $M \otimes_A N$, which is isomorphic to A, so this annihilator is zero and M is isomorphic to A. There is then a section s of $\mathscr{L}$ over an open neigbourhood U of x such that $t_x \mapsto t_x s_x$ is an isomorphism from $\mathscr{O}_{X,x}$ to $\mathscr{L}_x$. Since $\mathscr{L}$ is of finite type, we can, by shrinking U, suppose that s generates $\mathscr{L}|_U$ (Proposition 19.4.6), which means we have a surjective homomorphism $u : \mathscr{O}_U \to \mathscr{L}|_U$. Moreover, for any $y \in U$, the homomorphism $\mathscr{O}_{X,y}/\mathfrak{m}_y \to \mathscr{L}_y/\mathfrak{m}_y\mathscr{L}_y$ deduced from u is bijective, hence so is u (Proposition 10.3.19). □

The $\mathscr{O}_X$-modules locally free of rank 1 over a locally ringed space X are then called the **invertible** $\mathscr{O}_X$-modules.

Proposition 19.4.41. *Let X be a locally ringed space, $\mathscr{L}$ be an invertible $\mathscr{O}_X$-module, and f be a section of $\mathscr{L}$ over X. For any $x \in X$, the following conditions are equivalent:*

(i) f_x generates the $\mathscr{O}_{X,x}$-module $\mathscr{L}_x$.

(ii) $f_x \notin \mathfrak{m}_x\mathscr{L}_x$ (that is, $f(x) \neq 0$).

(iii) There exists a section g of $\mathscr{L}^{-1}$ over an open neigbourhood V of x such that the canonical image of $(f|_V) \otimes g$ in $\Gamma(V, \mathscr{O}_X)$ is the unit element.

Moreover, the set X_f of $x \in X$ satisfying these conditions is open in X.

Proof. The question is local on X so we can assume that $\mathscr{L} = \mathscr{O}_X$, and the proposition then follows. □

Chapter 20

Cohomology group of sheaves

In this chapter we consider the cohomology of shaves of modules. First we have a proposition.

Proposition 20.0.1. *A sequence of sheaves of $\mathcal{O}_X$-modules on a space X*

$$0 \longrightarrow \mathcal{F} \longrightarrow \mathcal{G} \longrightarrow \mathcal{H} \longrightarrow 0$$

is exact if and only if for all points $x \in X$ the sequence of stalks is exact. This is equivalent to

(a) For all open sets $U \subseteq X$ the sequence

$$0 \longrightarrow \mathcal{F}(U) \longrightarrow \mathcal{G}(U) \longrightarrow \mathcal{H}(U)$$

is exact.

(b) For any $s \in \mathcal{H}(U)$, we can find a covering $U = \bigcup_i U_i$ by open sets and $s_i \in \mathcal{F}(U_i)$ such that $s|_{U_i} = s_i$.

Applied to $U = X$ this tells us that the functor of global sections $\mathcal{F} \mapsto \mathcal{F}(X)$ is left-exact. It turns out that the category of sheaves of $\mathcal{O}_X$-modules has enough injectives, thus the right derived functors $\mathcal{R}^p\Gamma(X, -)$ exist, and for every sheaf $\mathcal{F}$ on X, the cohomology groups $\mathcal{R}^p\Gamma(X, -)(\mathcal{F})$ are defined. These groups denoted by $H^p(X, \mathcal{F})$ are called the **cohomology groups of the sheaf $\mathcal{F}$** or **the cohomology groups of X with values in $\mathcal{F}$**.

20.1 Definition of sheaf cohomology

We first show that the category $\mathbf{Mod}(\mathcal{O}_X)$ has enough injectives.

Proposition 20.1.1. *Let $(X, \mathcal{O}_X)$ be a ringed space. Then the category $\mathbf{Mod}(\mathcal{O}_X)$ of sheaves of $\mathcal{O}_X$-modules has enough injectives.*

Proof. Let $\mathcal{F}$ be a sheaf of $\mathcal{O}_X$-modules. For each point $x \in X$, the stalk $\mathcal{F}_x$ is an $\mathcal{O}_{X,x}$-module. Therefore there is an injection $\mathcal{F}_x \to I_x$, where $\mathcal{I}_x$ is an injective $\mathcal{O}_{X,x}$-module. For each point x, let i_x denote the inclusion of the one-point space $\{x\}$ into X, and consider the sheaf $\mathcal{I} = \prod_{X \in X} i_{x,*}(I_x)$. Here we consider I_x as a sheaf on the one-point space $\{x\}$.

Now for any sheaf $\mathscr{G}$ of $\mathscr{O}_X$-modules, we have

$$\mathrm{Hom}_{\mathscr{O}_X}(\mathscr{G}, \mathscr{I}) = \prod_{x \in X} \mathrm{Hom}_{\mathscr{O}_X}(\mathscr{G}, i_{x,*}(I_x))$$

by definition of the direct product. On the other hand, for each point $x \in X$, since $i_{x,*}$ is the adjoint of taking stalk, we have

$$\mathrm{Hom}_{\mathscr{O}_X}(\mathscr{G}, i_{x,*}(I_x)) = \mathrm{Hom}_{\mathscr{O}_{X,x}}(\mathscr{G}_x, I_x)$$

Thus we conclude first that there is a natural morphism of sheaves of $\mathscr{O}_X$-modules $\mathscr{F} \to \mathscr{I}$ obtained from the local maps $\mathscr{F}_x \to \mathscr{I}_x$. It is clearly injective. Second, the functor $\mathrm{Hom}_{\mathscr{O}_X}(-, \mathscr{I})$ is the direct product over all $x \in X$ of the stalk functor $\mathscr{G} \to \mathscr{G}$ which is exact, followed by $\mathrm{Hom}_{\mathscr{O}_{X,x}}(-, I_x)$, which is exact, since I_x is a injective. Hence $\mathrm{Hom}(-, \mathscr{I})$ is an exact functor, and therefore $\mathscr{I}$ is an injective $\mathscr{O}_X$-module. □

Corollary 20.1.2. *If X is any topological space, then the category $\mathbf{Ab}(X)$ of sheaves of abelian groups on X has enough injectives.*

Definition 20.1.3. *Let X be a topological space, and let $\Gamma(X, -) : \mathbf{Ab}(X) \to \mathbf{Ab}(X)$ be the global section functor. The cohomology groups of the sheaf $\mathscr{F}$ or the cohomology groups of X with values in $\mathscr{F}$, denoted by $H^i(X, \mathscr{F})$, are the groups $\mathscr{R}^i\Gamma(X, -)(\mathscr{F})$ induced by the right derived functor $\mathscr{R}^i\Gamma(X, -)$.*

Similarly, we can define cohomology groups of a $\mathscr{O}_X$-module to be the right-derived functor $\mathscr{R}^i\Gamma(X, -)$, where $\Gamma(X, -)$ is viewed as a functor from $\mathbf{Mod}(\mathcal{O}_X)$ to $\mathbf{Ab}(X)$. However, it turns out that this definition is unnecessary: the dericed functor of $\Gamma(X, -)$ in $\mathbf{Ab}(X)$ and $\mathbf{Mod}(\mathscr{O}_X)$ coincide.

20.2 Flasque sheaves

Definition 20.2.1. *A sheaf $\mathscr{F}$ on a topological space X is **flasque** if for every open subset U of X the restriction map $\mathscr{F}(X) \to \mathscr{F}(U)$ is surjective.*

We will see shortly that injective sheaves are flasque. Although this is not obvious from the definition, the notion of being flasque is local.

Proposition 20.2.2. *Let $\mathscr{F}$ be an $\mathscr{O}_X$-module. If $\mathscr{F}$ is flasque, so is $\mathscr{F}|_U$ for every open subset U of X. Conversely, if for every $x \in X$, there is a neighborhood U such that $\mathscr{F}|_U$ is flasque, then $\mathscr{F}$ is flasque.*

Proof. The first statement is trivial, let us prove the converse. Given any open set V of X, let s be a section of $\mathscr{F}$ over V. Let T be the set of all pairs (U, σ), where U is an open in X containing V, and σ is an extension of s to U. Partially order T by saying that $(U_1, \sigma_1) \leq (U_2, \sigma_2)$ if $U_1 \subseteq U_2$ and σ_2 extends σ_1, and observe that T is inductive, which means that every chain has an upper bound. Zorn's lemma provides us with a maximal extension of s to a section σ over an open set U_0. Were U_0 not X, there would exist an open set W in X not contained in U_0 such that $F|_W$ is flasque. Thus we could extend the section $\sigma|_{U_0 \cap W}$ to a section σ_0 of $\mathscr{F}$. Since σ and σ_0 agree on $U_0 \cap W$ by construction, their common extension to $U_0 \cup W$ extends s, a contradiction. □

Proposition 20.2.3. *Every $\mathscr{O}_X$-module may be embedded in a canonical functorial way into a flasque $\mathscr{O}_X$-module. Consequently, every $\mathscr{O}_X$-module has a canonical flasque resolution.*

Proof. Let $\mathscr{F}$ be an $\mathscr{O}_X$-module, and consider the Godement construction

$$U \mapsto \prod_{x \in U} \mathscr{F}_x$$

which we denote by $C^0(X, \mathscr{F})$. It is immediate that we have an injection of $\mathscr{O}_X$-modules $\mathscr{F} \to C^0(X, \mathscr{F})$ by Proposition 19.1.9. An element of $C^0(X, \mathscr{F})$ over any open set U is a collection (s_x) of elements indexed by U, each s_x lying over the $\mathscr{O}_{X,x}$-module $\mathscr{F}_x$. Such a sheaf is flasque because every U-indexed sequence s_x can be extended to an X-indexed sequence by assigning any arbitrary element of $\mathscr{F}_x$ to any $x \in X - U$. Hence $\mathbf{Mod}(\mathscr{O}_X)$ possesses enough flasque sheaves.

If $\mathscr{Z}_1$ is the cokernel of the canonical injection $\mathscr{F} \to C^0(X, \mathscr{F})$, we define $C^1(X, \mathscr{F})$ to be the flasque sheaf $C^0(X, \mathscr{Z}_1)$. In general,

$$\mathscr{Z}_n = \operatorname{coker}\left(\mathscr{Z}_{n-1} \hookrightarrow C^0(X, \mathscr{Z}_{n-1})\right) \quad \text{and} \quad C^n(X, \mathscr{F}) = C^0(X, \mathscr{Z}_n).$$

Putting all this information together, we obtain the desired flasque resolution of $\mathscr{F}$

$$0 \longrightarrow \mathscr{F} \longrightarrow C^0(X, \mathscr{F}) \longrightarrow C^1(X, \mathscr{F}) \longrightarrow C^2(X, \mathscr{F}) \longrightarrow \cdots$$

as claimed. □

Remark 20.2.1. The resolution of $\mathscr{F}$ constructed above will be called the **canonical flasque resolution** of $\mathscr{F}$ or the **Godement resolution** of $\mathscr{F}$.

Here is the principal property of flasque sheaves.

Theorem 20.2.4. *Let $0 \to \mathscr{F}_1 \to \mathscr{F}_2 \to \mathscr{F}_3 \to 0$ be an exact sequence of $\mathscr{O}_X$-modules, and assume $\mathscr{F}_1$ is flasque. Then this sequence is exact as a sequence of presheaves. If both $\mathscr{F}_1$ and $\mathscr{F}_2$ are flasque, so is $\mathscr{F}_3$. Finally, any direct summand of a flasque sheaf is flasque.*

Proof. Given any open set U, we must prove that

$$0 \longrightarrow \mathscr{F}_1(U) \xrightarrow{\varphi} \mathscr{F}_2(U) \xrightarrow{\psi} \mathscr{F}_3(U) \longrightarrow 0$$

is exact. By Proposition 19.1.53 and Proposition 19.1.54, the sole problem is to prove that $\mathscr{F}_2(U) \to \mathscr{F}_3(U)$ is surjective. By restricting we only need to prove the case for X. Let t be a global section of $\mathscr{F}_3$, then by Proposition 19.1.54, locally t may be lifted to sections of $\mathscr{F}$. Let T be the family of all pairs (U, σ) where U is an open in X, and σ is a section of $\mathscr{F}$ over U whose image in $\mathscr{F}_3(U)$ equal $t|_U$. Partially order T as in the proof of Proposition 20.2.2 and observe that T is inductive. Zorn's lemma provides us with a maximal lifting of t to a section $\sigma \in \mathscr{F}(U_0)$.

Were U_0 not X, there would exist $x \in X - U_0$, a neighborhood V of x, and a section τ of $\mathscr{F}$ over V which is a local lifting of $t|_V$. The sections $\sigma|_{V \cap U_0}$ and $\tau|_{V \cap U_0}$ have the same image in $\mathscr{F}_3(U_0 \cap V)$ under the map ψ, so their difference maps to 0. Since $\operatorname{im} \varphi = \ker \psi$, there is a section s of $\mathscr{F}_1(U_0 \cap V)$ such that

$$\sigma|_{U_0 \cap V} = \tau|_{V \cap U_0} + \varphi(s).$$

Since $\mathscr{F}_1$ is flasque, the section s is the restriction of a section $s_0 \in \mathscr{F}_1(V)$. Upon replacing τ by $\tau + \varphi(t_0)$ (which does not affect the image in $\mathscr{F}_3(V)$), we may assume that $\sigma|_{V\cap U_0} = \tau|_{V\cap U_0}$; that is, τ and σ agree on the overlap. Then we may extend σ to $U_0 \cup V$, contradicting the maximality of (U_0, σ); hence, $U_0 = X$.

Now suppose that $\mathscr{F}_1$ and $\mathscr{F}_2$ are flasque. If $t \in \mathscr{F}_3(U)$, then by the above, there is a section $s \in \mathscr{F}_2(U)$ mapping onto t. Since $\mathscr{F}_2$ is also flasque, we may lift s to a global section s_0 of $\mathscr{F}$. The image t_0 of s_0 in $\mathscr{F}_3(X)$ is the required extension of t to a global section of $\mathscr{F}_3$.

Finally, assume that $\mathscr{F}$ is flasque, and that $\mathscr{F} = \mathscr{F}_1 \oplus \mathscr{F}_2$ for some sheaf $\mathscr{F}_1, \mathscr{F}_2$. For any open subset U of X and any section $s \in \mathscr{F}_1(U)$, we can make s into a section $\tilde{s} \in \mathscr{F}(U)$ by setting the component of $\tilde{s}(U)$ in $\mathscr{F}_2(U)$ equal to the zero section. Since $\mathscr{F}$ is flasque, there is some section $t \in \mathscr{F}(X)$ such that $t|_U = \tilde{s}$. Write $t = t_1 + t_2$ for some unique $t_1 \in \mathscr{F}_1(X)$ and $t_2 \in \mathscr{F}_2(X)$, then

$$s + 0 = \tilde{s} = t|_U = (t_1)|_U + (t_2)|_U$$

with $(t_1)|_U \in \mathscr{F}_1(U)$ and $(t_2)|_U \in \mathscr{F}_2(U)$, so $s = (t_1)|_U$ with $t_1 \in \mathscr{F}_1(X)$, which shows that $\mathscr{F}_1$ is flasque. □

The following general proposition from Tohoku implies that flasque sheaves are $\Gamma(X, -)$-acyclic. It will also imply that soft sheaves are $\Gamma(X, -)$-acyclic. Since the only functor involved is the global section functor, it is customary to abbreviate $\Gamma(X, -)$-acyclic to acyclic.

Theorem 20.2.5. *Let $\mathscr{F}$ be an additive functor from the abelian category $\mathcal{C}$ to the abelian category $\mathcal{D}$, and suppose that $\mathcal{C}$ has enough injectives. Let $\mathfrak{X}$ be a class of objects in $\mathcal{C}$ which satisfies the following conditions:*

- *$\mathcal{C}$ possesses enough $\mathfrak{X}$-objects.*
- *If $0 \to A_1 \to A_2 \to A_3 \to 0$ is exact and if A_1 belongs to $\mathfrak{X}$, then $0 \to \mathscr{F}(A_1) \to \mathscr{F}(A_2) \to \mathscr{F}(A_3) \to 0$ is exact.*
- *If $0 \to A_1 \to A_2 \to A_3 \to 0$ is exact and A_1, A_2 belongs to $\mathfrak{X}$, then A_3 belongs to $\mathfrak{X}$.*
- *If A is an object of $\mathcal{C}$ and A is a direct summand of some object in $\mathfrak{X}$, then A belongs to $\mathfrak{X}$.*

Then every injective object belongs to $\mathfrak{X}$, for each M in $\mathfrak{X}$ we have $\mathcal{R}^i\mathscr{F}(M) = 0$ for $i > 0$, and finally the functors $\mathcal{R}^i\mathscr{F}$ may be computed by taking $\mathfrak{X}$-resolutions.

Proof. Let I be an injective of $\mathcal{C}$. Then I admits a monomorphism into some object M of the class $\mathfrak{X}$. We have an exact sequence

$$0 \longrightarrow I \xrightarrow{\varphi} M \longrightarrow \operatorname{coker}\varphi \longrightarrow 0$$

and as I is injective this sequence split. Thus I is a direct summand of M and thus belongs to $\mathfrak{X}$ be the condition.

Let us now show that $\mathcal{R}^n\mathscr{F}(M) = 0$ for $i > 0$ if M lies in $\mathfrak{X}$. Now, $\mathcal{C}$ possesses enough injectives, so if we have an exact sequence

$$0 \longrightarrow M \longrightarrow I \longrightarrow K \longrightarrow 0$$

where I is injective. Then from the long exact sequence of $\mathcal{R}^\bullet\mathscr{F}$ and the fact $\mathcal{R}^i\mathscr{F}(I) = 0$ for $i \geq 1$ we conclude

$$\mathcal{R}^1\mathscr{F}(M) = 0 \quad \text{and} \quad \mathcal{R}^i\mathscr{F}(M) = \mathcal{R}^{i-1}\mathscr{F}(K) \textit{ for } i \geq 2.$$

Since M and I are both in $\mathfrak{X}$, K is also in $\mathfrak{X}$. Therefore by applying the same argument on K we also get $\mathcal{R}^1\mathscr{F}(K) = 0$. Now the claim follows by an induction. □

This result tells us that flasque sheaves are acyclic for the functor $\Gamma(X, -)$. Hence we can calculate cohomology using flasque resolutions.

Proposition 20.2.6. *Flasque sheaves are acyclic, that is $H^i(X, \mathscr{F}) = 0$ for every flasque sheaf $\mathscr{F}$ and all $i \geq 1$, and the cohomology groups $H^i(X, \mathscr{F})$ of any arbitrary sheaf $\mathscr{F}$ can be computed using flasque resolutions.*

Proof. Apply Theorem 20.2.5 on the functor $\Gamma(X, -) : \mathbf{Ab}(X) \to \mathbf{Ab}(X)$. □

In view of the proposition above, we also have the following result.

Proposition 20.2.7. *Let $(X, \mathscr{O}_X)$ be a ringed space. Then the derived functors of the functor $\Gamma(X, -)$ from $\mathbf{Mod}(\mathscr{O}_X)$ to $\mathbf{Ab}(X)$ coincide with the cohomology functors $H^i(X, -)$.*

Proof. Let I be an injective $\mathscr{O}_X$-module, then $\mathscr{I}$ is a flasque $\mathscr{O}_X$-module by Theorem 20.2.5. Therefore an injective resolution in $\mathbf{Mod}(\mathscr{O}_X)$ is a flasque resolution in $\mathbf{Ab}(X)$, hence computes the sheaf cohomology. □

20.3 Locality of cohomology

we first sate a useful result in abelian categories.

Theorem 20.3.1. *Let (F, G) be an adjoint pair between abelian categories $\mathcal{C}$ and $\mathcal{D}$, in the sense that*

$$\mathrm{Hom}_{\mathcal{D}}(F(X), Y) = \mathrm{Hom}_{\mathcal{C}}(X, G(Y)).$$

Assume that F is exact, then G maps injectives to injectives.

Proof. Let I be injective in $\mathcal{D}$. Assume that we have an exact diagram in $\mathcal{C}$:

$$\begin{tikzcd} 0 \arrow[r] & X \arrow[r] \arrow[d] & Y \\ & G(I) & \end{tikzcd}$$

Then by applying the exact functor F we get an exact diagram in $\mathcal{D}$:

$$\begin{tikzcd} 0 \arrow[r] & F(X) \arrow[r] \arrow[d] & F(Y) \arrow[d, dashed] \\ & FG(I) \arrow[r] & I \end{tikzcd}$$

where $FG(I) \to I$ is the unit map of the adjunction (F, G). Since I is injective, this extends to a map $F(Y) \to I$. Applying G again and compose the counit map $I \to GF(Y)$ we get the desired map $Y \to G(I)$, so $G(I)$ is injective. □

Proposition 20.3.2. *Let $f : X \to Y$ be a morphism of ringed spaces. Assume f is flat. Then $f_*\mathcal{I}$ is an injective $\mathcal{O}_Y$-module for any injective $\mathcal{O}_X$-module $\mathcal{I}$. In particular, the pushforward $f_* : \mathbf{Ab}(X) \to \mathbf{Ab}(Y)$ transforms injective abelian sheaves into injective abelian sheaves.*

Proof. In this case f^* is exact, and we have an adjoint pair (f^*, f_*). Now apply Theorem 20.3.1 we get the claim. □

The following lemma says there is no ambiguity in defining the cohomology of a sheaf $\mathcal{F}$ over an open.

Lemma 20.3.3. *Let X be a ringed space. Let $U \subseteq X$ be an open subspace.*

(a) If $\mathcal{I}$ is an injective $\mathcal{O}_X$-module then $\mathcal{I}|_U$ is an injective $\mathcal{U}$-module.

(b) For any sheaf of $\mathcal{O}_X$-modules $\mathcal{F}$ we have $H^p(U, \mathcal{F}) = H^p(U, \mathcal{F}|_U)$.

Proof. Denote $j : U \to X$ the open immersion. Then $(j_!, j^{-1})$ satisfies the condition of Theorem 20.3.1. By definition $H^p(U, \mathcal{F}) = H^p(\Gamma(U, \mathcal{I}^\bullet))$ where $\mathcal{F} \to \mathcal{I}^\bullet$ is an injective resolution in $\mathbf{Mod}(\mathcal{O}_X)$. By the above we see that $\mathcal{F}|_U \to \mathcal{I}|_U$ is an injective resolution in $\mathbf{Mod}(\mathcal{O}_U)$. Hence $H^p(U, \mathcal{F}|_U)$ is equal to $H^p(\Gamma(U, \mathcal{I}^\bullet|_U))$. Of course $\Gamma(U, \mathcal{F}) = \Gamma(U, \mathcal{F}|_U)$ for any sheaf $\mathcal{F}$ on X. Hence the equality in (b). □

Let $f : X \to Y$ be a continuous. Since the functor f_* is left-exact, for an injective resolution $0 \to \mathcal{F} \to \mathcal{I}^\bullet$ we define

$$\mathcal{R}^i f_* \mathcal{F} = H^i(f_* \mathcal{I}^\bullet)$$

to be the ***i*-th higher direct image of** $\mathcal{F}$.

Proposition 20.3.4. *Let $f : X \to Y$ be a morphism of ringed spaces. Let $\mathcal{F}$ be a $\mathcal{O}_X$-module. The sheaves $\mathcal{R}^i f_* \mathcal{F}$ are the sheaves associated to the presheaves*

$$U \mapsto H^i(f^{-1}(U), \mathcal{F}).$$

Proof. Let $0 \to \mathcal{F} \to \mathcal{I}^\bullet$ be an injective resolution. Then $\mathcal{R}^i f_* \mathcal{F}$ is by definition the i-th cohomology sheaf of the complex

$$f_*\mathcal{I}^0 \longrightarrow f_*\mathcal{I}^1 \longrightarrow f_*\mathcal{I}^2 \longrightarrow \cdots$$

By definition of the abelian category structure on $\mathcal{O}_Y$-modules this cohomology sheaf is the sheaf associated to the presheaf

$$V \mapsto \frac{\ker(f_*\mathcal{I}^i(V) \to f_*\mathcal{I}^{i+1}(V))}{\operatorname{im}(f_*\mathcal{I}^{i-1}(V) \to f_*\mathcal{I}^i(V))}$$

and this is obviously equal to

$$\frac{\ker\left(\mathcal{I}^i(f^{-1}(V)) \to \mathcal{I}^{i+1}(f^{-1}(V))\right)}{\operatorname{im}\left(\mathcal{I}^{i-1}(f^{-1}(V)) \to \mathcal{I}^i(f^{-1}(V))\right)}$$

which is equal to $H^i(f^{-1}(V), \mathcal{F})$ and we win. □

Corollary 20.3.5. *Let $f : X \to Y$ be a morphism of ringed spaces. Let $\mathcal{F}$ be a sheaf of $\mathcal{O}_X$-modules. If $\mathcal{F}$ is flasque, then $\mathcal{R}^p f_* \mathcal{F} = 0$ for $p > 0$.*

Proof. This follows from Proposition 20.2.6 and Proposition 20.3.4. □

Proposition 20.3.6. *Let $f : X \to Y$ be a morphism of ringed spaces. Let $\mathcal{F}$ be an $\mathcal{O}_X$-module. Let $V \subseteq Y$ be an open subspace. Denote $g : f^{-1}(V) \to V$ the restriction of f. Then we have*

$$\mathcal{R}^i g_*(\mathcal{F}|_{f^{-1}(V)}) = (\mathcal{R}^i f_* \mathcal{F})|_V.$$

There is a similar statement for the derived image $\mathcal{R}^i f_* \mathcal{F}$ where $\mathcal{F}^\bullet$ is a bounded below complex of $\mathcal{O}_X$-modules.

Proof. Choose an injective resolution $0 \to \mathcal{F} \to \mathcal{I}^\bullet$ and use that $\mathcal{F}|_{f^{-1}(V)} \to \mathcal{I}|_{f^{-1}(V)}$ is an injective resolution also. □

Chapter 21

Čech cohomology

21.1 The Čech cohomology group with respect to a covering

Let X be a topological space and $\mathcal{U} = (U_i)_{i\in I}$ be an open covering of X. Given any finite sequence $(i_0, \ldots, i_p)$ of elements of I, we let

$$U_{i_0\ldots i_p} := U_{i_0} \cap \cdots \cap U_{i_p}.$$

Also, we denote by $U_{i_0\ldots\widehat{i_j}\ldots i_p}$ the intersection

$$U_{i_0\ldots\widehat{i_j}\ldots i_p} = U_{i_0} \cap \cdots \cap \widehat{U}_{i_j} \cap \cdots \cap U_{i_p}.$$

Then we have $p+1$ inclusion maps

$$\delta_j^p : U_{i_0\ldots i_p} \to U_{i_0\ldots\widehat{i_j}\ldots i_p} \quad \text{for } 0 \leq j \leq p.$$

Definition 21.1.1. *Given a topological space X, an open cover $\mathcal{U} = (U_i)_{i\in I}$ of X, and a abelian presheaf $\mathscr{F}$ on X, the* ***Čech p-cochains*** *$C^p(\mathcal{U}, \mathscr{F})$ is the set of all functions f with domain I^{p+1} such that $f(i_0, \ldots, i_p) \in \mathscr{F}(U_{i_0} \ldots i_p)$; in other words,*

$$C^p(\mathcal{U}, \mathscr{F}) = \prod_{(i_0,\ldots,i_p)\in I^{p+1}} \mathscr{F}(U_{i_0\ldots i_p})$$

the set of all I^{p+1}-indexed families $(f_{i_0\ldots i_p})$ with $f_{i_0\ldots i_p} \in \mathscr{F}(U_{i_0\ldots i_p})$.

Remark 21.1.1. Since $\mathscr{F}(\emptyset) = 0$, for any cochain $f \in C^p(\mathcal{U}, \mathscr{F})$, if $U_{i_0\ldots i_p} = \emptyset$, then $f_{i_0\ldots i_p} = 0$. Therefore, we could define $C^p(\mathcal{U}, \mathscr{F})$ as the set of families $f_{i_0\ldots i_p}$ corresponding to tuples $(i_0, \ldots, i_p) \in I^{p+1}$ such that $U_{i_0\ldots i_p} \neq \emptyset$.

Each inclusion map $\delta_j^p : U_{i_0\ldots i_p} \to U_{i_0\ldots\widehat{i_j}\ldots i_p}$ induces a map

$$\mathscr{F}(\delta_j^p) : \mathscr{F}(U_{i_0\ldots\widehat{i_j}\ldots i_p}) \to \mathscr{F}(U_{i_0\ldots i_p})$$

which is none other that the restriction map.

Definition 21.1.2. *Given a topological space X, an open cover $\mathcal{U} = (U_i)_{i\in I}$ of X, and a abelian presheaf*

$\mathscr{F}$ on X, the coboundary maps $d : C^p(\mathcal{U}, \mathscr{F}) \to C^{p+1}(\mathcal{U}, \mathscr{F})$ are given by

$$d = \sum_{j=0}^{p+1} (-1)^j \mathscr{F}(\delta_j^{p+1}).$$

More explicitly, for any p-cochain $f \in C^p(\mathcal{U}, \mathscr{F})$, for any sequence $(i_0, \dots, i_{p+1}) \in I^{p+2}$, we have

$$(df)_{i_0 \dots i_{p+1}} = \sum_{j=0}^{p+1} (-1)^j (f_{i_0 \dots \widehat{i_j} \dots i_{p+1}})|_{U_{i_0 \dots i_{p+1}}}.$$

Proposition 21.1.3. *With the notations above, we have $d^2 = 0$. Thus we obtain a complex $C^\bullet(\mathcal{U}, \mathscr{F})$.*

Proof. This is a typical computation. Let $f \in C^p(\mathcal{U}, \mathscr{F})$,

$$\begin{aligned}
(d^2 f)_{i_0 \dots i_{p+2}} &= \sum_{k=0}^{p+2} (-1)^k \big((df)_{i_0 \dots \widehat{i_k} \dots i_{p+2}}\big)|_{U_{i_0 \dots i_{p+2}}} \\
&= \sum_{j<k} (-1)^k \big((-1)^j (f_{i_0 \dots \widehat{i_j} \dots \widehat{i_k} \dots i_{p+1}})|_{U_{i_0 \dots \widehat{i_k} \dots i_{p+2}}}\big)|_{U_{i_0 \dots i_{p+2}}} \\
&+ \sum_{j>k} (-1)^k \big((-1)^{j-1} (f_{i_0 \dots \widehat{i_k} \dots \widehat{i_j} \dots i_{p+1}})|_{U_{i_0 \dots \widehat{i_k} \dots i_{p+2}}}\big)|_{U_{i_0 \dots i_{p+2}}} \\
&= \sum_{j<k} (-1)^k (-1)^j (f_{i_0 \dots \widehat{i_j} \dots \widehat{i_k} \dots i_{p+1}})|_{U_{i_0 \dots i_{p+2}}} \\
&- \sum_{j>k} (-1)^k (-1)^j (f_{i_0 \dots \widehat{i_k} \dots \widehat{i_j} \dots i_{p+1}})|_{U_{i_0 \dots i_{p+2}}} \\
&= 0
\end{aligned}$$

as desired. □

Therefore, we can form the Čech cohomology groups with respect to $\mathcal{U}$ as follows.

Definition 21.1.4. *Given a topological space X, an open cover $\mathcal{U} = (U_i)_{i \in I}$ of X, and a abelian presheaf $\mathscr{F}$ on X, we define*

$$\check{H}^p(\mathcal{U}, \mathscr{F}) = H^p(C^\bullet(\mathcal{U}, \mathscr{F}))$$

*to be the **p-th Čech-cohomology group with respect to the covering $\mathcal{U}$**.*

First of all, we note that $\check{H}^0(\mathcal{U}, \mathscr{F})$ can be easily computed.

Proposition 21.1.5. *Given a topological space X, an open cover $\mathcal{U}$ of X, and a sheaf $\mathscr{F}$ on X, then*

$$\check{H}^0(\mathcal{U}, \mathscr{F}) = \mathscr{F}(X) = \Gamma(X, \mathscr{F}).$$

More generally, if $\mathscr{F}$ is an abelian presheaf, then the following are equivalent

- *$\mathscr{F}$ is a sheaf.*
- *For every open covering $\mathcal{U} = (U_i)_{i \in I}$ the natural map*

$$\mathscr{F}(U) \to \check{H}^0(\mathcal{U}, \mathscr{F})$$

is bijective.

Proof. By definition, $\check{H}^0(\mathcal{U}, \mathcal{F}) = \ker(C^0(\mathcal{U}, \mathcal{F}) \to C^1(\mathcal{U}, \mathcal{F}))$. If $f \in C^0(\mathcal{U}, \mathcal{F})$ is given by (f_i), then for each $(i, j) \in I^2$, $(df)_{i,j} = f_j - f_i$. So $df = 0$ says the sections f_i and f_j agree on $U_i \cap U_j$. Thus it follows that $\ker d = \Gamma(X, \mathcal{F})$ if and only if $\mathcal{F}$ is a sheaf. □

An element of $C^p(\mathcal{U}, \mathcal{F})$ is called a ***p*-cochain**. We say that a p-cochain $f \in C^p(\mathcal{U}, \mathcal{F})$ is **alternating** if

- $f_{i_0 \dots i_p} = 0$ whenever any two of the indices $i_0, \dots, i_p$ are equal.
- For every permutation σ of the indices, we have $f_{i_{\sigma(0)} \dots i_{\sigma(p)}} = (-1)^\sigma f_{i_0 \dots i_p}$.

It is clear that if $f \in C^p(\mathcal{U}, \mathcal{F})$ is alternating, then df is also alternating, hence we get a complex $C^\bullet_{alt}(\mathcal{U}, \mathcal{F})$.

Definition 21.1.6. *Let X be a topological space. Let $\mathcal{U} = (U_i)_{i \in I}$ be an open covering. Let $\mathcal{F}$ be an abelian presheaf on X. The complex $C^\bullet_{alt}(\mathcal{U}, \mathcal{F})$ is the* ***alternating Čech complex*** *associated to $\mathcal{F}$ and the open covering $\mathcal{U}$.*

Let us endow the set of indices I with a total ordering and set

$$C^p_{ord}(\mathcal{U}, \mathcal{F}) := \prod_{i_0 < \dots < i_p} \mathcal{F}(U_{i_0 \dots i_p})$$

It can immediately be verified that the differential d of $C^\bullet(\mathcal{U}, \mathcal{F})$ induces a differential on $C^\bullet_{ord}(\mathcal{U}, \mathcal{F})$, by restriction.

Definition 21.1.7. *Let X be a topological space. Let $\mathcal{U} = (U_i)_{i \in I}$ be an open covering. Let $\mathcal{F}$ be an abelian presheaf on X. Assume given a total ordering on I. The complex $C^\bullet_{ord}(\mathcal{U}, \mathcal{F})$ is the* ***ordered Čech complex*** *associated to $\mathcal{F}$, the open covering $\mathcal{U}$ and the given total ordering on I.*

There is an obvious comparison map between the ordered Čech complex and the alternating Čech complex. Namely, consider the map

$$c : C^\bullet_{ord}(\mathcal{U}, \mathcal{F}) \to C^\bullet_{alt}(\mathcal{U}, \mathcal{F})$$

given by the rule

$$c(s)_{i_0 \dots i_p} = \begin{cases} (-1)^\sigma s_{i_{\sigma(0)}, \dots, i_{\sigma(p)}} & \text{if } i_{\sigma(0)} < \dots < i_{\sigma(p)}, \\ 0 & \text{if } i_n = i_m \text{ for some } n \neq m. \end{cases}$$

The alternating and ordered Čech complexes are often identified in the literature via the map c. Namely we have the following easy lemma.

Lemma 21.1.8. *Let X be a topological space. Let $\mathcal{U}$ be an open covering. Assume I comes equipped with a total ordering. The map c is a morphism of complexes. In fact it induces an isomorphism*

$$c : C^\bullet_{ord}(\mathcal{U}, \mathcal{F}) \to C^\bullet_{alt}(\mathcal{U}, \mathcal{F})$$

of complexes.

There is also a map $\pi : C^\bullet(\mathcal{U}, \mathcal{F}) \to C^\bullet_{ord}(\mathcal{U}, \mathcal{F})$ which is described by the rule

$$\pi(s)_{i_0 \dots i_p} = s_{i_0 \dots i_p}$$

whenever $i_0 < \cdots < i_p$. The following result is immediate.

Lemma 21.1.9. *Let X be a topological space. Let $\mathcal{U}$ be an open covering. Assume I comes equipped with a total ordering. The map $\pi : C^\bullet(\mathcal{U}, \mathcal{F}) \to C^\bullet_{ord}(\mathcal{U}, \mathcal{F})$ is a morphism of complexes which is a left inverse to the morphism c. Moreover, it induces an isomorphism*

$$\tilde{\pi} : C^\bullet_{alt}(\mathcal{U}, \mathcal{F}) \to C^\bullet_{ord}(\mathcal{U}, \mathcal{F})$$

of complexes.

It turns out that the maps π and c give a homotopy equivalence between $C^\bullet(\mathcal{U}, \mathcal{F})$ and $C^\bullet_{alt}(\mathcal{U}, \mathcal{F})$. Therefore, we can use the alternating complex to compute the Čech cohomology.

Theorem 21.1.10. *Let X be a topological space. Let $\mathcal{U}$ be an open covering. Assume I comes equipped with a total ordering. The map $c \circ \pi$ is homotopic to the identity on $C^\bullet(\mathcal{U}, \mathcal{F})$. In particular the inclusion map $C^\bullet_{alt}(\mathcal{U}, \mathcal{F}) \to C^\bullet(\mathcal{U}, \mathcal{F})$ is a homotopy equivalence.*

Corollary 21.1.11. *Given a total ordering on I, there exists a canonical isomorphism*

$$H^\bullet(C^\bullet_{ord}(\mathcal{U}, \mathcal{F})) \cong H^\bullet(C^\bullet(\mathcal{U}, \mathcal{F})).$$

Corollary 21.1.12. *If $\mathcal{U}$ is made up of n open subsets, then $\check{H}^p(\mathcal{U}, \mathcal{F}) = 0$ for every $p \geq n$.*

Proof. Indeed, if $p \geq n$, there does not exist any strictly increasing $(p+1)$-uple of indices $i_0, \dots, i_p$. Hence $C^p_{ord}(\mathcal{U}, \mathcal{F}) = 0$, whence $\check{H}^p(\mathcal{U}, \mathcal{F}) = 0$. □

21.2 Čech cohomology as a functor on presheaves

Warning: In this subsection we work almost exclusively with presheaves and categories of presheaves and the results are completely wrong in the setting of sheaves and categories of sheaves!

Let X be a ringed space. Let $\mathcal{U} = (U_i)_{i \in I}$ be an open covering. Let $\mathcal{F}$ be a presheaf of $\mathcal{O}_X$-modules. We have the Čech complex $C^\bullet(\mathcal{U}, \mathcal{F})$ of $\mathcal{F}$ just by thinking of $\mathcal{F}$ as a presheaf of abelian groups. However, each term $C^p(\mathcal{U}, \mathcal{F})$ has a natural structure of a $\mathcal{O}_X(X)$-module and the differential is given by $\mathcal{O}_X(X)$-module maps. Moreover, it is clear that the construction

$$\mathcal{F} \to C^\bullet(\mathcal{U}, \mathcal{F})$$

is functorial in $\mathcal{F}$. In fact, it is a functor

$$C^\bullet(\mathcal{U}, -) : \mathbf{PMod}(\mathcal{O}_X) \to \mathcal{C}^+(\mathbf{Mod}_{\mathcal{O}_X(X)})$$

Proposition 21.2.1. *The functor $C^\bullet(\mathcal{U}, -)$ is an exact functor.*

Proof. For any open $U \subseteq X$ the functor $\mathcal{F} \to \mathcal{F}(U)$ is an additive exact functor from $\mathbf{PMod}(\mathcal{O}_X)$ to $\mathbf{Mod}_{\mathcal{O}_X(X)}$. The terms $C^p(\mathcal{U}, \mathcal{F})$ of the complex are products of these exact functors and

hence exact. Moreover a sequence of complexes is exact if and only if the sequence of terms in a given degree is exact. Hence the lemma follows. □

Theorem 21.2.2. *Let X be a ringed space. Let $\mathcal{U} = (U_i)_{i\in I}$ be an open covering. The functors $\check{H}^p(\mathcal{U}, -)$ form a δ-functor from the abelian category of presheaves of $\mathcal{O}_X$-modules to the category of $\mathcal{O}_X(X)$-modules*

Proof. By Proposition 21.2.1 a short exact sequence of presheaves of $\mathcal{O}_X$-modules is turned into a short exact sequence of complexes of $\mathcal{O}_X(X)$-modules. Hence we can get a long exact sequence. □

Proposition 21.2.3. *Let X be a ringed space. Let $\mathcal{U}$ be an open covering of X. The Čech cohomology functors $\check{H}^p(\mathcal{U}, -)$ are canonically isomorphic as a δ-functor to the right derived functors of the functor*

$$\check{H}^0(\mathcal{U}, -) : \mathbf{PMod}(\mathcal{O}_X) \to \mathbf{Mod}_{\mathcal{O}_X(X)}.$$

Moreover, there is a functorial quasi-isomorphism

$$C^\bullet(\mathcal{U}, \mathcal{F}) \to \mathcal{R}\check{H}^0(\mathcal{U}, \mathcal{F}).$$

Proof. This comes from the universal property of the δ-functor. □

21.3 The Čech cohomology groups

Our next goal is to define Čech cohomology groups $\check{H}^p(X, \mathcal{F})$ that are independent of the open cover $\mathcal{U}$ chosen for X.

We say that a covering $\mathcal{V} = (V_j)_{j\in J}$ of X is a **refinement** of another covering $\mathcal{U} = \{U_i\}_{i\in I}$ if there exists a map $\tau : J \to I$ such that $V_j \subseteq U_{\tau(j)}$ for every $j \in J$. We then have a homomorphism, which we also denote by τ:

$$C^p(\mathcal{U}, \mathcal{F}) \to C^p(\mathcal{V}, \mathcal{F})$$

defined by

$$\tau(f)_{j_0\dots j_p} = f_{\tau(j_0)\dots\tau(j_p)}|_{V_{j_0\dots j_p}}$$

This homomorphism commutes with the differentials and therefore induces a homomorphism

$$\tau^* : \check{H}^p(\mathcal{U}, \mathcal{F}) \to \check{H}^p(\mathcal{V}, \mathcal{F}).$$

Proposition 21.3.1. *The homomorphisms $\tau^* : \check{H}^p(\mathcal{U}, \mathcal{F}) \to \check{H}^p(\mathcal{V}, \mathcal{F})$ depend only on $\mathcal{U}$ and $\mathcal{V}$ and not on the chosen mapping τ.*

Proof. Let τ_1 and τ_2 be two mappings from I to J such that $V_j \subseteq U_{\tau_1(j)}$ and $V_j \subseteq U_{\tau_2(j)}$, we have to show that $\tau_1^* = \tau_2^*$.

Let $f \in C^p(\mathcal{U}, \mathcal{F})$, define a map $\kappa : C^p(\mathcal{U}, \mathcal{F}) \to C^{p-1}(\mathcal{V}, \mathcal{F})$ by setting

$$(\kappa f)_{j_0\dots j_{p-1}} = \sum_{k=0}^{p-1} (-1)^k (f_{\tau_1(j_1)\dots\tau_1(j_k)\tau_2(j_k)\dots\tau_2(j_{p-1})})|_{V_{j_0\dots j_{p-1}}}.$$

Then, it can be verified that

$$\kappa(df) + d(\kappa f) = \tau_2(f) - \tau_1(f).$$

Thus k defines a homotopy from τ_2^* to τ_1^*, which implies the claim. □

Corollary 21.3.2. *If $\mathcal{V}$ is a refinement of $\mathcal{U}$ and if $\mathcal{U}$ is a refinement of $\mathcal{V}$, then $\check{H}^p(\mathcal{U}, \mathcal{F}) \to \check{H}^p(\mathcal{V}, \mathcal{F})$ is an isomorphism.*

Proof. Let us keep the notation above. If $\mathcal{U}$ is a refinement of a covering $\mathcal{W}$ with a map σ such that $U_i \subseteq W_{\sigma(i)}$, then $\mathcal{V}$ is a refinement of $\mathcal{W}$ because $V_j \subseteq W_{\sigma\circ\tau(j)}$. Moreover, $(\sigma \circ \tau)^* = \sigma^* \circ \tau^*$ in an obvious way. Let us now take $\mathcal{W} = \mathcal{V}$. Then $\sigma^* \circ \tau^*$ and $\tau^* \circ \sigma^*$ coincides with $\mathbf{1}^*$ by the result above. Hence τ^* is bijective. □

The relation $\mathcal{U}$ is a refinement of $\mathcal{V}$ (which we denote henceforth by $\mathcal{U} \prec \mathcal{V}$) is a relation of a preorder between coverings of X; moreover, this relation is filtered, since if $\mathcal{U} = \{U_i\}_{i\in I}$ and $\mathcal{V} = \{V_j\}_{j\in J}$ are two coverings, then the covering $\mathcal{W} = \{U_i \cap V_j\}_{(i,j)\in I\times J}$ is a refinement of $\mathcal{U}$ and $\mathcal{V}$. Consequently, it appears that the family $(\check{H}^p(\mathcal{U}, \mathcal{F}))_{\mathcal{U}}$ is a direct mapping family of groups indexed by the directed set of open covers of X. However, there is a set-theoretic diffculty, which is that the family of open covers of X is not a set because it allows arbitrary index sets.

A way to circumvent this difficulty is provided by Serre. The key observation is that any covering $(U_i)_{i\in I}$ is equivalent to a covering $(U'_j)_{j\in L}$ whose index set L is a subset of 2^X. Indeed, we can take for $(U'_j)_{j\in L}$ the set of all open subsets of X that belong to the family $(U_i)_{i\in I}$.

As we noted earlier, if $\mathcal{U}$ and $\mathcal{V}$ are equivalent, then there is an isomorphism between $\check{H}^p(\mathcal{U}, \mathcal{F})$ and $\check{H}^p(\mathcal{V}, \mathcal{F})$, so we can define

$$\check{H}^p(X, \mathcal{F}) = \varinjlim \check{H}^p(\mathcal{U}, \mathcal{F})$$

with respect to coverings $\mathcal{U}$ whose index set is a subset of 2^X. In summary, we have the following definition.

Definition 21.3.3. *Given a topological space X and a abelian presheaf $\mathcal{F}$ on X, the* ***Čech cohomology groups*** *$\check{H}^p(X, \mathcal{F})$ with values in $\mathcal{F}$ are defined by*

$$\check{H}^p(X, \mathcal{F}) = \varinjlim \check{H}^p(\mathcal{U}, \mathcal{F})$$

with respect to coverings $\mathcal{U}$ whose index set is a subset of 2^X.

21.4 Long exact sequence of Čech-cohomology

21.4.1 General case

Let $0 \to \mathcal{A} \to \mathcal{B} \to \mathcal{C} \to 0$ be an exact sequence of sheaves. If $\mathcal{U}$ is a covering of X, the sequence

$$0 \longrightarrow C^\bullet(\mathcal{U}, \mathcal{A}) \xrightarrow{\alpha} C^\bullet(\mathcal{U}, \mathcal{B}) \xrightarrow{\beta} C^\bullet(\mathcal{U}, \mathcal{C})$$

is obviously exact, but the homomorphism β need not be surjective in general. Denote by $C_0^\bullet(\mathcal{U}, \mathcal{C})$ the image of this homomorphism; it is a subcomplex of $C^\bullet(\mathcal{U}, \mathcal{C})$ whose cohomology

groups will be denoted by $\check{H}_0^p(\mathcal{U},\mathscr{C})$. The exact sequence of complexes:

$$0 \longrightarrow C^\bullet(\mathcal{U},\mathscr{A}) \xrightarrow{\alpha} C^\bullet(\mathcal{U},\mathscr{B}) \xrightarrow{\beta} C_0^\bullet(\mathcal{U},\mathscr{C}) \longrightarrow 0$$

giving rise to a long exact sequence of cohomology

$$\cdots \longrightarrow \check{H}^p(\mathcal{U},\mathscr{A}) \longrightarrow \check{H}^p(\mathcal{U},\mathscr{B}) \longrightarrow \check{H}_0^p(\mathcal{U},\mathscr{C}) \xrightarrow{\delta} \check{H}^{p+1}(\mathcal{U},\mathscr{A}) \longrightarrow \cdots$$

where the coboundary operator δ is defined as usual.

Now let $\mathcal{U} = (U_i)_{i\in I}$ and $\mathcal{V} = (V_j)_{j\in J}$ be two coverings and let $\tau : J \to I$ be such that $V_j \subseteq U_{\tau(j)}$; we thus have $\mathcal{V} \prec \mathcal{U}$. The commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & C^\bullet(\mathcal{U},\mathscr{A}) \arrow[r, "\alpha"] \arrow[d, "\tau"] & C^\bullet(\mathcal{U},\mathscr{B}) \arrow[r, "\beta"] \arrow[d, "\tau"] & C^\bullet(\mathcal{U},\mathscr{C}) \arrow[d, "\tau"] \\
0 \arrow[r] & C^\bullet(\mathcal{V},\mathscr{A}) \arrow[r, "\alpha"] & C^\bullet(\mathcal{V},\mathscr{B}) \arrow[r, "\beta"] & C^\bullet(\mathcal{V},\mathscr{C})
\end{tikzcd}$$

shows that τ maps $C_0^\bullet(\mathcal{U},\mathscr{C})$ into $C_0^\bullet(\mathcal{V},\mathscr{C})$, thus defining the homomorphisms

$$\tau^* : \check{H}_0^p(\mathcal{U},\mathscr{C}) \to \check{H}_0^p(\mathcal{V},\mathscr{C}).$$

Moreover, the homomorphisms τ are independent of the choice of the mapping τ: this follows from the fact that, if $f \in C_0^p(\mathcal{U},\mathscr{C})$, we have $\kappa f \in C_0^{p-1}(\mathcal{V},\mathscr{C})$, with the notations of Proposition 21.3.1. We have thus obtained canonical homomorphisms $H_0^p(\mathcal{U},\mathscr{C}) \to \check{H}_0^p(\mathcal{V},\mathscr{C})$; we might then define $\check{H}_0^p(X,\mathscr{C})$ as the inductive limit of the groups $\check{H}^p(X,\mathscr{C})$.

Because an inductive limit of exact sequences is an exact sequence, we obtain:

Proposition 21.4.1. *The sequence*

$$\cdots \longrightarrow \check{H}^p(X,\mathscr{A}) \xrightarrow{\alpha^*} \check{H}^p(X,\mathscr{B}) \xrightarrow{\beta^*} \check{H}_0^p(X,\mathscr{C}) \xrightarrow{\delta} \check{H}^{p+1}(X,\mathscr{A}) \longrightarrow \cdots$$

is exact.

To apply the preceding proposition, it is convenient to compare the groups $\check{H}_0^p(X,\mathscr{C})$ and $\check{H}^p(X,\mathscr{C})$. The inclusion of $C_0^\bullet(\mathcal{U},\mathscr{C})$ in $C^\bullet(\mathcal{U},\mathscr{C})$ defines the homomorphisms

$$\check{H}_0^p(\mathcal{U},\mathscr{C}) \to \check{H}^p(\mathcal{U},\mathscr{C}),$$

hence, by passing to the limit with $\mathcal{U}$, the homomorphisms:

$$\check{H}_0^p(X,\mathscr{C}) \to \check{H}^p(X,\mathscr{C})$$

We first prove a lemma.

Lemma 21.4.2. *Let $\mathcal{U} = (U_i)_{i\in I}$ be a covering and let $f = (f_j)$ be an element of $C^0(\mathcal{U},\mathscr{C})$. There exists a covering $\mathcal{V} = (V_j)_{j\in J}$ and a mapping $\tau : J \to I$ such that $V_j \subseteq U_{\tau(j)}$ and $\tau(f) \in C_0^0(\mathcal{V},\mathscr{C})$.*

Proof. For any $x \in X$, take a $\tau(x) \in I$ such that $x \in U_{\tau(x)}$. Since $f_{\tau(x)}$ is a section of $\mathscr{C}$ over $U_{\tau(x)}$, by the surjectivity of β there exists an open neighborhood V_x of x, contained in $U_{\tau(x)}$ and

a section b_x of $\mathscr{B}$ over V_x such that $\beta(b_x) = f_{\tau(x)}|_{V_x}$ on V_x. The $(V_x)_{x\in X}$ form a covering $\mathcal{V}$ of X, and the b_x form a 0-chain b of $\mathcal{V}$ with values in $\mathcal{U}$. From the construction we have $\tau(f) = \beta(b)$, so that $\tau(f) \in C_0^0(\mathcal{V}, \mathscr{C})$. □

Now we can prove the following result.

Theorem 21.4.3. *The canonical homomorphism $\check{H}_0^p(X, \mathscr{C}) \to \check{H}^p(X, \mathscr{C})$ is bijective for $p = 0$ and injective for $p = 1$.*

Proof. By Lemma 21.4.2 the bijectivity for $p = 0$ is immediate. We now show that

$$\check{H}_0^1(X, \mathscr{C}) \to \check{H}^1(X, \mathscr{C})$$

is injective. Let $[z]$ be in the kernel of this map, which is represented by a 1-cocycle $z = (z_{i_0 i_1}) \in C_0^1(\mathcal{U}, \mathscr{C})$. Then since $[z] = 0$ in $\check{H}^1(X, \mathscr{C})$, there exists an $f = (f_i) \in C^0(\mathcal{U}, \mathscr{C})$ with $df = z$; applying Lemma 21.4.2 (and its notations) to f yields a covering $\mathcal{V}$ such that $\tau(f) \in C_0^0(\mathcal{V}, \mathscr{C})$, which shows that $\tau(z)$ is cohomologous to 0 in $C_0^1(\mathcal{V}, \mathscr{C})$, thus its image $[z]$ in $\check{H}_0^1(X, \mathscr{C})$ is 0. This shows the claim. □

Corollary 21.4.4. *With notations above, we have an exact sequence:*

$$0 \longrightarrow \Gamma(X, \mathscr{A}) \longrightarrow \Gamma(X, \mathscr{B}) \longrightarrow \Gamma(X, \mathscr{C}) \xrightarrow{\delta} \check{H}^1(X, \mathscr{A}) \longrightarrow \check{H}^1(X, \mathscr{B}) \longrightarrow \check{H}^1(X, \mathscr{C})$$

Corollary 21.4.5. *If $\check{H}^1(X, \mathscr{A}) = 0$, then $\Gamma(X, \mathscr{B}) \to \Gamma(X, \mathscr{C})$ is surjective.*

21.4.2 Paracompact space

Recall that a space X is said to be paracompact if any covering of X admits a locally finite refinement. On paracompact spaces, we can extend Theorem 21.4.3 for all values of p:

Theorem 21.4.6. *If X is paracompact, the canonical homomorphism*

$$\check{H}_0^p(X, \mathscr{C}) \to \check{H}^p(X, \mathscr{C})$$

is bijective for all $p \geq 0$.

This Proposition is an immediate consequence of the following lemma, analogous to Lemma 21.4.2:

Lemma 21.4.7. *Let X be a paracompact space. Let $\mathcal{U} = (U_i)_{i\in I}$ be a covering, and let $f = (f_{i_0\ldots i_p})$ be an element of $C^p(\mathcal{U}, \mathscr{C})$. Then there exists a covering $\mathcal{V} = (V_j)_{j\in J}$ and a mapping $\tau : J \to I$ such that $V_j \subseteq U_{\tau(j)}$ and $\tau(f) \in C_0^p(\mathcal{V}, \mathscr{C})$.*

Proof. Since X is paracompact, we might assume that $\mathcal{U}$ is locally finite. For every $x \in X$, we can choose an open neighborhood V_x of x such that

(a) If $x \in U_i$, then $V_x \subseteq U_i$.

(b) If $V_x \cap U_i \neq \varnothing$, then $V_x \subseteq U_i$.

(c) If $x \in U_{i_0\ldots i_p}$, there exists a section b of $\mathscr{B}$ over V_x such that $\beta(b) = f_{i_0\ldots i_p}|_{V_x}$.

The condition (c) can be satisfid due to the surjectivity of β and to the fact that x belongs to a finite number of sets $U_{i_0 \dots i_p}$. Having (c) satisfied, it suffices to restrict V_x to satisfy (a) and (b).

The family $(V_x)_{x \in X}$ forms a covering $\mathcal{V}$; for any $x \in X$, choose $\tau(x) \in I$ such that $x \in U_{\tau(x)}$. We now check that $\tau(f)$ belongs to $C_0^p(\mathcal{V}, \mathscr{C})$. If $V_{x_0 \dots x_p}$ is empty, this is obvious; if not, we have $V_{x_0} \cap U_{x_k} \neq \varnothing$ for $0 \leq k \leq p$, and then

$$V_{x_0} \cap U_{\tau(x_k)} \neq \varnothing \quad \text{for} \quad 0 \leq k \leq p,$$

which implies by (b) that $V_{x_0} \subseteq U_{\tau(x_k)}$ for all k, and hence $x_0 \in U_{\tau(x_0) \dots \tau(x_p)}$. We then apply (c) to get a section b of $\mathscr{B}$ over V_{x_0} such that $\beta(b) = f_{\tau(x_0) \dots \tau(x_p)}|_{V_{x_0}}$. Thus $\tau(f) \in C_0^p(\mathcal{V}, \mathscr{C})$, which completes the proof. □

Corollary 21.4.8. *If X is paracompact, we have an exact sequence:*

$$\cdots \longrightarrow \check{H}^p(X, \mathscr{A}) \xrightarrow{\alpha^*} \check{H}^p(X, \mathscr{B}) \xrightarrow{\beta^*} \check{H}^p(X, \mathscr{C}) \xrightarrow{\delta} \check{H}^{p+1}(X, \mathscr{A}) \longrightarrow \cdots$$

The exact sequence mentioned above is called the long exact sequence of cohomology defined by a given exact sequence of sheaves $0 \to \mathscr{A} \to \mathscr{B} \to \mathscr{C} \to 0$. More generally, it exists whenever we can show that $\check{H}_0^p(X, \mathscr{C}) \to \check{H}^p(X, \mathscr{C})$ is bijective.

21.5 Čech resolution and Leray Acyclic Theorem

We will now compare the Čech cohomology and derived functor cohomology of a sheaf $\mathscr{F}$ on a topological space X. We will see that in some cases we are able to conclude that these two cohomologies coincide. In order to compare Čech cohomology with derived functor cohomology, we will need to consider first a sheafified version of the Čech complex.

Fix a space X, an open cover $\mathcal{U} = (U_i)_{i \in I}$ and a sheaf $\mathscr{F}$ on X. For every open set U of X, let $j_U : U \hookrightarrow X$ denote the inclusion. Define a sheaf $\mathscr{C}^p(\mathcal{U}, \mathscr{F})$ by

$$\mathscr{C}^p(\mathcal{U}, \mathscr{F}) = \prod_{(i_0, \dots, i_p)} (j_{U_{i_0 \dots i_p}})_*(\mathscr{F}|_{U_{i_0 \dots i_p}}).$$

Explicitly, for an open subset $V \subseteq X$ we have

$$\Gamma(V, \mathscr{C}^p(\mathcal{U}, \mathscr{F})) = \prod_{(i_0, \dots, i_p)} \mathscr{F}(V \cap U_{i_0 \dots i_p}).$$

For each inclusion $\delta_j^p : U_{i_0 \dots i_p} \to U_{i_0 \dots \widehat{i_j} \dots i_p}$, we also have a restriction map

$$\mathscr{C}(\delta_j^p) : (j_{U_{i_0 \dots \widehat{i_j} \dots i_p}})_*(\mathscr{F}|_{U_{i_0 \dots \widehat{i_j} \dots i_p}}) \to (j_{U_{i_0 \dots i_p}})_*(\mathscr{F}|_{U_{i_0 \dots i_p}})$$

so we can define the differential $d : \mathscr{C}^p(\mathcal{U}, \mathscr{F}) \to \mathscr{C}^{p+1}(\mathcal{U}, \mathscr{F})$ by

$$d = \sum_{j=0}^{p+1} (-1)^j \mathscr{C}(\delta_j^{p+1}).$$

Thus we get complex $\mathscr{C}^\bullet(\mathcal{U},\mathscr{F})$. By definition, we have

$$\Gamma(X,\mathscr{C}^\bullet(\mathcal{U},\mathscr{F})) = C^\bullet(\mathcal{U},\mathscr{F})$$

Also, there is a product map $\epsilon : \mathscr{F} \to \mathscr{C}^0(\mathcal{U},\mathscr{F})$ defined by

$$\mathscr{F} \to \prod_i (j_{U_i})_*(j_{U_i})^{-1}\mathscr{F} = \prod_i (j_{U_i})_*(\mathscr{F}|_{U_i}).$$

Proposition 21.5.1. *For an open cover $\mathcal{U}$ and a sheaf $\mathscr{F}$, there is an exact sequence of sheaves*

$$0 \longrightarrow \mathscr{F} \xrightarrow{\epsilon} \mathscr{C}^0(\mathcal{U},\mathscr{F}) \longrightarrow \mathscr{C}^1(\mathcal{U},\mathscr{F}) \longrightarrow \mathscr{C}^2(\mathcal{U},\mathscr{F}) \longrightarrow \cdots$$

This is called the ***Čech resolution*** *of $\mathscr{F}$ with respect to the cover $\mathcal{U}$.*

Proof. The facts that ϵ is injective and that $\operatorname{im}\epsilon = \ker d^0$ follow directly from $\mathscr{F}$ being a sheaf.

It remains to be shown that the proposed sequence is exact in degrees $p > 0$. For this, it suffices to work at the level of stalks.

To prove the exactness at $\mathscr{C}^p(\mathcal{U},\mathscr{F})$, we need to check the sequence of stalks $\mathscr{C}^\bullet(\mathcal{U},\mathscr{F})$ is exact for all $x \in X$. Since $\mathcal{U}$ covers X, we can choose an open subset U_j containing x. Take $f_x \in \mathscr{C}^p(\mathcal{U},\mathscr{F})_x$ which is represented by (V,f), where V is a neighborhood of x and $f \in \Gamma(V,\mathscr{C}^p(\mathcal{U},\mathscr{F}))$. We may assume $V \subseteq U_j$. Then we observe that for any index $(i_0,\dots,i_{p-1}) \in I^p$ we have

$$V \cap U_{i_0\dots i_{p-1}} = V \cap U_{j,i_0\dots i_{p-1}}$$

Thus, we may define an element $\theta f \in \Gamma(V,\mathscr{C}^{p-1}(\mathcal{U},\mathscr{F}))$ by the formula

$$(\theta f)_{i_0\dots i_{p-1}} := f_{j,i_0\dots i_{p-1}}$$

This gives a map

$$\theta^p : \mathscr{C}^p(\mathcal{U},\mathscr{F})_x \to \mathscr{C}^{p-1}(\mathcal{U},\mathscr{F})_x, \quad f_x \mapsto (\theta f)_x$$

Now we check that

$$(\theta(df))_{i_0\dots i_p} = (df)_{j,i_0\dots i_p} = f_{i_0\dots i_p} - \sum_{k=0}^{p}(-1)^k(f_{j,i_0\dots\widehat{i_k}\dots i_p})|_{U_{i_0\dots i_p}}.$$

and

$$(d(\theta f))_{i_0\dots i_p} = \sum_{k=0}^{p}(-1)^k((\theta f)_{i_0\dots\widehat{i_k}\dots i_p})|_{U_{i_0\dots i_p}} = \sum_{k=0}^{p}(-1)^k(f_{j,i_0\dots\widehat{i_k}\dots i_p})|_{U_{i_0\dots i_p}}.$$

Therefore

$$\theta^{p+1}\big((df)_x\big) = (\theta(df))_x = \big(f - d(\theta f)\big)_x = f_x - d((\theta f)_x) = f_x - d(\theta^p f_x).$$

Hence θ^p is a homotopy from the identity of $\mathscr{C}^p(\mathcal{U},\mathscr{F})_x$ to the zero map, which shows the sequence of stalks is exact. □

One of the motivitions of defining the Čech resolution is the following proposition.

Proposition 21.5.2. *The Čech resolution computes the Čech cohomology. In the sense that the Čech*

cohomology groups can be derived from the Čech cohomology by appying the global section and taking cohomology.

Proof. Applying the global section on the complex $0 \to \mathscr{F} \to \mathscr{C}^\bullet(\mathscr{U}, \mathscr{F})$ gives the complex

$$0 \longrightarrow \mathscr{F}(X) \longrightarrow C^0(\mathscr{U}, \mathscr{F}) \longrightarrow C^1(\mathscr{U}, \mathscr{F}) \longrightarrow C^2(\mathscr{U}, \mathscr{F}) \longrightarrow \cdots$$

which is exactly the Čech complex. Thus its cohomology gives the Čech cohomology. □

Corollary 21.5.3. *With X, $\mathscr{U}$, $\mathscr{F}$ as above, there is a canonical map*

$$\check{H}^\bullet(\mathscr{U}, \mathscr{F}) \to H^\bullet(X, \mathscr{F}).$$

Proof. Let $0 \to \mathscr{F} \to \mathscr{I}^\bullet$ be an injective resolution of $\mathscr{F}$. Then since $0 \to \mathscr{F} \to \mathscr{C}^\bullet(\mathscr{U}, \mathscr{F})$ is also a resolution of $\mathscr{F}$, we have a canonical induced map $\mathscr{C}^\bullet(\mathscr{U}, \mathscr{F}) \to \mathscr{I}^\bullet$ induced by the identity of $\mathscr{F}$. The induced map on cohomology is what we want. □

We will now state some results stating sufficient conditions for these canonical morphisms to actually be isomorphisms, thus enabling us to calculate sheaf cohomology via Čech cohomology.

Proposition 21.5.4. *If $\mathscr{F}$ is a flasque sheaf on X, then $\check{H}^p(\mathscr{U}, \mathscr{F}) = 0$ for all open covers $\mathscr{U}$ of X and all $p > 0$.*

Proof. Let $\mathscr{C}^\bullet(\mathscr{U}, \mathscr{F})$ be the Čech resolution of $\mathscr{F}$ with respect to $\mathscr{U}$. Recall that $\mathscr{C}^p(\mathscr{U}, \mathscr{F})$ is defined for any open $V \subseteq X$ by

$$\Gamma(V, \mathscr{C}^p(\mathscr{U}, \mathscr{F})) = \prod \mathscr{F}(V \cap U_{i_0 \dots i_p}).$$

For each of these $U_{i_0 \dots i_p}$, the sheaf $V \mapsto \mathscr{F}(V \cap U_{i_0 \dots i_p})$ is flasque and since products of flasque sheaves are flasque, the entire sheaf $\mathscr{C}^p(\mathscr{U}, \mathscr{F})$ is flasque. Therefore $\mathscr{C}^p(\mathscr{U}, \mathscr{F})$ is acyclic by Proposition 20.2.6, so the Čech resolution can used to compute sheaf cohomology:

$$\check{H}^p(\mathscr{U}, \mathscr{F}) = H^p(X, \mathscr{F}) = 0$$

as desired. □

Corollary 21.5.5. *For any sheaf $\mathscr{F}$ on X, the map $\check{H}^1(X, \mathscr{F}) \to H^1(X, \mathscr{F})$ is an isomorphism.*

Proof. Let $\mathscr{G}$ be a flasque sheaf and $0 \to \mathscr{F} \to \mathscr{G} \to \mathscr{Q} \to 0$ be a short exact sequence of sheaves on X. Then $\check{H}^1(X, \mathscr{G}) = 0$, and by Corollary 21.4.4 there is an exact sequence

$$\begin{tikzcd}
0 \arrow[r] & \Gamma(X, \mathscr{F}) \arrow[r] \arrow[d, "1"] & \Gamma(X, \mathscr{G}) \arrow[r] \arrow[d, "1"] & \Gamma(X, \mathscr{Q}) \arrow[r] \arrow[d, "1"] & \check{H}^1(X, \mathscr{F}) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \Gamma(X, \mathscr{F}) \arrow[r] & \Gamma(X, \mathscr{G}) \arrow[r] & \Gamma(X, \mathscr{Q}) \arrow[r] & H^1(X, \mathscr{F}) \arrow[r] & 0
\end{tikzcd}$$

Thus the map $\check{H}^1(X, \mathscr{F}) \to H^1(X, \mathscr{F})$ is an isomorphism by the five lemma. □

Proposition 21.5.6. *Let X be a paracompact space, and $\mathscr{F}$ be a sheaf on X. Then the canonical maps*

$$\check{H}^p(X, \mathscr{F}) \to H^p(X, \mathscr{F})$$

are isomorphisms for $p \geq 0$.

Proof. This follows from Corollary 21.4.8 and an induction. □

Definition 21.5.7. *A sheaf $\mathscr{F}$ on X is* ***acyclic for an open cover*** $\mathscr{U} = (U_i)_{i \in I}$ *if for all $p > 0$ we have*

$$H^p(U_{i_0 \dots i_p}, \mathscr{F}|_{U_{i_0 \dots i_p}}) = 0.$$

Theorem 21.5.8 (Leray). *If $\mathscr{F}$ is a sheaf on X which is acyclic for an open cover $\mathscr{U}$, then the canonical maps*

$$\check{H}^p(\mathscr{U}, \mathscr{F}) \to H^p(X, \mathscr{F})$$

are isomorphisms for all $p \geq 0$.

Proof. We proceed by induction on the degree p. For $p = 0$ we already know that the result is true thanks to Proposition 21.1.5.

Now, assume $\check{H}^j(U, \mathscr{G}) \to H^j(X, \mathscr{G})$ is an isomorphism for all $j \leq p$ and all sheaves $\mathscr{G}$ acyclic for $\mathscr{U}$. Embed $\mathscr{F}$ in a flasque sheaf $\mathscr{G}$ and let $\mathscr{H}$ be the quotient, so that we have an exact sequence

$$0 \longrightarrow \mathscr{F} \longrightarrow \mathscr{G} \longrightarrow \mathscr{H} \longrightarrow 0$$

For each finite sequence $\sigma = (i_0, \dots, i_p)$, by hypothesis we have $H^i(U_\sigma, \mathscr{F}|_{U_\sigma}) = 0$ and $H^i(U_\sigma, \mathscr{G}|_{U_\sigma}) = 0$. Therefore $H^i(U_\sigma, \mathscr{H}|_{U_\sigma})$ is zero by the long exact sequence of $H^i(U_\sigma.-)$, and by taking the product over all such U_σ, we conclude that $\mathscr{H}$ is also acyclic for $\mathscr{U}$.

Now by the argument above, the sequence

$$0 \longrightarrow \mathscr{F}(U_\sigma) \longrightarrow \mathscr{G}(U_\sigma) \longrightarrow \mathscr{H}(U_\sigma) \longrightarrow 0$$

is exact. Hence by taking product the corresponding short sequence of Čech complexes

$$0 \longrightarrow \mathscr{C}^\bullet(\mathscr{U}, \mathscr{F}) \longrightarrow \mathscr{C}^\bullet(\mathscr{U}, \mathscr{G}) \longrightarrow \mathscr{C}^\bullet(\mathscr{U}, \mathscr{H}) \longrightarrow 0$$

is exact, so that we get a long exact sequence in Čech cohomology

$$\cdots \longrightarrow \check{H}^p(\mathscr{U}, \mathscr{F}) \longrightarrow \check{H}^p(\mathscr{U}, \mathscr{G}) \longrightarrow \check{H}^p(\mathscr{U}, \mathscr{H}) \longrightarrow \check{H}^{p+1}(\mathscr{U}, \mathscr{F}) \longrightarrow \cdots$$

Now since $\mathscr{G}$ is flasque, Proposition 21.5.4 shows that $\check{H}^p(\mathscr{U}, \mathscr{G}) = 0$. Therefore we have a diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & \check{H}^p(\mathscr{U}, \mathscr{H}) \arrow[r] \arrow[d] & \check{H}^{p+1}(\mathscr{U}, \mathscr{F}) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & H^p(\mathscr{U}, \mathscr{H}) \arrow[r] & H^{p+1}(\mathscr{U}, \mathscr{F}) \arrow[r] & 0
\end{tikzcd}$$

By induction, the left column is an isomorphism, so $\check{H}^{p+1}(X, \mathscr{F}) \to H^{p+1}(X, \mathscr{F})$ is also an isomorphism. □

21.6 Čech vs. Sheaf cohomology

Proposition 21.6.1. *Let X be a ringed space. Let*

$$0 \longrightarrow \mathcal{F} \longrightarrow \mathcal{G} \longrightarrow \mathcal{H} \longrightarrow 0$$

be a short exact sequence of $\mathcal{O}_X$-modules. Let $U \subseteq X$ be an open subset. If there exists a cofinal system of open coverings $\mathcal{U}$ of U such that $\check{H}^1(\mathcal{U}, \mathcal{F}) = 0$, then the map $\mathcal{G}(U) \to \mathcal{H}(U)$ is surjective.

Proof. Take an element $s \in \mathcal{H}(U)$. Choose an open covering $\mathcal{U} : U = (U_i)_{i \in I}$ such that

(a) $\check{H}^1(\mathcal{U}, \mathcal{F}) = 0$.

(b) $s|_{U_i}$ is the image of a section $s_i \in \mathcal{G}(U_i)$.

Since we can certainly find a covering such that (b) holds by the exactness of the sequence, it follows from the assumptions that we can find a covering such that (a) and (b) both hold. Consider the sections

$$s_{i_0 i_1} = s_{i_1}|_{U_{i_0 i_1}} - s_{i_0}|_{U_{i_0 i_1}}$$

Since s_i lifts s we see that $s_{i_0 i_1} \in \mathcal{F}(U_{i_0 i_1})$. By the vanishing of $\check{H}^1(\mathcal{U}, \mathcal{F})$ we can find sections $t_i \in \mathcal{F}(U_i)$ such that

$$s_{i_0 i_1} = t_{i_1}|_{U_{i_0 i_1}} - t_{i_0}|_{U_{i_0 i_1}}$$

Then clearly the sections $s_i - t_i$ satisfy the sheaf condition and glue to a section of $\mathcal{G}$ over U which maps to s. Hence we win. □

Proposition 21.6.2. *Let X be a ringed space. Let $\mathcal{F}$ be an $\mathcal{O}_X$-module such that*

$$\check{H}^p(\mathcal{U}, \mathcal{F}) = 0$$

for all $p > 0$ and any open covering $\mathcal{U} : U = \bigcup_{i \in I} U_i$ of an open subset U of X. Then $H^p(U, \mathcal{F}) = 0$ for all $p > 0$ and any open $U \subseteq X$.

Proof. Choose an embedding $\mathcal{F} \to \mathcal{I}$ into an injective $\mathcal{O}_X$-module. By Proposition 21.5.4 $\mathcal{I}$ has vanishing higher Čech cohomology for any open covering. Let $\mathcal{Q} = \mathcal{I}/\mathcal{F}$ so that we have a short exact sequence

$$0 \longrightarrow \mathcal{F} \longrightarrow \mathcal{I} \longrightarrow \mathcal{Q} \longrightarrow 0$$

By Proposition21.6.1 and our assumptions this sequence is actually exact as a sequence of presheaves! In particular we have a long exact sequence of Čech cohomology groups for any open covering $\mathcal{U}$, see Theorem 21.2.2 for example. This implies that $\mathcal{Q}$ is also an $\mathcal{O}_X$-module with vanishing higher Čech cohomology for all open coverings.

Next, we look at the long exact cohomology sequence

$$\cdots \longrightarrow H^p(U, \mathcal{F}) \longrightarrow H^p(U, \mathcal{I}) \longrightarrow H^p(U, \mathcal{Q}) \longrightarrow H^{p+1}(U, \mathcal{F}) \longrightarrow \cdots$$

for any open $U \subseteq X$. Since $\mathcal{I}$ is injective we have $H^p(U, \mathcal{I}) = 0$ for $p > 0$. By the above we see that $H^0(U, \mathcal{I}) \to H^0(U, \mathcal{Q})$ is surjective, thus $H^1(U, \mathcal{F}) = 0$. Also, $H^p(U, \mathcal{Q}) = H^{p+1}(U, \mathcal{F})$ for $p \geq 1$. Thus the claim follows by an induction. □

Proposition 21.6.3. *Let X be a ringed space. Let $\mathcal{B}$ be a basis for the topology on X. Let $\mathcal{F}$ be an $\mathcal{O}_X$-module. Assume there exists a set of open coverings* Cov *with the following properties:*

(i) For every $\mathcal{U} \in \text{Cov}$ with $\mathcal{U} : U = \bigcup_{i \in I} U_i$ we have $U, U_i \in \mathcal{B}$ and every $U_{i_0 \ldots i_p} \in \mathcal{B}$.

(ii) For every $U \in \mathcal{B}$ the open coverings of U occurring in Cov *is a cofinal system of open coverings of U.*

(iii) For every $\mathcal{U} \in \text{Cov}$ we have $\check{H}^p(\mathcal{U}, \mathcal{F}) = 0$ for all $p > 0$.

Then $H^p(U, \mathcal{F}) = 0$ for all $p > 0$ and any $U \in \mathcal{B}$.

Proof. Let $\mathcal{F}$ and Cov be as in the lemma. We will indicate this by saying $\mathcal{F}$ has vanishing higher Čech cohomology for any $\mathcal{U} \in \text{Cov}$. Choose an embedding $\mathcal{F} \hookrightarrow \mathcal{I}$ into an injective $\mathcal{O}_X$-module. By Proposition 21.5.4 has vanishing higher Čech cohomology for any $\mathcal{U} \in \text{Cov}$. Let $\mathcal{Q} = \mathcal{I}/\mathcal{F}$ so that we have a short exact sequence

$$0 \longrightarrow \mathcal{F} \longrightarrow \mathcal{I} \longrightarrow \mathcal{Q} \longrightarrow 0$$

By Proposition 21.6.1 and our assumption (ii) this sequence gives rise to an exact sequence

$$0 \longrightarrow \mathcal{F}(U) \longrightarrow \mathcal{I}(U) \longrightarrow \mathcal{Q}(U) \longrightarrow 0$$

for every $U \in \mathcal{B}$. Hence for any $\mathcal{U} \in \text{Cov}$ we get a short exact sequence of Čech complexes

$$0 \longrightarrow \mathcal{C}^\bullet(\mathcal{U}, \mathcal{F}) \longrightarrow \mathcal{C}^\bullet(\mathcal{U}, \mathcal{I}) \longrightarrow \mathcal{C}^\bullet(\mathcal{U}, \mathcal{Q}) \longrightarrow 0$$

since each term in the Čech complex is made up out of a product of values over elements of $\mathcal{B}$ by assumption (i). In particular we have a long exact sequence of Čech cohomology groups for any open covering $\mathcal{U} \in \text{Cov}$. This implies that $\mathcal{Q}$ is also an $\mathcal{O}_X$-module with vanishing higher Čech cohomology for all $\mathcal{U} \in \text{Cov}$.

Next, we look at the long exact cohomology sequence

$$\cdots \longrightarrow H^p(U, \mathcal{F}) \longrightarrow H^p(U, \mathcal{I}) \longrightarrow H^p(U, \mathcal{Q}) \longrightarrow H^{p+1}(U, \mathcal{F}) \longrightarrow \cdots$$

for any open $U \in \mathcal{B}$. Since $\mathcal{I}$ is injective we have $H^n(U, \mathcal{I}) = 0$ for $n > 0$. By the above we see that $H^0(U, \mathcal{I}) \to H^0(U, \mathcal{Q})$ is surjective and hence $H^1(U, \mathcal{F}) = 0$. Since $\mathcal{F}$ was an arbitrary $\mathcal{O}_X$-module with vanishing higher Čech cohomology for all $\mathcal{U} \in \text{Cov}$ we conclude that also $H^1(U, \mathcal{Q}) = 0$ since $\mathcal{Q}$ is another of these sheaves (see above). Also, $H^p(U, \mathcal{Q}) = H^{p+1}(U, \mathcal{F})$ for $p \geq 1$. Thus the claim follows by an induction. □

Proposition 21.6.4. *Let $f : X \to Y$ be a morphism of ringed spaces. Let $\mathcal{I}$ be an injective $\mathcal{O}_X$-module. Then*

- *$\check{H}^p(\mathcal{V}, f_*\mathcal{I}) = 0$ for all $p > 0$ and any open covering $\mathcal{V} = (V_j)_{j \in J}$ of Y.*
- *$H^p(V, f_*\mathcal{I}) = 0$ for all $p > 0$ and every open $V \subseteq Y$.*

In other words, $f_*\mathcal{I}$ is right acyclic for $\Gamma(U, -)$ for any $U \subseteq X$ open.

Proof. Set $\mathcal{U} = f^{-1}(\mathcal{V})$. It is an open covering of X and

$$C^\bullet(\mathcal{V}, f_*\mathcal{I}) = C^\bullet(\mathcal{U}, \mathcal{I}).$$

This is true because

$$f_*\mathcal{I}(V_{j_0\ldots j_p}) = \mathcal{I}(f^{-1}(V_{j_0\ldots j_p})) = \mathcal{I}\big(f^{-1}(V_{j_0}) \cap \cdots \cap f^{-1}(V_{j_p})\big) = \mathcal{I}(U_{j_0\ldots j_p}).$$

Thus the first statement of the lemma follows from Proposition 21.5.4. The second statement follows from the first and Proposition 21.6.2. □

Chapter 22

The language of schemes

22.1 Affine schemes

Let A be a ring. Recall that we have associate with A a topological space $\mathrm{Spec}(A)$, called the spectrum of A. In this section we shall make $\mathrm{Spec}(A)$ a locally ringed space and consider sheaf of modules over it; such spaces will be called **affine schemes**.

22.1.1 Sheaves associated with a module

Let A be a ring and M an A-module. For any element $f \in A$, let S_f be the multiplicative subset consisting of powers of f. Recall that the localization of M with respect to S_f is then denoted by M_f, and that of A by A_f. Let $\bar{S}_f$ be the saturation of S_f, which is defined to be the complement of the union of prime ideals of A that are disjoint from S_f, or equivalently not contains f. By Proposition 10.2.24, the set $\bar{S}_f$ is also characterized by

$$\bar{S}_f = \{x \in A : \text{there exist } n, m \geq 0 \text{ such that } f^n x = f^m\}.$$

Also, by Proposition 10.2.23, we have $\bar{S}_f A = A_f$ and $\bar{S}_f M = M_f$.

Lemma 22.1.1. *Let f, g be elements of A. Then the following conditions are equivalent:*

(i) $g \in \bar{S}_f$*, or equivalently* $\bar{S}_g \subseteq \bar{S}_f$*;*

(ii) $f \in \sqrt{(g)}$*, or equivalently* $\sqrt{(f)} \subseteq \sqrt{(g)}$*;*

(iii) $D(f) \subseteq D(g)$*, or equivalently* $V(g) \subseteq V(f)$*.*

Proof. We first note that $g \in \bar{S}_f$ is equivalent to $S_g \subseteq \bar{S}_f$, so the equivalence in (i). Also, the equivalence of (ii) and (iii) follows from Proposition 10.4.3. Finally, if $g \in \bar{S}_f$, then there exist $n, m \geq 0$ such that $f^n g = f^m$, which is an element of (g), and thus $f \in \sqrt{(g)}$. Conversely, if $D(f) \subseteq D(g)$, then by the discriptions $S_f = \bigcup_{f \notin \mathfrak{p}} \mathfrak{p}$ and $S_g = \bigcup_{g \notin \mathfrak{p}} \mathfrak{p}$, we conclude that $\bar{S}_g \subseteq \bar{S}_f$, whence the lemma. □

If $D(g) \subseteq D(f)$ in $\mathrm{Spec}(A)$, then by Lemma 22.1.1, we have $\bar{S}_f \subseteq \bar{S}_g$, so there is a canonical homomorphism $\rho_{g,f} : M_f \to M_g$; moreover, if $D(f) \supseteq D(g) \supseteq D(h)$, we then have

$$\rho_{h,g} \circ \rho_{g,f} = \rho_{h,f}.$$

As f runs through $A-\mathfrak{p}$ (where $\mathfrak{p}$ is a point in $X = \mathrm{Spec}(A)$), the set S_f then constitute a filtered set indexed by $A-\mathfrak{p}$, since any two element f, g of $A-\mathfrak{p}$ contains S_{fg}; as the union of the S_f for $f \in A-\mathfrak{p}$ is $A-\mathfrak{p}$, we conclude from Proposition 10.2.34 that the $A_\mathfrak{p}$-module $M_\mathfrak{p}$ is canonically identified with the direct limit $\varinjlim M_f$, relative to the family $(\rho_{g,f})$ of homomorphisms. For each $f \in A-\mathfrak{p}$, we denote the canonical homomorphism from M_f to $M_\mathfrak{p}$ by

$$\rho_\mathfrak{p}^f : M_f \to M_\mathfrak{p}.$$

We now define the **structural sheaf** of the prime spectrum $X = \mathrm{Spec}(A)$, denoted by $\widetilde{A}$, to be the sheaf of rings associated with the presheaf $D(f) \mapsto A_f$ over the basis $\mathcal{B}$ of X, formed by $D(f)$ with $f \in A$. Simialrly, for an A-module M,we define the **associated sheaf** $\widetilde{M}$ to be the sheaf associated presheaf $D(f) \mapsto M_f$ over the basis $\mathcal{B}$ of X. By the property of sheafification, it is clear that the stalk $\widetilde{A}_\mathfrak{p}$ (resp. $\widetilde{M}_\mathfrak{p}$) is identified with the ring $A_\mathfrak{p}$ (resp. with $A_\mathfrak{p}$-module $M_\mathfrak{p}$).

Theorem 22.1.2. *For each A-module M, the presheaf $D(f) \to M_f$ is a sheaf on the basis $\mathcal{B}$ of X, so for each $f \in A$ we have a canonical isomorphism*

$$M_f \to \Gamma(D(f), \widetilde{M}).$$

In particular, M is canonically identified with $\Gamma(X, \widetilde{M})$.

Proof. To show that the presheaf $D(f) \mapsto M_f$ is a sheaf on the basis $\mathcal{B}$ of X, we need to check the sheaf condition for the standard open coverings. If $D(f) = \bigcup_{i=1}^n D(g_i)$, then the sheaf condition for this covering is equivalent with the exactness of the sequence

$$0 \longrightarrow M_f \longrightarrow \bigoplus_i M_{g_i} \longrightarrow \bigoplus_{i,j} M_{g_i g_j}$$

Note that $D(g_i) = D(fg_i)$, and hence we can rewrite this sequence as the sequence

$$0 \longrightarrow M_f \longrightarrow \bigoplus_i M_{fg_i} \longrightarrow \bigoplus_{i,j} M_{fg_i g_j}$$

In addition, since $D(g_i)$'s cover $D(f)$ (which is identified with $\mathrm{Spec}(A_f)$), the elements $g_1, \ldots, g_n$ generate the unit ideal in A_f, so we may apply Corollary 10.4.48 to the module M_f over A_f and the elements $g_1, \ldots, g_n$ to conclude that the sequence is exact. □

Corollary 22.1.3. *Let M, N be A-modules. The canonical homomorphism*

$$\mathrm{Hom}_A(M, N) \to \mathrm{Hom}_{\widetilde{A}}(\widetilde{M}, \widetilde{N}), \quad \phi \mapsto \tilde{\phi}$$

is bijective. In particular, the relations $M = 0$ and $\widetilde{M} = 0$ are equivalent.

Proof. Consider the canonical homomorphism $\mathrm{Hom}_{\widetilde{A}}(\widetilde{M}, \widetilde{N}) \to \mathrm{Hom}_A(M, N)$, $\varphi \mapsto \Gamma(\varphi)$ (Theorem 22.1.2). It suffices to show that $\phi \mapsto \tilde{\phi}$ and $\varphi \mapsto \Gamma(\varphi)$ are inverses of each other. Now, it is evident that $\Gamma(\tilde{\phi}) = \phi$, by the definition of $\tilde{\phi}$. On the other hand, if we put $\phi = \Gamma(\varphi)$ for $\varphi \in \mathrm{Hom}_{\widetilde{A}}(\widetilde{M}, \widetilde{N})$, the map $\varphi_{D(f)} : \Gamma(D(f), \widetilde{M}) \to \Gamma(D(f), \widetilde{N})$ induced by φ is making the

following diagram commutes:

$$\begin{tikzcd} M \arrow[r, "\phi"] \arrow[d, "\rho_{f,1}"'] & N \arrow[d, "\rho_{f,1}"] \\ M_f \arrow[r, "\varphi_{D(f)}"] & N_f \end{tikzcd}$$

We then have necessarily $\varphi_{D(f)} = \phi_f$ for each $f \in A$, which shows $\widetilde{\Gamma(\varphi)} = \varphi$. □

Proposition 22.1.4. *For each $f \in A$, the open set $D(f) \subseteq X$ is canonically identified with the spectrum* $\operatorname{Spec}(A_f)$*, and the sheaf $\widetilde{M}_f$ associated with the A_f-module M_f is canonically identified with the restriction $\widetilde{M}_{D(f)}$.*

Proof. The first assertion is proved in Corollary 10.4.23. Now for $D(g) \subseteq D(f)$, then M_g is identified with the localization of M_f with respect to the canonical image of g in A_f, so the canonical identification of $\widetilde{M}_f$ and $\widetilde{M}_{D(f)}$ follows by definition. □

Proposition 22.1.5. *The functor $M \mapsto \widetilde{M}$ is an exact functor from the category of A-modules to the category of $\widetilde{A}$-modules.*

Proof. Let M, N be two A-modules and $\phi : M \to N$ a homomorphism; for any $f \in A$, we have a corresponding homomorphism $\phi_f : M_f \to N_f$, and for $D(g) \subseteq D(f)$ the diagram

$$\begin{tikzcd} M_f \arrow[r, "\phi_f"] \arrow[d, "\rho_{g,f}"'] & N_f \arrow[d, "\rho_{g,f}"] \\ M_g \arrow[r, "\phi_g"] & N_g \end{tikzcd}$$

is commutative. These then give a homomorphism of $\widetilde{A}$-modules $\tilde{\phi} : \widetilde{M} \to \widetilde{N}$. Moreover, for each $\mathfrak{p} \in X$, $\tilde{\phi}_x$ is the direct limit of ϕ_f for $f \in A - \mathfrak{p}$, and concequently identified with the canonical homomorphism $\phi_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$. If P is another A-module, $\psi : N \to P$ a homomorphism and $\eta = \psi \circ \phi$, then it is immediate that $\eta_{\mathfrak{p}} = \psi_{\mathfrak{p}} \circ \phi_{\mathfrak{p}}$, hence $\tilde{\eta} = \tilde{\psi} \circ \tilde{\phi}$. We thus get a covariant functor $\widetilde{(-)}$ from the category of A-modules to the category of $\widetilde{A}$-modules. This functor is exact since for each $\mathfrak{p} \in X$, $M \mapsto M_{\mathfrak{p}}$ is an exact functor; furthermore, we have $\operatorname{supp}(M) = \operatorname{supp}(\widetilde{M})$ by the definitions of these two members. □

Corollary 22.1.6. *Let M and N be two A-modules.*

(a) If $\phi : M \to N$ is a homomorphism, then the sheaves associated with $\ker \phi$, $\operatorname{im} \phi$, *and* $\operatorname{coker} \phi$ *are* $\ker \tilde{\phi}$, $\operatorname{im} \tilde{\phi}$, *and* $\operatorname{coker} \tilde{\phi}$, *respectively. In particular, $\tilde{\phi}$ is injective (resp. surjective, bijective) if and only if ϕ is injective (resp. surjective, bijective).*

(b) If M is a filtered limit (resp. direct sum) of a family $(M_i)_{i \in I}$ of A-modules, then $\widetilde{M}$ is a filtered limit (resp. direct sum) of the family $(\widetilde{M}_i)$.

Proof. For (a), it suffices to apply the exact functor $M \mapsto \widetilde{M}$ to the following exact sequences:

$$0 \longrightarrow \ker \phi \longrightarrow M \longrightarrow \operatorname{im} \phi \longrightarrow 0$$

$$0 \longrightarrow \operatorname{im} \phi \longrightarrow N \longrightarrow \operatorname{coker} \phi \longrightarrow 0$$

Now let (M_i, ρ_{ji}) be a filtered system of A-modules, with limit M, and let $\rho_i : M_i \to M$ be the canonical homomorphism. Since we have $\tilde{\rho}_{kj} \circ \tilde{\rho}_{ji} = \tilde{\rho}_{ji}$ and $\tilde{\rho}_i = \tilde{\rho}_j \circ \tilde{\rho}_{ji}$ for $i \leq j \leq k$, we see $(\widetilde{M}, \tilde{\rho}_{ji})$ is a direct system of sheaves over X, and if we denote by $\eta_i : \widetilde{M}_i \to \varinjlim \widetilde{M}_i$ the canonical homomorphism, a unique homomorphism $\psi : \varinjlim \widetilde{M}_i \to \widetilde{M}$ such that $\psi \circ \eta_i = \tilde{\rho}_i$. For this ψ to be bijective, it suffices that for each $\mathfrak{p} \in X$, $\psi_{\mathfrak{p}}$ is a bijection from $(\varinjlim \widetilde{M}_i)_{\mathfrak{p}}$ to $\widetilde{M}_{\mathfrak{p}}$; but $\widetilde{M}_{\mathfrak{p}} = M_{\mathfrak{p}}$ and

$$(\varinjlim \widetilde{M}_i)_{\mathfrak{p}} = \varinjlim (\widetilde{M}_i)_{\mathfrak{p}} = \varinjlim (M_i)_{\mathfrak{p}} = M_{\mathfrak{p}}$$

Also, it follows by definition that $(\tilde{\rho}_i)_{\mathfrak{p}}$ and $(\eta_i)_{\mathfrak{p}}$ are equal to the canonical homomorphism from $(M_i)_{\mathfrak{p}}$ to $M_{\mathfrak{p}}$; since $(\tilde{\rho}_i)_{\mathfrak{p}} = \psi_{\mathfrak{p}} \circ (\eta_i)_{\mathfrak{p}}$, $\psi_{\mathfrak{p}}$ is therefore the identity.

Finally, if M is a direct sum of two modules N and P, it is immediate that $\widetilde{M} = \widetilde{M} \oplus \widetilde{P}$; by taking filtered limits, we then generalize this result for the direct sum of an arbitrary family. This completes the proof. □

Remark 22.1.1. By Proposition 22.1.5, we conclude that the sheaves which are isomorphic to the sheaves associated with A-modules form an abelian category. Note also that it follows from Corollary 22.1.6 that if M is a finitely generated A-module, that is, if there exists a surjective homomorphism $A^n \to M$, then there exists a homomorphism surjective $\widetilde{A}^n \to \widetilde{M}$, in other words, the $\widetilde{A}$-module $\widetilde{M}$ is generated by a finite family of sections over X, and vice versa.

Corollary 22.1.7. *Let N and P be submodules of M. The sheaves $\widetilde{N}$ and $\widetilde{P}$ can be identified with sub-$\widetilde{A}$-modules of $\widetilde{M}$, and we have*

$$\widetilde{N + P} = \widetilde{N} + \widetilde{P}, \quad \widetilde{N \cap P} = \widetilde{N} \cap \widetilde{P}.$$

In particular, if $\widetilde{N} = \widetilde{P}$, then $N = P$.

Proof. If N is a submodule of an A-module M, the canonical injection $N \to M$ induced an injective homomorphism $\widetilde{N} \to \widetilde{M}$, hence identifies $\widetilde{N}$ with a sub-$\widetilde{A}$-module of $\widetilde{M}$. Now note that $N + P$ is the image of the canonical homomorphism $\alpha : N \oplus P \to M$, so by Corollary 22.1.6 we have

$$\widetilde{N + P} = \widetilde{\operatorname{im} \alpha} = \operatorname{im} \tilde{\alpha} = \widetilde{N} + \widetilde{P}$$

since $\tilde{\alpha}$ is equal to the canonical homomorphism $\widetilde{N} \oplus \widetilde{P} \to \widetilde{M}$. Similarly, since $N \cap P$ is the kenrel of the canonical homomorphism $M \to (M/N) \oplus (M/P)$, we also have $\widetilde{N \cap P} = \widetilde{N} \cap \widetilde{P}$. □

Corollary 22.1.8. *Over the category of sheaves isomorphic to sheaves associated with A-modules, the global section functor Γ is exact.*

Proof. In fact, let $\widetilde{M} \xrightarrow{\tilde{\phi}} \tilde{N} \xrightarrow{\tilde{\psi}} P$ be an exact sequence corresponding to two homomorphisms $\phi : M \to N$ and $\psi : N \to P$. If $Q = \operatorname{im} \phi$ and $R = \ker \psi$, we have

$$\widetilde{Q} = \operatorname{im} \tilde{\phi} = \ker \tilde{\psi} = \widetilde{R}$$

by Corollary 22.1.6, so $Q = R$ and the sequence is exact. □

Corollary 22.1.9. *Let M and N be two A-modules.*

(a) The sheaf associated with $M \otimes_A N$ is canonically identified with $\widetilde{M} \otimes_{\widetilde{A}} \widetilde{N}$.

(b) *If moreover M is finitely presented, the sheaf associated with* $\mathrm{Hom}_A(M,N)$ *is canonically identified with* $\widetilde{\mathscr{H}om}_{\widetilde{A}}(\widetilde{M},\widetilde{N})$.

Proof. The sheaf $\mathscr{F} = \widetilde{M} \otimes_{\widetilde{A}} \widetilde{N}$ is the sheafification of the presheaf

$$U \mapsto \mathscr{F}(U) = \Gamma(U,\widetilde{M}) \otimes_{\Gamma(U,\widetilde{A})} \Gamma(U,\widetilde{N})$$

where U runs through the basis $\mathscr{B}$ of X formed by $D(f)$, $f \in A$. Now, $\mathscr{F}(D(f))$ is canonically identified with $M_f \otimes_{A_f} N_f$ by Theorem 22.1.2, which is isomorphic to $\Gamma(D(f), \widetilde{M \otimes_A N})$. Moreover, it is immediately verified that the canonical isomorphisms

$$\mathscr{F}(D(f)) \cong \Gamma(D(f), \widetilde{M \otimes_A N})$$

is compatible with the restriction maps, so they define a canonical isomorphism $\widetilde{M} \otimes_{\widetilde{A}} \widetilde{N} \cong \widetilde{M \otimes_A N}$.

Now assume that M is finitely presented. The sheaf $\mathscr{G} = \widetilde{\mathscr{H}om}_{\widetilde{A}}(\widetilde{M},\widetilde{N})$ is the sheafification of the presheaf

$$U \mapsto \mathscr{G}(U) = \mathrm{Hom}_{\widetilde{A}|_U}(\widetilde{M}|_U, \widetilde{N}|_U)$$

where U runs through the basis $\mathscr{B}$ of X. By Proposition 22.1.4 and Corollary 22.1.3, the module $\mathscr{G}(D(f))$ is then identified with $\mathrm{Hom}_{A_f}(M_f, N_f)$, which is isomorphic to $\Gamma(D(f), \widetilde{\mathrm{Hom}_A(M,N)})$ by Proposition 10.2.46. It is clear that these isomorphisms are compatible with the restriction maps, so we conclude that $\widetilde{\mathscr{H}om}_{\widetilde{A}}(\widetilde{M},\widetilde{N}) \cong \widetilde{\mathrm{Hom}_A(M,N)}$. □

Now consider an A-algebra B (commutative); this can be interpreted by saying that B is an A-module and that we are given an element $e \in B$ and an A-homomorphism $\varphi : B \otimes_A B \to B$ so that the diagrams

$$\begin{tikzcd} B \otimes_A B \otimes_A B \arrow[r, "\varphi\otimes 1"] \arrow[d, "1\otimes\varphi"'] & B \otimes_A B \arrow[d, "\varphi"] \\ B \otimes_A B \arrow[r, "\varphi"] & B \end{tikzcd} \qquad \begin{tikzcd} B \otimes_A B \arrow[rr, "\sigma"] \arrow[dr, "\varphi"'] & & B \otimes_A B \arrow[dl, "\varphi"] \\ & B & \end{tikzcd}$$

(where σ is the canonical symmetry) commute, and that $\varphi(e \otimes x) = \varphi(x \otimes e) = x$. In view of Corollary 22.1.9, the homomorphism $\tilde{\varphi} : \widetilde{B} \otimes_{\widetilde{A}} \widetilde{B} \to \widetilde{B}$ of $\widetilde{A}$-modules satisfies similar conditions, hence defines a $\widetilde{A}$**-algebra** structure on $\widetilde{B}$. In the same way, the data of a B-module N amounts to giving an A-module N and an A-homomorphism $\psi : B \otimes_A N \to N$ such that the diagram

$$\begin{tikzcd} B \otimes_A B \otimes_A N \arrow[r, "\varphi\otimes 1"] \arrow[d, "1\otimes\psi"'] & B \otimes_A N \arrow[d, "\psi"] \\ B \otimes_A N \arrow[r, "\psi"] & N \end{tikzcd}$$

commutes and $\psi(e \otimes n) = n$; the homomorphism $\tilde{\psi} : \widetilde{B} \otimes_{\widetilde{A}} \widetilde{N} \to \widetilde{N}$ then satisfies similar conditions, and defines on $\widetilde{N}$ a $\widetilde{B}$-module structure.

If $\rho : B \to B'$ (resp. $\phi : N \to N'$) is a homomorphism of A-algebras (resp. a homomorphisms of B-modules), then $\tilde{\rho}$ (resp. $\tilde{\phi}$) is a homomorphism of $\widetilde{A}$-algebras (resp. a homomorphisms of $\widetilde{B}$-modules), $\ker \tilde{\rho}$ is an ideal of $\widetilde{B}$ (resp. $\ker \tilde{\phi}$, $\operatorname{coker} \tilde{\phi}$, and $\operatorname{im} \tilde{\phi}$ are $\widetilde{B}$-modules).

Moreover, by Proposition 10.4.51(b) if N is a B-module, then $\widetilde{N}$ is a finitely generated $\widetilde{B}$-module if and only if N is finitely generated over B.

If M and N are two B-modules, the $\widetilde{B}$-module $\widetilde{M} \otimes_{\widetilde{B}} \widetilde{N}$ is canonically identified with $\widetilde{M \otimes_B N}$; similarly, $\mathscr{H}om_{\widetilde{B}}(\widetilde{M}, \widetilde{N})$ is canonically identified with $\widetilde{\mathrm{Hom}_B(M, N)}$ if M is finitely presented. If $\mathfrak{b}$ is an ideal of B, then $\widetilde{\mathfrak{b}N} = \widetilde{\mathfrak{b}}\widetilde{N}$.

Finally, if B is a graded A-algebra with (B_n) its graduation, the $\widetilde{A}$-algebra $\widetilde{B}$ is then the direct sum of the sub-$\widetilde{A}$-modules $\widetilde{B}_n$ (Corollary 22.1.6), so $(\widetilde{B}_n)$ is a graduation of $\widetilde{B}$. Similarly, if M is a graded B-module with graduation (M_n), then $\widetilde{M}$ is a graded $\widetilde{B}$-module with graduation $(\widetilde{M}_n)$.

22.1.2 Functorial properties of the associated sheaf

We now consider the functorial properties of the operation $M \mapsto \widetilde{M}$. Let A and B be rings and $\varphi : B \to A$ be a ring homomorphism. Then we have an associated map

$$^a\varphi : X = \mathrm{Spec}(A) \to Y = \mathrm{Spec}(B)$$

We will define a canonical homomorphism

$$\varphi^\# : \mathscr{O}_Y \to {}^a\varphi_*(\mathscr{O}_X)$$

of sheaf of rings. For any $g \in B$, we set $f = \varphi(g)$; we have $\varphi^{-1}(D(g)) = D(f)$ by Proposition 10.4.18. Now the sections $\Gamma(D(g), \widetilde{B})$ and $\Gamma(D(f), \widetilde{A})$ are canonically identified with B_g and A_f, respectively, and we have an induced map $\varphi_g : B_g \to A_f$, which then gives a homomorphism of rings

$$\Gamma(D(g), \widetilde{B}) \to \Gamma(\varphi^{-1}(D(g)), \widetilde{A}) = \Gamma(D(g), {}^a\varphi_*(\widetilde{A})).$$

Moreover, these homomorphisms satisfy the following compatible conditions: for $D(g) \supseteq D(g')$ in Y, the diagram

$$\begin{array}{ccc} \Gamma(D(g), \widetilde{A}) & \longrightarrow & \Gamma(D(g), {}^a\varphi_*(\widetilde{A})) \\ \downarrow & & \downarrow \\ \Gamma(D(g'), \widetilde{A}) & \longrightarrow & \Gamma(D(g'), {}^a\varphi_*(\widetilde{A})) \end{array}$$

is commutative; we then get a morphism of $\mathscr{O}_Y$-algebras, since $D(g)$ form a basis for the topological space Y. The couple $({}^a\varphi, \varphi^\#)$ is called the **canonical morphism** of the locally ringed spaces induced by φ.

We also note that, if $y = {}^a\varphi(x)$, the homomorphism $\varphi^\#_x$ is no other that the homomorphism

$$\varphi_x : B_y \to A_x$$

induced by the homomorphism $\varphi : B \to A$. In fact, for $b/g \in B_y$, where $b, g \in B$ and $g \notin \mathfrak{p}_y$, $D(g)$ is then an open neighborhood of y in Y, and the homomorphism

$$\Gamma(D(g), \widetilde{B}) \to \Gamma(D(g), ({}^a\varphi)_*(\widetilde{A}))$$

induced by $\varphi^\#$ is just φ_g; by considering the section $\xi \in \Gamma(D(g), \widetilde{B})$ corresponding to b/g, we

then obtain that $\varphi_x^\#(\xi) = \varphi(b)/\varphi(g)$ in A_x.

Example 22.1.10. Let S be a miltiplicative subset of A and $\varphi : A \to S^{-1}A$ the canonical homomorphism. We have seen in Proposition 10.4.22 that ${}^a\varphi$ is a homeomorphism from $Y = \mathrm{Spec}(S^{-1}A)$ to the subspace $X = \mathrm{Spec}(A)$ formed by x such that $\mathfrak{p}_x \cap S = \varnothing$. Moreover, for any x in this subspace, hence of the form ${}^a\varphi(y)$ where $y \in Y$, the homomorphism $\varphi_y^\# : \mathcal{O}_{Y,y} \to \mathcal{O}_{X,x}$ is bijective; therefore, $\mathcal{O}_Y$ is identified with the sheaf induced over Y by $\mathcal{O}_X$.

Proposition 22.1.11. *Let $\varphi : B \to A$ be a ring homomorphism and $\Phi : X \to Y$ the associated morphism. For any A-module M, there exists a canonical functorial isomorphism of the $\mathcal{O}_Y$-module $\widetilde{\varphi^*(M)}$ to its direct image $\Phi_*(\widetilde{M})$.*

Proof. For $g \in B$, put $f = \varphi(g)$; the modules $\Gamma(D(g), \widetilde{\varphi^*(M)})$ and $\Gamma(D(f), \widetilde{M})$ are identified with $(\varphi^*(M))_g$ and M_f, respectively; moreover, the B_g-module $\varphi_g^*(M_f)$ is canonically isomorphic to $(\varphi^*(M))_g$. We then have a functorial isomorphism of $\Gamma(D(g), \widetilde{B})$-modules:

$$\Gamma(D(g), \widetilde{\varphi^*(M)}) \cong \varphi^*(\Gamma(D(\varphi(g)), \widetilde{M}))$$

and this isomorphism satisfies the compatible conditions with restrictions, hence define an isomorphism of sheaves. □

This proof also proves that for any A-algebra R, the canonical functorial isomorphism $\widetilde{\varphi^*(R)} \to \Phi_*(\widetilde{R})$ is an isomorphism of $\mathcal{O}_Y$-algebras. If M is an R-module, the canonical isomorphism $\widetilde{\varphi^*(M)} \cong \Phi_*(\widetilde{M})$ is an isomorphism of $\Phi_*(\widetilde{R})$-modules.

Corollary 22.1.12. *The direct image functor Φ_* is exact on the category of quasi-coherent sheaves.*

Proof. Recall that the functor φ^* is exact and $M \mapsto \widetilde{M}$ is an exact functor. □

Proposition 22.1.13. *Let $\varphi : B \to A$ be a ring homomorphism and $\Phi : X \to Y$ the associated morphism. Let N be a B-module and $\varphi_*(N)$ the A-module $N \otimes_B A$. Then there exist a canonical functorial isomorphism of the $\mathcal{O}_X$-module $\Phi^*(\widetilde{N})$ to $\widetilde{\varphi_*(N)}$.*

Proof. We first remark that $j : z \mapsto z \otimes 1$ is a B-homomorphism from N to $\varphi^*\varphi_*(N)$: this holds because for $g \in B$, we have

$$(gz) \otimes 1 = z \otimes \varphi(g) = \varphi(g)(z \otimes 1).$$

By Corollary 22.1.3, this corresponds to a homomorphism $\tilde{j} : \widetilde{N} \to \widetilde{\varphi^*(\varphi_*(N))}$ of $\mathcal{O}_Y$-modules, and via Proposition 22.1.11 we can think that $\tilde{j}$ maps $\widetilde{N}$ to $\Phi_*(\widetilde{\varphi_*(N)})$. From the adjointness of Φ^* and Φ_*, this canonically corresponds to a homomorphism

$$\theta : \Phi^*(\widetilde{N}) \to \widetilde{\varphi_*(N)}.$$

It then remains to show that θ is bijective, or equivalently that θ_x is bijective for every $x \in X$. For this, put $y = {}^a\varphi(x)$, choose $g \in B$ such that $y \in D(g)$, and let $f = \varphi(g)$. Then the ring $\Gamma(D(f), \widetilde{A})$ is identified with A_f, the module $\Gamma(D(f), \widetilde{\varphi_*(N)})$ is identified with $(\varphi_*(N))_f$, and $\Gamma(D(g), \widetilde{N})$ is identified with N_g. Let $s = n/g^p$ ($n \in N$) be a section of $\Gamma(D(g), \widetilde{N})$ and $t = a/f^q$ ($a \in A$) a section of $\Gamma(D(f), \widetilde{A})$. Then, since s is send to $(n \otimes 1)/f^p$ be $\tilde{j}$, by definition we have

$$\theta_x(s_x \otimes t_x) = t_x \cdot s_x.$$

Recall that we can identify $(\varphi_*(N))_f$ with $N_f \otimes_{B_g} \varphi^*(A_f)$, under which n/g^p is identified with $(n/g^p) \otimes 1$. So it is immediately seen that θ_x is none other than the canonical isomorphism

$$N_y \otimes_{B_y} \varphi_y^*(A_x) \cong (\varphi_*(N))_x = (N \otimes_B \varphi^*(A))_x.$$

Finally, let $v : N_1 \to N_2$ be a homomorphism of B-modules; since $\tilde{v}_y = v_y$ for any $y \in Y$, it follows immediately from the preceding argument that $\Phi^*(\tilde{v})$ is canonically identified to $\widetilde{v \otimes 1}$, which completes the proof. □

If S is an B-algebra, the canonical isomorphism of $\Phi^*(\widetilde{S})$ to $\widetilde{\varphi_*(S)}$ is an isomorphism of $\mathscr{O}_X$-algebras; if moreover N is a S-module, the canonical isomorphism of $\Phi^*(\widetilde{N})$ to $\widetilde{\varphi_*(N)}$ is an isomorphism of $\Phi^*(\widetilde{S})$-algebras.

Corollary 22.1.14. *The sections of $\Phi^*(\widetilde{N})$ which are cannical images of section of the B-module $\Gamma(\widetilde{N})$, generate the A-module $\Gamma(\Phi^*(\widetilde{N}))$.*

Proof. In fact, these images are identified with the elements $z \otimes 1$ of $\varphi_*(N)$, if we identify N and $\varphi_*(N)$ with $\Gamma(\widetilde{N})$ and $\Gamma(\widetilde{\varphi_*(N)})$. □

By the proof of Proposition 22.1.13, we see that the canonical map $\alpha : \widetilde{N} \to \Phi_*\Phi^*(\widetilde{N})$ is none other than the homomorphism $\tilde{j}$, where $j : N \to \varphi_*(N)$ is the canonical map $z \mapsto z \otimes 1$. Similarly, the canonical map $\beta : \Phi^*\Phi_*(\widetilde{M}) \to \widetilde{M}$ is none other than the homomorphism $\tilde{p}$, where $p : \varphi^*(M) \otimes_B \varphi^*(A) \to M$ is the canonical homomorphism that sends $m \otimes a$ to am.

Corollary 22.1.15. *Let N_1 and N_2 be B-modules and assume that N_1 is finitely presented. Then there is a canonical homomorphism*

$$\Phi^*(\mathscr{H}om_{\widetilde{B}}(\widetilde{N}_1, \widetilde{N}_2)) \to \mathscr{H}om_{\widetilde{A}}(\Phi^*(\widetilde{N}_1), \Phi^*(\widetilde{N}_2)).$$

This homomorphism is bijective if φ is a flat homomorphism.

Proof. By the above remarks and Corollary 22.1.9, this homomorphism is induced by the homomorphism

$$\mathrm{Hom}_B(N_1, N_2) \otimes_B A \to \mathrm{Hom}_A(N_1 \otimes_B A, N_2 \otimes_B A).$$

The last assertion follows from Proposition 7.2.29. □

A locally ringed space $(X, \mathscr{O}_X)$ is called an **affine scheme** if it is isomorphic to the spectrum of a ring A. In this case, the ring $\Gamma(X, \mathscr{O}_X)$ is canonically identified with A. By absuing language, we often call $\mathrm{Spec}(A)$ an affine scheme, without mention the structural sheaf.

Let A and B be two rings and $(X, \mathscr{O}_X)$, $(Y, \mathscr{O}_Y)$ the corresponding affine schemes. Then any ring homomorphism $\varphi : B \to A$ corresponds to a morphism $({}^a\varphi, \varphi^\#) : (X, \mathscr{O}_X) \to (Y, \mathscr{O}_Y)$. Note that the homomorphism φ is completely determined by $({}^a\varphi, \varphi^\#)$, since by definition we have $\varphi = \Gamma(\varphi^\#) : \Gamma(\widetilde{B}) \to \Gamma(\widetilde{A})$.

Theorem 22.1.16. *Let $(X, \mathscr{O}_X)$ and $(Y, \mathscr{O}_Y)$ be two affine schemes. Then any morphism $(\psi, \psi^\#) : (X, \mathscr{O}_X) \to (Y, \mathscr{O}_Y)$ of locally ringed spaces is of the form $({}^a\varphi, \varphi^\#)$, where $\varphi : \Gamma(Y, \mathscr{O}_Y) \to \Gamma(X, \mathscr{O}_X)$ is a ring homomorphism.*

Proof. Put $A = \Gamma(X, \mathcal{O}_X)$ and $B = \Gamma(Y, \mathcal{O}_Y)$. Let $(\psi, \psi^\#) : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ be a morphism of locally ringed spaces. By definition, $\psi^\#$ is a homomorphism from $\mathcal{O}_Y$ to $\psi_*\mathcal{O}_X$, and we then deduce a canonical homomorphism of rings

$$\varphi = \Gamma(\psi^\#) : B = \Gamma(Y, \mathcal{O}_Y) \to \Gamma(Y, \psi_*\mathcal{O}_X) = \Gamma(X, \mathcal{O}_X) = A.$$

Since $\psi^\#_x$ is a local homomorphism, by passing to quotients we deduce a monomorphism θ^x from the residue field $\kappa(\psi(x))$ into the residue field $\kappa(x)$ such that, for any section $f \in \Gamma(Y, \mathcal{O}_Y)$, we have $\theta^x(f(\psi(x))) = \varphi(f)(x)$ (we consider the elements of $\Gamma(Y, \mathcal{O}_Y)$ as functions on B). The relationship $f(\psi(x)) = 0$ is therefore equivalent to $\varphi(f)(x) = 0$, which means $\psi(x) = {}^a\varphi(x)$. Since this hold for any $x \in X$, we conclude that $\psi = {}^a\varphi$. We also know that the diagram

$$\begin{tikzcd} B = \Gamma(Y, \mathcal{O}_Y) \arrow[r, "{}^a\varphi"] \arrow[d] & \Gamma(X, \mathcal{O}_X) = A \arrow[d] \\ B_{\psi(x)} \arrow[r, "\psi^\#_x"] & A_x \end{tikzcd}$$

is commutative, so $\psi^\#_x$ is equal to the homomorphism $\varphi_x : B_{\psi(x)} \to A_x$ induced from φ. Since the morphism $\psi^\#$ is determined by $\psi^\#_x$, we obtain that $\psi^\# = \varphi^\#$. □

Corollary 22.1.17. *Let $(X, \mathcal{O}_X)$ and $(Y, \mathcal{O}_Y)$ be two affine schemes. Then there is a canonical bijection*

$$\mathrm{Mor}(X, Y) \to \mathrm{Hom}_{\mathbf{Ring}}(\Gamma(Y, \mathcal{O}_Y), \Gamma(X, \mathcal{O}_X))$$

which sends a morphism $(f, f^\#)$ to the global section of $f^\#$.

We can also say that the functors $(\mathrm{Spec}(A), \widetilde{A})$ in A and $\Gamma(X, \mathcal{O}_X)$ in $(X, \mathcal{O}_X)$ define an equivalence of the opposite category of commutative rings and of the category of the category of affine schemes.

Corollary 22.1.18. *If $\varphi : B \to A$ is surjective, then the corresponding morphism Φ is a monomorphism of locally ringed spaces.*

Proof. The map ${}^a\varphi$ is injective by Proposition 10.4.20, and since φ is surjective, for any $x \in x$ the map $\varphi^\#_x : B_{{}^a\varphi(x)} \to A_x$, obtained by passing to localization, is surjective; these prove the assertion. □

22.1.3 Quasi-coherent sheaves over affine schemes

Recall that we have defined the abstract notion of a quasi-coherent sheaf. In this part we show that any quasi-coherent sheaf on an affine scheme $\mathrm{Spec}(A)$ corresponds to the sheaf $\widetilde{M}$ associated with an A-module M.

Lemma 22.1.19. *Let $X = \mathrm{Spec}(A)$ and $V = \bigcup_{i=1}^n D(g_i)$ be a union of finitely may standard opens. Let $\mathcal{F}$ be an $\mathcal{O}_X$-module satisfying the conditions:*

(a) For any $D(f) \subseteq D(g_i)$ (resp. $D(g_ig_j)$) and any section $s \in \Gamma(D(f), \mathcal{F})$, there exists $n \geq 0$ such that $f^n s$ can be extended to a section of $\mathcal{F}$ on $D(g_i)$ (resp. on $D(g_ig_j)$).

(b) For any $D(f) \subseteq D(g_i)$ (resp. $D(g_ig_j)$) and any section $t \in \Gamma(V, \mathcal{F})$ such that $t|_{D(f)} = 0$, there exists $n \geq 0$ such that $f^n t = 0$.

Then we have the stronger conditions:

(α) *For any $f \in A$ and any section $s \in \Gamma(D(f) \cap V, \mathscr{F})$, there exists $n \geq 0$ such that $f^n s$ can be extended to a section of $\mathscr{F}$ on V.*

(β) *For any $f \in A$ and any section $t \in \Gamma(V, \mathscr{F})$ such that $t|_{D(f)\cap V} = 0$, there exists $n \geq 0$ such that $f^n t = 0$.*

Proof. First we prove condition (β). Since $D(f) \cap D(g_i) = D(fg_i)$, for each i we have an integer $n_i \geq 0$ such that $(fg_i)^{n_i} t$ restricts to zero on $D(g_i)$. Since g_i is invertible in $A_{g_i} = \Gamma(D(g_i), \mathscr{O}_X)$, this implies $f^{n_i} t = 0$ on $D(g_i)$. Take n such that $n \geq n_i$, then $f^n t = 0$ on each $D(g_i)$, whence $f^n t = 0$ and we get (β).

To show (α), we apply (a) on $\mathscr{F}|_{D(g_i)}$ to get an integer integers $n_i \geq 0$ and $s_i' \in \Gamma(D(g_i), \mathscr{F})$ such that

$$s_i'|_{D(fg_i)} = (fg_i)^{n_i} s|_{D(fg_i)}.$$

By inverting g_i, this produces sections $s_i \in \Gamma(D(g_i), \mathscr{F})$ such that

$$s_i|_{D(fg_i)} = f^{n_i} s|_{D(fg_i)}.$$

We may assume that all n_i take the same value n. Then each $s_i - s_j$ restricts to zero on $D(f) \cap D(g_i) \cap D(g_j) = D(fg_ig_j)$, so by applying (b) on $\mathscr{F}|_{D(g_ig_j)}$ we get an integer m_{ij} such that

$$(fg_ig_j)^{m_{ij}}(s_i - s_j)|_{D(g_ig_j)} = 0.$$

Then similarly, since g_ig_j is invertible in $A_{g_ig_j}$, this implies

$$f^{m_{ij}}(s_i - s_j)|_{D(g_ig_j)} = 0.$$

We can also assume that all m_{ij}'s take the same value m, so that by the sheaf condition there exists a section $u \in \Gamma(V, \mathscr{F})$ such that $u|_{D(g_i)} = f^m s_i$. Then $f^n u$ extends $f^{m+n} s$, as desired. □

Theorem 22.1.20. *Let $X = \mathrm{Spec}(A)$ be an affine scheme. Let V be a quasi-compact open subset and $\mathscr{F}$ be an $\mathscr{O}_X|_V$-module. Then the following are equivalent:*

(i) *There is a A-module M such that $\mathscr{F}$ is isomorphic to $\widetilde{M}|_V$.*

(ii) *There exists a finite open covering (V_i) of V by sets of the form $D(f_i)$ ($f_i \in A$) contained in V, such that, for each i, $\mathscr{F}|_{V_i}$ is isomorphic to a sheaf of the form $\widetilde{M}_i$, where M_i is an A_{f_i}-module.*

(iii) *The sheaf $\mathscr{F}$ is quasi-coherent.*

(iv) (***Serre's lifting criterion***) *The following conditions are satisfied:*

  (a) *For any $D(f) \subseteq V$ and any section $s \in \Gamma(D(f), \mathscr{F})$, there exists $n \geq 0$ such that $f^n s$ can be extended to a section of $\mathscr{F}$ on V.*

  (b) *For any $D(f) \subseteq V$ and any section $t \in \Gamma(V, \mathscr{F})$ such that $t|_{D(f)} = 0$, there exists $n \geq 0$ such that $f^n t = 0$.*

Proof. The implication (i)⇒(ii) is immediate from Proposition 22.1.4 since X can be covered by standard opens. Also, since any A-module is isomorphic to the kernel of a homomorphism

$A^{\oplus I} \to A^{\oplus J}$, Corollary 22.1.6 shows that (ii)⇒(iii). Conversely, if $\mathscr{F}$ is quasi-coherent, any point $x \in V$ possesses a neighborhood of the form $D(f) \subseteq V$ such that $\mathscr{F}|_{D(f)}$ is isomorphic to the cokernel of a homomorphism $(\widetilde{A}_f)^{\oplus I} \to (\widetilde{A}_f)^{\oplus J}$, hence to the sheaf associated with the cokernel of the corresponding homomorphism $A_f^{\oplus I} \to A_f^{\oplus J}$ (Corollary 22.1.3 and Corollary 22.1.6); since V is quasi-compact, it then follows that (iii) implies (ii).

Now we prove that (ii)⇒(iv). First assume that $V = D(g)$ for some $g \in A$, and $\mathscr{F}$ is isomorphic to $\widetilde{N}$ for some A_g-module N. Since $D(g)$ can be identified with $\mathrm{Spec}(A_g)$, we can assume that $g = 1$ and $V = X$. In this case, the set $\Gamma(D(f), \mathscr{F})$ and N_f are canonically identified (Theorem 22.1.2), and it is clear that conditions (a) and (b) in (iv) are satisfied. To prove the general case, since V is quasi-compact we can choose a finite covering by standard opens $D(g_i)$ with $\mathscr{F}|_{D(g_i)}$ isomorphic to $\widetilde{M}_i$ for some A_{g_i}-module M_i. Then $\mathscr{F}$ satisfies the conditions (a) and (b) in Lemma 22.1.19, so by Lemma 22.1.19, $\mathscr{F}$ also satisfies conditions (α) and (β), which is what we want.

Finally, we show that (iv)⇒(i). First we prove that, if (a) and (b) hold for $\mathscr{F}$, then they hold for $\mathscr{F}|_{D(g)}$ with $D(g) \subseteq V$. This is evident for condition (a); as for (b), if $t \in \Gamma(D(g), \mathscr{F})$ restricts to zero on $D(f) \subseteq D(g)$, then by condition (a) there is an integer $m \geq 0$ such that $g^m t$ can be extended to V. By applying condition (b) on the extension of $g^m t$, we get another integer $n \geq 0$ such that $f^n g^m t = 0$. Since g is invertible in A_g, this gives $f^n t = 0$ as desired.

This being done, since V is quasi-compact, by Lemma 22.1.19 we know that conditions (α) and (β) holds for $\mathscr{F}$. Now consider the module $M = \Gamma(V, \mathscr{F})$; we shall define a morphism $\varphi : \widetilde{M} \to j_*\mathscr{F}$, where $j : V \hookrightarrow X$ is the inclusion. For this, it suffices to define

$$\varphi_f : M_f \to \Gamma(D(f), j_*\mathscr{F}) = \Gamma(D(f) \cap V, \mathscr{F})$$

for each $f \in A$. Since f is invertible in A_f and $\Gamma(D(f) \cap V, \mathscr{F})$ is a A_f-module, the restriction $M = \Gamma(V, \mathscr{F}) \to \Gamma(D(f) \cap V, \mathscr{F})$ factors into

$$M \longrightarrow M_f \xrightarrow{\varphi_f} \Gamma(D(f) \cap V, \mathscr{F})$$

which gives the desired maps φ_f. We now claim that the conditions (a) and (b) in (iv) imply that φ is an isomorphism. In fact, if $s \in \Gamma(D(f) \cap V, \mathscr{F})$, then by condition (a) there exist an integer $n \geq 0$ and $z \in \Gamma(V, \mathscr{F}) = M$ such that $z|_{D(f)\cap V} = f^n s$; then $\varphi_f(z/f^n) = s$, showing that φ is surjective. Similarly, if there is $z \in M$ such that $\varphi_f(z/1) = 0$ in $D(f) \cap V$, then by condition (b) there is $n \geq 0$ such that $f^n z = 0$, so that $z/1 = 0$ in M_f. This means φ_f is injective, so we get an isomorphism $\widetilde{M} \cong j_*\mathscr{F}$. By restriction, we then conclude that $\mathscr{F} \cong \widetilde{M}|_V$. □

Corollary 22.1.21. *Let $X = \mathrm{Spec}(A)$ be an affine scheme. Then the functors $M \mapsto \widetilde{M}$ and $\mathscr{F} \mapsto \Gamma(X, \mathscr{F})$ define equivalences of categories between the category of quasi-coherent $\mathscr{O}_X$-modules and the category of A-modules.*

Proof. The space X it self is quasi-compact, so we can apply Theorem 22.1.20. □

Corollary 22.1.22. *Let $X = \mathrm{Spec}(A)$ be an affine scheme. Then kernels and cokernels of maps of quasi-coherent $\mathscr{O}_X$-modules are quasi-coherent.*

Proof. This follows from the exactness of the functor $\widetilde{M}$ and Corollary 22.1.6. □

Corollary 22.1.23. *For $\widetilde{M}$ to be a $\mathcal{O}_X$-module of finite type (resp. of finite presentation), it is necessary and sufficient that M is a finitely generated A-module (resp. of finite presentation).*

Proof. In view of the exactness of the functor $M \mapsto \widetilde{M}$, it is immediate that if M is of finite type (resp. finite presentation), so is $\widetilde{M}$. Conversely, if $\widetilde{M}$ is of finite type (resp. finite presentation), since X is quasi-compact, there exists finitely many $f_i \in A$ such that $D(f_i)$ cover X and M_{f_i} is of finite type (resp. finite presentation) over A_{f_i}. It then follows from Proposition 10.4.51 that M is of finite type (resp. finite presentation). □

Corollary 22.1.24. *For an A-module M, the $\mathcal{O}_X$-module is locally free of finite rank if and only if M is a finitely generated projective A-module.*

Proof. Since X is quasi-compact, this follows from Theorem 10.5.4. □

Corollary 22.1.25. *Let $X = \operatorname{Spec}(A)$ be an affine scheme. Then any quasi-coherent $\mathcal{O}_X$-algebra over X is isomorphic to an $\mathcal{O}_X$-algebra of the form $\widetilde{B}$, where B is an algebra over A. Moreover, any quasi-coherent $\widetilde{B}$-module is isomorphic to a $\widetilde{B}$-module of the form $\widetilde{N}$, where N is a B-module.*

Proof. In fact, a quasi-coherent $\mathcal{O}_X$-algebra is a quasi-coherent $\mathcal{O}_X$-module, hence of the form $\widetilde{B}$, where B is an A-module. The fact that B is an A-algebra follows from the structural morphism $\widetilde{B} \otimes_{\mathcal{O}_X} \widetilde{B} \to \widetilde{B}$ of $\mathcal{O}_X$-modules, which induces an A-algebra map $B \otimes_A B \to B$.

If $\mathcal{G}$ is a quasi-coherent $\widetilde{B}$-module, it suffices to show that $\mathcal{G}$ is also a quasi-coherent $\mathcal{O}_X$-module to then conclude in the same way. As the question is local, we can, by restricting ourselves to an open set of X of the form $D(f)$, over which $\mathcal{G}$ is the cokernel of a morphism $\widetilde{B}^{\oplus I} \to \widetilde{B}^{\oplus J}$ of $\widetilde{B}$-modules (and a fortiori $\mathcal{O}_X$-modules). The claim then follows from Corollary 22.1.3 and Corollary 22.1.6. □

Proposition 22.1.26. *Let $X = \operatorname{Spec}(A)$ be an affine scheme, Suppose that*

$$0 \longrightarrow \mathcal{F}_1 \longrightarrow \mathcal{F}_2 \longrightarrow \mathcal{F}_3 \longrightarrow 0$$

is a short exact sequence of $\mathcal{O}_X$-modules, and assume that $\mathcal{F}_1$ is quasi-coherent. Then the sequence

$$0 \longrightarrow \Gamma(X, \mathcal{F}_1) \longrightarrow \Gamma(X, \mathcal{F}_2) \longrightarrow \Gamma(X, \mathcal{F}_3) \longrightarrow 0$$

is exact.

Proof. We know already that Γ is a left-exact functor so we have only to show that the last map is surjective (which we denot by $\psi : \Gamma(X, \mathcal{F}_2) \to \Gamma(X, \mathcal{F}_3)$). Let $s \in \Gamma(X, \mathcal{F}_3)$ be a global section. Since the morphism $\mathcal{F}_2 \to \mathcal{F}_3$ is surjective, for any $x \in X$ there is an open neighborhood $D(f)$ of x such that

$$s|_{D(f)} = \psi(t)$$

where $t \in \mathcal{F}_2(D(f))$. We claim that for some $n > 0$, $f^n s = \psi(u)$ for some $u \in \Gamma(X, \mathcal{F}_2)$. Indeed, we can cover X with a finite number of open sets $D(g_i)$ such that for each i, $s|_{D(g_i)} = \psi(t_i)$ for a section $t_i \in \mathcal{F}_2(D(g_i))$. Then by the exactness of the original sequence, on $D(f) \cap D(g_i) = D(fg_i)$ we have

$$(t - t_i)|_{D(fg_i)} \in \mathcal{F}_1(D(fg_i))$$

where we identify $\mathscr{F}_1$ as the kernel of ψ. Since $\mathscr{F}_1$ is quasi-coherent, by Corollary 22.1.21, there is an integer $n \geq 0$ such that the $f^n(t-t_i)|_{D(fg_i)}$ can be extended to a section $u_i \in \mathscr{F}_1(D(g_i))$. Let

$$\tilde{t}_i = f^n t_i + u_i \in \mathscr{F}_2(D(g_i)).$$

Then $\tilde{t}_i|_{D(fg_i)} = f^n t_i|_{D(fg_i)} + f^n(t-t_i)|_{D(fg_i)} = f^n t|_{D(fg_i)}$ and we have

$$f^n s|_{D(g_i)} = f^n \psi(t_i) = \psi(\tilde{t}_i - u_i) = \psi(\tilde{t}_i). \tag{1.3.1}$$

Now on $D(g_i g_j)$ the two sections $\tilde{t}_i$ and $\tilde{t}_j$ of $\mathscr{F}_2$ are mapped to $f^n s|_{D(g_i g_j)}$ by ψ, so $\tilde{t}_i - \tilde{t}_j \in \mathscr{F}_1(D(g_i g_j))$. Furthermore, since $\tilde{t}_i$ and $\tilde{t}_j$ are both equal to $f^n t|_{D(fg_i g_j)}$ on $D(fg_i g_j)$, by Corollary 22.1.21 there exists $m \geq 0$ such that $f^m(\tilde{t}_i - \tilde{t}_j) = 0$ on $D(g_i g_j)$, which we may take to be independent of i and j. Then the sections $f^m \tilde{t}_i$ glue to give a global section of $\mathscr{F}_2$ over X, which lifts $f^{m+n} s$ by (1.3.1). This proves the claim.

Now cover X by a finite number of open sets $D(f_i)$ such that $s|_{D(f_i)}$ lifts to a section of $\mathscr{F}_2$ over $D(f_i)$ for each i. Then by the previous proof, we can find an integer $n \geq 0$ (one for all i) and global sections $t_i \in \Gamma(X, \mathscr{F}_2)$ such that $\psi(t_i) = f^n s$. Since the open sets $D(f_i)$ cover X, the ideal $(f_1^n, \ldots, f_r^n)$ is the unit ideal of A, and we can write $1 = \sum a_i f_i^n$, with $a_i \in A$. Let $t = \sum a_i t_i$. Then t is a global section of $\mathscr{F}_2$ whose image under ψ is $\sum a_i f_i^n s = s$. □

Proposition 22.1.27. *Let $X = \operatorname{Spec}(A)$ be an affine scheme. Then the direct sum of an arbitrary collection of quasi-coherent sheaves on X is quasi-coherent. More generally, colimits of quasi-coherent sheaves are quasi-coherent.*

Proof. Let $\{\mathscr{F}_i\}_{i \in I}$ be a collection of quasi-coherent sheaves on X. By Theorem 22.1.20 we can write $\mathscr{F}_i = \widetilde{M}_i$ for A-modules M_i, so the assertion follows from Corollary 22.1.6. □

Proposition 22.1.28. *Let X be an affine scheme. Suppose that*

$$0 \longrightarrow \mathscr{F}_1 \longrightarrow \mathscr{F}_2 \longrightarrow \mathscr{F}_3 \longrightarrow 0$$

is a short exact sequence of sheaves $\mathscr{O}_X$-modules. If two out of three are quasi-coherent then so is the third.

Proof. The statement about kernels and cokernels follows from the fact that the functor $M \mapsto \widetilde{M}$ is exact and fully faithful from A-modules to quasi-coherent sheaves. Now let $\mathscr{F}_1$ and $\mathscr{F}_3$ be quasi-coherent. By Proposition 22.1.26, the corresponding sequence of global sections over X is exact, say $0 \to M_1 \to M_2 \to M_3 \to 0$. Applying the functor $\widetilde{M}$ we get an exact commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \widetilde{M}_1 \arrow[r] \arrow[d] & \widetilde{M}_2 \arrow[r] \arrow[d] & \widetilde{M}_3 \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathscr{F}_1 \arrow[r] & \mathscr{F}_2 \arrow[r] & \mathscr{F}_3 \arrow[r] & 0
\end{tikzcd}$$

The two outside arrows are isomorphisms, since $\mathscr{F}_1$ and $\mathscr{F}_3$ are quasi-coherent. So by the five lemma, the middle one is also, showing that $\mathscr{F}_2$ is quasi-coherent. □

Theorem 22.1.29. *Let $X = \operatorname{Spec}(A)$ be an affine scheme where A is Noetherian. Let V be an open subset of X and $\mathscr{F}$ an $\mathscr{O}_X|_V$-module. Then the following conditions are equivalent:*

(i) $\mathscr{F}$ *is coherent.*

(ii) $\mathscr{F}$ *is of finite type and quasi-coherent.*

(iii) There exists a finitely generated A*-moduel* M *such that* $\mathscr{F} \cong \widetilde{M}|_V$.

Proof. It is clear that (i) implies (ii). To show (ii) implies (iii), we note that V is quasi-compact since X is Noetherian, so by Theorem 22.1.20, $\mathscr{F}$ is isomorphic to $\widetilde{M}|_V$, where M is an A-module. Now we have $M = \varinjlim M_\lambda$, where M_λ is the set of finitely generated sub-A-modules of M. Since the functor $\widetilde{(-)}$ is exact, this implies $\mathscr{F} = \widetilde{N}|_V = \varinjlim \widetilde{M_\lambda}|_V$. But $\mathscr{F}$ is of finite type and V is quasi-compact, so by Proposition 19.4.10 there exists an index λ such that $\mathscr{F} = \widetilde{M_\lambda}|_V$ (note that the canonical homomorphism $\widetilde{M}_\lambda \to \widetilde{M}$ is injective). This proves (iii).

It remains to show that $\widetilde{M}|_V$ is coherent if M is finitely generated. Since $\mathscr{F}$ is clearly of finite type, it suffices to show that for every open $U \subseteq X$ and $s_1, \dots, s_n \in \mathscr{F}(U)$, the associated map $\bigoplus_{i=1}^n \mathscr{O}_U \to \mathscr{F}|_U$ is of finite type. Since the question is local, we may assume $V = D(f)$ for $f \in A$. Then it suffices to show the kernel of a morphism $\bigoplus_{i=1}^n \widetilde{A}_f \to \widetilde{M}$ is of finite type. But this morphism corresponds to a homomorphism $A_f^n \to M$, whose kernel is finitely generated since A_f is Noetherian, so the claim follows. □

Corollary 22.1.30. *Let* $X = \operatorname{Spec}(A)$ *be an affine scheme where* A *is Noetherian. Then any quasi-coherent* $\mathscr{O}_X$*-module* $\mathscr{F}$ *is the inductive limit of coherent* $\mathscr{O}_X$*-modules.*

Proof. We have $\mathscr{F} = \widetilde{M}$ for an A-module M, and M is the inductive limit of its finitely generated submodules. □

Corollary 22.1.31. *Let* $X = \operatorname{Spec}(A)$ *be an affine scheme where* A *is Noetherian. Then the functor* $M \mapsto \widetilde{M}$ *gives an equivalence of categories between the category of finite generated* A*-modules and the category of coherent* $\mathscr{O}_X$*-modules.*

22.2 General schemes

22.2.1 Schemes and morphisms of schemes

Let $(X, \mathscr{O}_X)$ be a ringed space. An oepn subset V of X is said to be **affine** if the ringed space $(V, \mathscr{O}_X|_V)$ is an affine scheme (i.e. isomorphic to the spectrum of a ring). We say $(X, \mathscr{O}_X)$ is a **scheme** if every point of X admits an affine open neighborhood. If $(X, \mathscr{O}_X)$ is a scheme, then affine open subsets of X form a basis for X (because the standard opens form a basis for a spectrum $\operatorname{Spec}(A)$, and they are again affine), and in particular $(X, \mathscr{O}_X)$ is a locally ringed space. With this, for any open subset U of X, the ringed space $(U, \mathscr{O}_X|_U)$ is also a scheme, called the scheme **induced** on U by X, or the **restriction** of $(X, \mathscr{O}_X)$ on U.

Proposition 22.2.1. *The underlying space of a scheme is Kolmogoroff.*

Proof. In fact, if x and y are two points of a scheme X, then it is obvious that there exists an open neighborhood of one of these points not containing the other if x, y are not not in a same open affine; and if they are in the same open affine, this follows from the fact that the underlying spaces of affine schemes are Kolmogoroff (Corollary 10.4.10). □

Proposition 22.2.2. *If $(X, \mathcal{O}_X)$ is a scheme, any irreducible closed subset of X admits a unique generic point, and the map $x \mapsto \overline{\{x\}}$ is a bijection of X to the family of irreducible closed subsets of X.*

Proof. Let Y is an irreducible closed subset of X and $y \in Y$. If U is an affine open neighborhood of y in X, then $U \cap Y$ is dense in Y and is irreducible (Proposition 4.1.1), so it is the closure in U of a point $x \in U$, and therefore $Y \subseteq \overline{U}$ is the closure of x in X. The uniqueness of the generic point of X follows from Proposition 22.2.1 and **??**. □

If Y is an irreducible closed subset of X and y its generic point, the local ring $\mathcal{O}_{X,y}$ is then denoted by $\mathcal{O}_{X,Y}$ and called the **local ring of X along Y**, or the **local ring of Y in X**. We say a scheme $(X, \mathcal{O}_X)$ is **irreducible** (resp. **connected**) if the underlying space X is irreducible (resp. connected), and **integral** if it is irreducible and reduced. We say the scheme $(X, \mathcal{O}_X)$ is **locally integral** if each point $x \in X$ admits an open neighborhoods U such that the scheme induced over U by $(X, \mathcal{O}_X)$ is integral. If X is an irreducible scheme and x is its generic point, the local ring $\mathcal{O}_{X,x}$ is called **the ring of rational functions on X**.

Let $(X, \mathcal{O}_X)$ and $(Y, \mathcal{O}_Y)$ be schemes. A **morphism** (of schemes) from $(X, \mathcal{O}_X)$ to $(Y, \mathcal{O}_Y)$ is defined to be that of locally ringed space. That is, a pair $(f, f^\#)$ such that for each $x \in X$, the homomorphism $f_x^\#$ is local. In this case, by passing to quotients, $f_x^\#$ induces a monomorphism $f^x : \kappa(f(x)) \to \kappa(x)$, so $\kappa(x)$ can be considered as an extension of the field $\kappa(f(x))$.

The composition of two morphisms of schemes is defined in the same way with that of locally ringed spaces, and we then see that schemes form a category, denoted by **Sch**. Following the general notation, we denote by $\mathrm{Hom}_{\mathbf{Sch}}(X, Y)$ the set of morphisms from a scheme X to a scheme Y.

Example 22.2.3. Let U be an open subset of X. Then the canonical injection of $(U, \mathcal{O}_X|_U)$ to $(X, \mathcal{O}_X)$ is a morphism of schemes; it is moreover a monomorphism of ringed spaces (and a fortiori a monomorphism of schemes).

Proposition 22.2.4. *Let $(X, \mathcal{O}_X)$ be a scheme and $(Y, \mathcal{O}_Y)$ be an affine scheme. Then there exists a canonical bijection*

$$\mathrm{Hom}_{\mathbf{Sch}}(X, Y) \to \mathrm{Hom}_{\mathbf{Ring}}(\Gamma(X, \mathcal{O}_X), \Gamma(X, \mathcal{O}_X)).$$

Proof. Let $A = \Gamma(Y, \mathcal{O}_Y)$. Note first that, if $(X, \mathcal{O}_X)$ and $(Y, \mathcal{O}_Y)$ are any two ringed spaces, a morphism $(\psi, \psi^\#) : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ canonically defines a homomorphism of rings

$$\Gamma(Y, \mathcal{O}_Y) \to \Gamma(Y, \psi_*(\mathcal{O}_X)) = \Gamma(X, \mathcal{O}_X).$$

It then remains to see that any homomorphism $\rho : A \to \Gamma(X, \mathcal{O}_X)$ is of the form $\Gamma(\psi^\#)$ for a unique morphism $(\psi, \psi^\#)$. However, there is by hypothesis a covering (V_α) of X by affine open sets. By considering the composition

$$A \xrightarrow{\rho} \Gamma(X, \mathcal{O}_X) \longrightarrow \Gamma(V_\alpha, \mathcal{O}_X|_{V_\alpha})$$

we obtain a homomorphism $\rho_\alpha : A \to \Gamma(V_\alpha, \mathcal{O}_X|_{V_\alpha})$, which corresponds to a morphism $(\psi_\alpha, \psi_\alpha^\#)$ from the scheme $(V_\alpha, \mathcal{O}_X|_{V_\alpha})$ to $(Y, \mathcal{O}_Y)$ (Theorem 22.1.16). Moreover, for each pair (α, β) of indices, any point of $V_\alpha \cap V_\beta$ admits an affine open neighborhood W contained in $V_\alpha \cap V_\beta$; it is clear that by composing ρ_α and ρ_β with the restriction homomorphism to W, we obtain the same homomorphism $A \to \Gamma(W, \mathcal{O}_X|_W)$, so, by virtue of the relation $(\psi_\alpha^\#)_x = (\rho_\alpha)_x$ for any

$x \in V_\alpha$ and any α, the restrictions of $(\psi_\alpha, \psi_\alpha^\#)$ and $(\psi_\beta, \psi_\beta^\#)$ to W coincide. By gluing we then get a unique morphism $(\psi, \psi^\#) : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ which extending $(\psi_\alpha, \psi_\alpha^\#)$ on each V_α. It is clear that $(\psi, \psi^\#)$ is a morphism of schemes, and we have $\Gamma(\psi^\#) = \rho$. □

Remark 22.2.1. Let $\rho : A \to \Gamma(X, \mathcal{O}_X)$ be a ring homomorphism, and let $(\psi, \psi^\#)$ be the corresponding morphism $(X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$. For each $f \in A$, we have

$$\psi^{-1}(D(f)) = \{x \in X : f \notin \mathfrak{m}_{\psi(x)}\} = \{x \in X : (\rho(x))_x \notin \mathfrak{m}_x\} = X_{\rho(f)}.$$

Note that this can be viewed as a generalization of Proposition 10.4.18(a).

Proposition 22.2.5. *Under the hypothesis of Proposition 22.2.4, let $\rho : A \to \Gamma(X, \mathcal{O}_X)$ be a ring homomorphism and $f : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ the corresponding morphism of schemes. Let $\mathcal{F}$ (resp. $\mathcal{G}$) be a quasi-coherent $\mathcal{O}_X$-module (resp. $\mathcal{O}_Y$-module). Then there exist a canonical bijection*

$$\mathrm{Hom}_{\mathbf{Qcoh(Y)}}(\mathcal{G}, f_*(\mathcal{F})) \to \mathrm{Hom}_A(\Gamma(Y, \mathcal{G}), \rho^*(\Gamma(X, \mathcal{F}))).$$

Proof. Indeed, by reasoning as in Proposition 22.2.4, we are immediately reduced to the case where X is affine and the proposition then follows from Corollary 22.1.3 and Proposition 22.1.11. □

We say a morphism $f : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ is **open** (resp. **closed**) if for any open subset U of X (resp. any closed subset F of X), $f(U)$ is open in Y (resp. $f(F)$ is closed in Y). We say f is **dominant** if $f(X)$ is dense in Y, and **surjective** if f is surjective. It should be noted that these conditions only involve the continuous map f.

Proposition 22.2.6. *Let $f : (X, \mathcal{O}_X)$ and $g : (Y, \mathcal{O}_Y) \to (Z, \mathcal{O}_Z)$ be morphisms of schemes.*

(a) If f and g are open (resp. closed, dominant, surjective), so is the composition $g \circ f$.

(b) If f is surjective and $g \circ f$ is closed, g is closed.

(c) If $g \circ f$ is surjective, g is surjective.

Proof. The assertions (a) and (c) are evident. Put $h = g \circ f$. If F is closed in Y, then $f^{-1}(F)$ is closed in X, so $h(f^{-1}(F))$ is closed in Z. But since f is surjective, we have $f(f^{-1}(F)) = F$, so $h(f^{-1}(F)) = g(F)$, which shows g is closed. □

Proposition 22.2.7. *Let $f : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ be a morphism of schemes and (U_α) an open covering of Y. For f to be open (resp. closed, surjective, dominant), it is necessary and sufficient that for each U_α, the restrictions $f : f^{-1}(U_\alpha) \to U_\alpha$ is open (resp. closed, surjective, dominant).*

Proof. The proposition follows immediately from the definitions, taking into account the fact that a subset F of Y is closed (resp. open, dense) in Y if and only if each of the sets $F \cap U_\alpha$ is closed (resp. open, dense) in U_α. □

Let $(X, \mathcal{O}_X)$ and $(Y, \mathcal{O}_Y)$ be schemes; suppose that X and Y have a same finite number of irreducible components X_i (resp. Y_i) $(1 \le i \le n)$; let ξ_i (resp. η_i) be the generic point of X_i (resp. Y_i). We say that a morphism

$$f : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$$

is **birational** if, for any i, we have $f^{-1}(\eta_i) = \{\xi_i\}$ and $f^{\#}_{\xi_i} : \mathcal{O}_{Y,\eta_i} \to \mathcal{O}_{X,\xi_i}$ is an isomorphism. It is clear that any birational morphism is dominant, hence surjective if it is closed.

Remark 22.2.2. Throughout the remainder of this chapter and when there is no risk of creating confusion, we will omit in the notation of a scheme (resp. of a morphism) the structural sheaf (resp. the morphism of structural sheaf). If U is an open subset of the underlying space of a scheme X, when we speak of U as of a scheme, it will always be the scheme induced on U by X.

With the morphisms of schemes defined, we can talk about glueing schemes as in the case of ringed spaces. It follows immediately from the definition that any ringed space obtained by glueing schemes is again a scheme. In particular, since any scheme admits a basis of affine open subsets, we see any scheme is obtained by glueing affine schemes.

Example 22.2.8. Cosnider a field K, $A = K[s]$, $B = K[t]$ be two rings of polynomials over K with one indeterminate, and $X_1 = \mathrm{Spec}(A)$, $X_2 = \mathrm{Spec}(B)$. In X_1 (resp. X_2), let U_{12} (resp. U_{21}) be the affine open set $D(s)$ (resp. $D(t)$), whose ring A_s (resp. B_t) is formed by the rational fractions of the form $f(s)/s^m$ (resp. $g(t)/t^n$) with $f \in A$ (resp. $g \in B$). Let φ_{12} be the isomorphism of of schemes $U_{21} \to U_{12}$ corresponding to the isomorphism of A and B such that, $f(s)/s^m$ is mapped to the rational fraction $f(1/t)/(1/t^m)$ (i.e. we map s to $1/t$). We can then glue X_1 and X_2 along U_{12} and U_{21} by the isomorphism u_{12}, which evidently satisfies the glueing condition. We will see later the schem X thus obtained is a particular case of a general method of construction. We only show here that X is not an affine scheme, which will result from the fact that the ring $\Gamma(X, \mathcal{O}_X)$ is isomorphic to K, therefore has a spectrum reduced to a point. Indeed, a section of $\mathcal{O}_X$ above X has a restriction over X_1 (resp. X_2), identified with an open affine of X, which is a polynomial $f(s)$ (resp. $g(t)$), and it follows from the definition of u_{12} that we must have $g(t) = f(1/t)$, which is not possible only if $f = g \in K$.

22.2.2 Local schemes

Let X be a scheme and $A = \Gamma(X, \mathcal{O}_X)$. We say X is a local scheme if X is affine and the ring X is local. In this case, there then exists a unique closed point ξ in X, and for any point $x \in X$ we have $\xi \in \overline{\{x\}}$.

Following this notation, for a general scheme Y and $y \in Y$, the scheme $\mathrm{Spec}(\mathcal{O}_{Y,y})$ is called the **local scheme of Y at y**. Let V be an affine open subset of Y containing y, and B the ring of V. The local ring $\mathcal{O}_{Y,y}$ is then canonically identified with B_y, and the canonical homomorphism $B \to B_y$ then induces a morphism $\mathrm{Spec}(\mathcal{O}_{Y,y}) \to V$ of schemes. If we compose this with the canonical injection of V into Y, we then get a morphism $\mathrm{Spec}(\mathcal{O}_{Y,y}) \to Y$, which is independent of the choice of the affine open V containing y: in fact, if U is another affine neighborhood of y, there exists an affine open neighborhood W of y contained in $U \cap V$; we can then limit ourselves to the case $U \subseteq V$, and if A is the ring of U, we have a commutative diagram

$$\begin{tikzcd} A \arrow[rr] \arrow[dr] & & B \arrow[dl] \\ & \mathcal{O}_{Y,y} & \end{tikzcd}$$

The morphism $\mathrm{Spec}(\mathcal{O}_{Y,y}) \to Y$ thus defined is said to be **canonical**.

Proposition 22.2.9. *Let Y be a scheme, $y \in Y$, and $f : \mathrm{Spec}(\mathcal{O}_{Y,y}) \to Y$ be the canonical morphism.*

(a) The map f is a homeomorphism of $\mathrm{Spec}(\mathcal{O}_{Y,y})$ onto the subspace S_y of points $z \in Y$ such that $y \in \overline{\{z\}}$ (i.e. the set of generalizations of y).

(b) For each $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_{Y,y})$, the homomorphism $f^{\#}_{\mathfrak{p}} : \mathcal{O}_{Y,f(\mathfrak{p})} \to (\mathcal{O}_{Y,y})_{\mathfrak{p}}$ is an isomorphism.

In particular, f is a monomorphism of locally ringed spaces.

Proof. Since the unique closed point η of $\mathrm{Spec}(\mathcal{O}_{Y,y})$ belongs to the closure of any other point in this space, and $f(\eta) = y$, the image of $\mathrm{Spec}(\mathcal{O}_{Y,y})$ by the continuous map f is contained in S_y. As S_y is contained in any affine open neighborhood of y, we can reduce to the case where Y is an affine scheme; but in this case the proposition follows immediately. □

Corollary 22.2.10. *There is a bijective correspondence between $\mathrm{Spec}(\mathcal{O}_{Y,y})$ and irreducible closed subsets of Y containing y.*

Proof. This follows from Proposition 22.2.9 and the fact that every irreducible closed set in Y has a unique generic point. □

Corollary 22.2.11. *For a point $y \in Y$ to be the generic point of an irreducible component of Y, it is necessary and suffcient that $\mathcal{O}_{Y,y}$ is zero-dimensional.*

Proof. This follows from the observation that y is the generic point of an irreducible component if and only if it is a maximal element under generalization, which is then equivalent by Corollary 22.2.10 to that $\mathrm{Spec}(\mathcal{O}_{Y,y})$ is a singleton. □

Proposition 22.2.12. *Let $(X, \mathcal{O}_X)$ be a local scheme with $A = \Gamma(X, \mathcal{O}_X)$, ξ its unique closed point, and $(Y, \mathcal{O}_Y)$ a scheme. Then any morphism $f : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ factors through $\mathrm{Spec}(\mathcal{O}_{Y,f(\xi)})$:*

$$f : X \to \mathrm{Spec}(\mathcal{O}_{Y,f(\xi)}) \to Y$$

where the second one is the canonical morphism, and the first one corresponds to a local homomorphism $\mathcal{O}_{Y,f(\xi)} \to A$.

Proof. In fact, for any $x \in X$, we have $\xi \in \overline{\{x\}}$, hence $f(\xi) \in \overline{\{f(x)\}}$. It then follows that $f(X)$ is contained in any affine open neighborhood of $f(\xi)$ (in fact any open neighborhood of $f(\xi)$). We can then reduce to the case that $(Y, \mathcal{O}_Y)$ is an affine scheme with ring $B = \Gamma(Y, \mathcal{O}_Y)$, and the morphism f corresponds to a ring homomorphism $\rho : B \to A$. We have $\rho^{-1}(\mathfrak{p}_\xi) = \mathfrak{p}_{f(\xi)}$, so the image under ρ of an element of $B - \mathfrak{p}_{f(\xi)}$ is invertible in the local ring A, and we get a canonical homomorphism $\rho_\xi : B_{f(\xi)} \to A$. □

Corollary 22.2.13. *There is a canonical bijection between $\mathrm{Hom}_{\mathbf{Sch}}(X, Y)$ to the set of local homomorphisms $\mathcal{O}_{Y,y} \to A$, where $y \in Y$.*

Proof. It suffices to note that any local homomorphism $\mathcal{O}_{Y,y} \to A$ corresponds to a unique morphism $f : X \to \mathrm{Spec}(\mathcal{O}_{Y,y})$ such that $f(\xi) = y$, and by composing this with the canonical morphism $\mathrm{Spec}(\mathcal{O}_{Y,y}) \to Y$, we get a morphism $X \to Y$. □

Example 22.2.14. The affine scheme whose ring is a field K have an underlying space reduced to one point. If A is a local ring of maximal ideal $\mathfrak{m}$, any local homomorphism $A \to K$ has a kernel equal to $\mathfrak{m}$, so factors into $A \to A/\mathfrak{m} \to K$, where the second arrow is a monomorphism. The morphisms $\mathrm{Spec}(K) \to \mathrm{Spec}(A)$ correspond therefore bijectively to the field extensions $A/\mathfrak{m} \to K$.

Let $(Y, \mathcal{O}_Y)$ be a scheme; for any $y \in Y$ and any ideal $\mathfrak{a}_y$ of $\mathcal{O}_{Y,y}$, the canonical homomorphism $\mathcal{O}_{Y,y}/\mathfrak{a}_y$ defines a morphism $\mathrm{Spec}(\mathcal{O}_{Y,y}/\mathfrak{a}_y) \to \mathrm{Spec}(\mathcal{O}_{Y,y})$; by composing this with the canonical morphism $\mathrm{Spec}(\mathcal{O}_{Y,y}) \to Y$, we obtain a morphism $\mathrm{Spec}(\mathcal{O}_{Y,y}/\mathfrak{a}_y) \to Y$, also called canonical. If $\mathfrak{a}_y = \mathfrak{m}_y$ is the maximal ideal of $\mathcal{O}_{Y,y}$, then $\mathcal{O}_{Y,y} = \kappa(y)$ and Corollary 22.2.13 then imply the following result:

Corollary 22.2.15. *Let $(X, \mathcal{O}_X)$ be a local scheme with $K = \Gamma(X, \mathcal{O}_X)$ a field, ξ its unique point, and $(Y, \mathcal{O}_Y)$ be a scheme. Then any morphism $f : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ factors into*

$$f : X \to \mathrm{Spec}(\kappa(f(\xi))) \to Y$$

where the second arrow is the canonical morphism, and the first arrow corresponds to a field extension $\kappa(f(\xi)) \to K$. This establishes a canonical bijection between $\mathrm{Hom}_{\mathbf{Sch}}(X, Y)$ to the set of field extensions $\kappa(y) \to K$, where $y \in Y$.

Corollary 22.2.16. *For any $y \in Y$, the canonical morphism $\mathrm{Spec}(\mathcal{O}_{Y,y}/\mathfrak{a}_y) \to Y$ is a monomorphism of locally ringed spaces.*

Proof. This follows from Proposition 22.2.9 and Corollary 22.1.18. □

Remark 22.2.3. Let X be a local scheme, ξ its unique closed point. Since any affine open neighborhood of ξ is necessarily all of X, any invertible $\mathcal{O}_X$-module is necessarily isomorphic to $\mathcal{O}_X$ (in other words, is trivial). This property does not hold in general for any affine scheme $\mathrm{Spec}(A)$, but we will see that if A is a normal ring, this is true when A is factorial.

22.2.3 Shemes over a scheme

As in any category, for a scheme S we can define the category $\mathbf{Sch}/S$ of S-objects in the category of schemes, which will be a morphism $\varphi : X \to S$ where X is a scheme. In this case we also say that X is a **scheme over S**, or an **S-scheme**. We say that S is the **base scheme** of the S-scheme X and φ is called the structural morphism of the S-scheme X. When S is an affine scheme of the ring A, we also say that X is a **scheme over A** or an **A-scheme**.

It follows from Proposition 22.2.4 that giving a scheme over a ring A is equivalent to giving a scheme $(X, \mathcal{O}_X)$, where $\mathcal{O}_X$ is an A-algebra. In particular, any scheme can be considered as a scheme over $\mathbb{Z}$. In other words, the scheme $\mathrm{Spec}(\mathbb{Z})$ is a final object in the category of schemes (also a final object in the category of locally ringed spaces).

If $\varphi : X \to S$ is the structural morphism of an S-scheme X, we say a point $x \in X$ is **lying over** a point $s \in S$ if $\varphi(x) = s$. We say X **dominates** S if the morphism φ is dominant. Let X and Y be two S-schemes; a morphism $u : X \to Y$ is called a **morphism of schemes over S** (or **S-morphism**) if the diagram

$$\begin{tikzcd} X \arrow[rr, "u"] \arrow[dr] & & Y \arrow[dl] \\ & S & \end{tikzcd}$$

is commutative; in other words, if for any $s \in S$ and any $x \in X$ lying over s, the point $u(x)$ is lying over s. This definition immediately shows that the composite of two S-morphisms is an S-morphism, so the S-schemes thus form a category. We denote by $\mathrm{Hom}_S(X, Y)$ the set of S-morphisms from an S-scheme X to an S-scheme Y; the identity morphism of an S-scheme X is then denoted by 1_X or id_X. If S is an affine scheme S, we also say A-morphisms for S-morphisms.

If X is an S-scheme, $\varphi : X \to S$ the structural morphism, an ***S*-section** of X is defined to be an S-morphism of S to X, which is equivalently a morphism $\psi : S \to X$ of schemes such that $\varphi \circ \psi = \mathrm{id}_S$. We denote by $\Gamma(X/S)$ the set of S-sections of X.

Example 22.2.17. If X is an S-scheme and $v : X' \to X$ a morphism of schemes, the composition scheme

$$X' \xrightarrow{v} X \longrightarrow S$$

then defines X' as an S-scheme; in particular, any scheme induceed over an open subset U of X can be considered as an S-scheme by means of the canonical injection.

Example 22.2.18. Let $u : X \to Y$ be an S-morphism of S-schemes, the restriction of u on any open subset U of X is then an S-morphism $U \to Y$. Conversely, let (U_α) be a covering of X and for each α, let $u_\alpha : U_\alpha \to Y$ be an S-morphism; if for any pair (α, β) of indices, the restrictions of u_α and u_β on $U_\alpha \cap U_\beta$ coincide, then there exists a unique S-morphism $X \to Y$ whose restriction on U_α equals to u_α.

Let $S \to S'$ be a morphism of schemes; for any S'-scheme X, the composition morphism $X \to S' \to S$ then defines X as an S-scheme. Conversely, suppose that S' is the scheme induced over an open subset of S; let X be an S-scheme and suppose that the structural morphism $X \to S$ has image contained in S'; then we can consider X as an S'-scheme. In the latter case, if Y is an S-scheme whose structural morphism also maps the underlying space in S', any S-morphism from X in Y is also an S'-morphism.

22.2.4 Quasi-coherent sheaves on schemes

Proposition 22.2.19. *Let X be a scheme. For an $\mathcal{O}_X$-module $\mathcal{F}$ to be quasi-coherent, it is necessary and sufficient that, for any affine open subset V of X, the restriction $\mathcal{F}|_V$ is isomorphism to the sheaf associated with a $\Gamma(V, \mathcal{O}_X)$-module.*

Proof. We recall that being quasi-coherent is a local property, and affine opens form a basis for X. Also, by Theorem 22.1.20, a quasi-coherent sheaf on an affine open V is isomorphic to $\widetilde{M}$ for some $\Gamma(V, \mathcal{O}_X)$-module M. □

Corollary 22.2.20. *Let X be an arbitrary scheme.*

(i) Let $0 \to \mathcal{F} \to \mathcal{G} \to \mathcal{H} \to 0$ be an exact sequence of $\mathcal{O}_X$-modules; if two of them are quasi-coherent, then so is the third one.

(ii) The images, kernels and cokernels of homomorphisms of quasi-coherent $\mathcal{O}_X$-modules are quasi-coherent. The inductive limits and direct sums of quasi-coherent sheaves are quasi-coherent. If $\mathcal{G}$ and $\mathcal{H}$ are quasi-coherent $\mathcal{O}_X$-modules of a quasi-coherent $\mathcal{O}_X$-module $\mathcal{F}$, then $\mathcal{G} + \mathcal{H}$ and $\mathcal{G} \cap \mathcal{H}$ are quasi-coherent.

(iii) Let $0 \to \mathscr{F}_1 \to \mathscr{F}_2 \to \mathscr{F}_3 \to \mathscr{F}_4 \to \mathscr{F}_5 \to 0$ *be an exact sequence of* $\mathscr{O}_X$*-modules. If* $\mathscr{F}_1, \mathscr{F}_2, \mathscr{F}_4, \mathscr{F}_5$ *are quasi-coherent, so is* $\mathscr{F}_3$*.*

(iv) If $\mathscr{F}$ *and* $\mathscr{G}$ *are quasi-coherent* $\mathscr{O}_X$*-modules,* $\mathscr{F} \otimes_{\mathscr{O}_X} \mathscr{G}$ *is quasi-coherent. In particular, if* $\mathscr{I}$ *is a quasi-coherent ideal of* $\mathscr{O}_X$*,* $\mathscr{I}\mathscr{F}$ *is a quasi-coherent* $\mathscr{O}_X$*-module.*

(v) Let $\mathscr{F}$ *be a quasi-coherent* $\mathscr{O}_X$*-module with finite presentation. Then for any quasi-coherent* $\mathscr{O}_X$*-module* $\mathscr{G}$*,* $\mathscr{H}om_{\mathscr{O}_X}(\mathscr{F}, \mathscr{G})$ *is quasi-coherent.*

(vi) If $\mathscr{F}$ *is a quasi-coherent* $\mathscr{O}_X$*-module of finite type, the annihilator* $\mathscr{I}$ *of* $\mathscr{F}$ *is a quasi-coherent ideal of* $\mathscr{O}_X$*.*

Proof. By Proposition 22.2.19, assertions (i) to (v) follow from Proposition 22.1.28, Corollary 22.1.6, and Corollary 22.1.9. To prove (vi), we can assume that $X = \operatorname{Spec}(A)$ is affine, $\mathscr{F} = \widetilde{M}$, where M is a finitely generated A-module, with generators $t_1, \dots, t_r$. The ideal $\mathscr{I}$ is then the intersection of the annihilators of t_i. But the annihilator of t_i is by definition the kernel of the canonical morphism $\mathscr{O}_X \to \mathscr{F}$ corresponding to $s \mapsto st_i$ from A to M, hence quasi-coherent. It then follows that $\mathscr{I}$ is quasi-coherent, as an intersection of quasi-coherent $\mathscr{O}_X$-modules. □

Corollary 22.2.21. *Let* X *be a scheme,* $0 \to \mathscr{F} \to \mathscr{G} \to \mathscr{H} \to 0$ *an exact sequence of quasi-coherent* $\mathscr{O}_X$*-modules. If* $\mathscr{H}$ *is finitely presented and* $\mathscr{G}$ *is of finite type, then* $\mathscr{F}$ *is of finite type.*

Proof. Since this question is local, we may assume that X is affine, and the corresponding result is then Proposition 7.2.26. □

Proposition 22.2.22. *Let* X *be a scheme and* $\mathscr{B}$ *be a quasi-coherent* $\mathscr{O}_X$*-algebra. For a* $\mathscr{B}$*-module* $\mathscr{F}$ *to be quasi-coherent, it is necessary and sufficient that* $\mathscr{F}$ *is a quasi-coherent* $\mathscr{O}_X$*-module. In particular, if* $\mathscr{F}$ *and* $\mathscr{G}$ *are quasi-coherent* $\mathscr{B}$*-modules,* $\mathscr{F} \otimes_{\mathscr{B}} \mathscr{G}$ *is a quasi-coherent* $\mathscr{B}$*-module; the same holds for* $\mathscr{H}om_{\mathscr{B}}(\mathscr{F}, \mathscr{G})$ *if* $\mathscr{F}$ *is a finitely presented* $\mathscr{B}$*-module.*

Proof. Since the question is local, we can suppose that X is affine with ring A, and then $\mathscr{B} = \widetilde{B}$, where B is an A-algebra. If $\mathscr{F}$ is quasi-coherent over the space $(X, \mathscr{B})$, we can write $\mathscr{F}$ as the cokernel of $\mathscr{B}$-homomorphism $\mathscr{B}^{\oplus I} \to \mathscr{B}^{\oplus J}$; since this homomorphism is also an $\mathscr{O}_X$-homomorphism, and $\mathscr{B}^{\oplus I}$, $\mathscr{B}^{\oplus J}$ are quasi-coherent $\mathscr{O}_X$-modules, we conclude that $\mathscr{F}$ is also quasi-coherent.

Conversely, if $\mathscr{F}$ is a quasi-coherent $\mathscr{O}_X$-module, we have $\mathscr{F} = \widetilde{M}$ where M is a B-module (Corollary 22.1.25); M is isomorphic to the cokernel of a homomorphism $B^{\oplus I} \to B^{\oplus J}$, so $\mathscr{F}$ is a $\mathscr{B}$-module isomorphic to the cokernel of the corresponding homomorphism $\mathscr{B}^{\oplus I} \to \mathscr{B}^{\oplus J}$. This completes the proof. □

Let X be a scheme. A quasi-coherent $\mathscr{O}_X$-algebra $\mathscr{B}$ is **of finite type** (resp. **of finite presentation**) if for all $x \in X$, there exists an open affine neighborhood U of x such that $\Gamma(U, \mathscr{B}) = B$ is an algebra of type finite (resp. of finite presentation[1]) over $\Gamma(U, \mathscr{O}_X) = A$. If this is the case, we have $\mathscr{B}|_U = \widetilde{B}$, and for all $f \in A$, the $(\mathscr{O}_X|_{D(f)})$-algebra $\mathscr{B}|_{D(f)}$ induced on $D(f)$ is of finite type (resp. of finite presentation), because it is isomorphic to $\widetilde{B \otimes_A A_f}$. As the $D(f)$ form a basis of the topology of X, we deduce that for any open set V of X, $\mathscr{B}|_V$ is a $(\mathscr{O}_X|_V)$-algebra of finite type (resp. of finite presentation).

[1] Recall that an algebra B is finitely presented over A if it is isomorphic to the quotient of a polynomial ring over A in finitely many variables by a finitely generated ideal.

Proposition 22.2.23. *Let X be a scheme, $\mathscr{E}$ a locally free $\mathscr{O}_X$-module of rank r, Z a finite subset of X contained in an affine open V. Then there exists an open neighborhood $U \subseteq V$ of Z such that $\mathscr{E}|_U$ is isomorphic to $\mathscr{O}_U^r$.*

Proof. By replacing X by V, we can assume that $X = \operatorname{Spec}(A)$ is affine. For each $z_i \in Z$ there exists a closed point z_i' in the closure $\overline{\{z_i\}}$ (that is, a maximal ideal containing $\mathfrak{p}_{z_i}$); if Z' is the set of the z_i', any neighborhood of Z' is a neighborhood of Z, and we can then suppose that Z is closed in X. Now, the subset Z of X is defined by an ideal $\mathfrak{a}$ of A; consider the scheme $\operatorname{Spec}(A/\mathfrak{a})$, with Z its underlying space, and the injection $\iota : Z \to X$ corresponds to the canonical homomorphism $A \to A/\mathfrak{a}$. Then $\iota^*(\mathscr{E}) = \mathscr{E} \otimes_{\mathscr{O}_X} \mathscr{O}_Z$ is locally free with rank r over the discrete scheme Z, so is isomorphic to $\mathscr{O}_Z^r$. In other words, there exist sections $s_1, \dots, s_r$ of $\mathscr{E} \otimes_{\mathscr{O}_X} \mathscr{O}_Z$ over Z such that the homomorphism $\mathscr{O}_Z^r \to \mathscr{E} \otimes_{\mathscr{O}_X} \mathscr{O}_Z$ defined by these sections is bijective. On the other hand, we have $\mathscr{E} = \widetilde{M}$ where M is an A-module; then each s_i belongs to $M \otimes_A (A/\mathfrak{a})$, and is then the image of an element $t_i \in M = \Gamma(X, \mathscr{E})$. For each $z_j \in Z$, by Corollary 19.4.38, there then exists a neighborhood V_i of z_i in X such that the restrictions of t_i to V_j define an isomorphism $\mathscr{O}_X^r|_{V_j} \to \mathscr{E}|_{V_j}$; the union U of the V_j's then satisfies the requirement. □

Proposition 22.2.24. *Let X a scheme and $\mathscr{F}$ be a quasi-coherent $\mathscr{O}_X$-module of finite type. Then there exists a closed subscheme Y of X with underlying space* $\operatorname{supp}(\mathscr{F})$ *and a quasi-coherent $\mathscr{O}_Y$-module $\mathscr{G}$ of finite type supported on Y such that, if $j : Y \to X$ is the canonical injection, $\mathscr{F}$ is isomorphic to $j_*(\mathscr{G})$.*

Proof. It suffices to note that the annihilator $\mathscr{I}$ of $\mathscr{F}$ is a quasi-coherent ideal of $\mathscr{O}_X$ (Corollary 22.2.20), so if Y is the closed subscheme of X defined by $\mathscr{I}$, as $\mathscr{I}\mathscr{F} = 0$, $\mathscr{F}$ is an $(\mathscr{O}_X/\mathscr{I})$-module, and we can take $\mathscr{G} = j^*(\mathscr{F})$. □

22.2.5 Noetherian schemes and locally Noetherian schemes

We say a scheme X is Noetherian (resp. locally Noetherian) if there is a finite covering (resp. a covering) of open affines V_α such that each ring $\Gamma(V_\alpha, \mathscr{O}_X)$ is Noetherian. The underlying space of a Noetherian (resp. locally Noetherian) scheme is then a Noetherian space (resp. locally Noetherian). Moreover, if X is locally Noetherian. the structural sheaf $\mathscr{O}_X$ is coherent, any quasi-coherent $\mathscr{O}_X$-module of finite type is coherent (Theorem 22.1.29), and any local ring $\mathscr{O}_{X,x}$ is Noetherian. Any quasi-coherent sub-$\mathscr{O}_X$-module (resp. any quasi-coherent $\mathscr{O}_X$-quotient) of a coherent $\mathscr{O}_X$-module $\mathscr{F}$ is then coherent, because the question is local again, and we just apply Theorem 22.1.29, together with the fact that a sub-module (resp. quotient module) of a finitely generated module on a Noetherian ring is finitely generated. More particularly, any quasi-consistent ideal of $\mathscr{O}_X$ is consistent.

If a scheme X is a finite union (resp. a union) of open Noetherian (resp. locally Noetherian) subschemes W_λ, it is clear that X is then Noetherian (resp. locally Noetherian).

Proposition 22.2.25. *For a scheme X to be Noetherian, it is necessary and sufficient that it is locally Noetherian and its underlying space is quasi-compact.*

Proof. This follows from the definition, since a Noetherian space is quasi-compact. □

Proposition 22.2.26. *Let X be an affine scheme with ring A. Then the following conditions are equivalent:*

(i) *X is Noetherian;*

(ii) *X is locally Noetherian;*

(iii) *A is Noetherian.*

Proof. Since X is quasi-compact, it is clear that (i) and (ii) are equivalent. Also, (iii) implies (i) by definition. Now assume that X is Noetherian, then there is a finite covering (V_i) of X by affine opens where $A_i = \Gamma(V_i, \mathscr{O}_X)$ is Noetherian. Let $(\mathfrak{a}_n)$ be an increasing sequence of ideals of A; it corresponds to it canonically in a one-to-one way to an increasing sequence $(\tilde{\mathfrak{a}}_n)$ of ideals in $\widetilde{A} = \mathscr{O}_X$; to see that the sequence $(\mathfrak{a}_n)$ is stationary, it suffices to prove that the sequence $(\tilde{\mathfrak{a}}_n)$ is. However, the restriction $\tilde{\mathfrak{a}}_n|_{V_i}$ is a quasi-coherent ideal of $\mathscr{O}_X|_{V_i}$; $\tilde{\mathfrak{a}}_n|_{V_i}$ is then of the form $\tilde{\mathfrak{a}}_{n,i}$, where $\mathfrak{a}_{n,i}$ is an ideal of A_i. As A_i is Noetherian, the sequence $(\mathfrak{a}_{n,i})$ is stationary for all i, hence the proposition. □

Note that the above reasoning also proves that if X is a Noetherian scheme, any increasing sequence of coherent ideals of $\mathscr{O}_X$ is stationary.

Proposition 22.2.27. *Let X be a locally Noetherian scheme. Any quasi-coherent $\mathscr{O}_X$-algebra $\mathscr{B}$ of finite type is a coherent shaf of rings and an $\mathscr{O}_X$-algebra of finite presentation.*

Proof. We can assume that $X = \operatorname{Spec}(A)$ is affine, where A is a Noetherian ring, and $\mathscr{B} = \widetilde{B}$, where B is an A-algebra of finite type. It then follows that B is finitely presented over A, so $\mathscr{B}$ is of finite presentation. To show that $\mathscr{B}$ is coherent, we must prove that the kernel $\mathscr{N}$ of a $\mathscr{B}$-homomorphism $\mathscr{B}^m \to \mathscr{B}$ is a $\mathscr{B}$-module of finite type; but it is of the form $\widetilde{N}$, where N is the kernel of the corresponding homomorphism $B^m \to B$ of B-modules. Since B is also Noetherian, N is a finitely generated B-module. There then exists a surjective B-homomorphism $B^n \to N$, so a surjective homomorphism $\mathscr{B}^n \to \mathscr{N}$, which proves our assertion. □

Corollary 22.2.28. *Let X be a locally Noetherian scheme and $\mathscr{B}$ be a quasi-coherent $\mathscr{O}_X$-algebra of finite type. For a $\mathscr{B}$-module $\mathscr{F}$ to be coherent, it is necessary and sufficient that $\mathscr{F}$ is a quasi-coherent $\mathscr{O}_X$-module and a $\mathscr{B}$-module of finite type, and if $\mathscr{G}$ is a sub-$\mathscr{B}$-module or a quotient $\mathscr{B}$-module of $\mathscr{F}$, for $\mathscr{G}$ to be a coherent $\mathscr{B}$-module, it is necessary and sufficient that $\mathscr{G}$ is a quasi-coherent $\mathscr{O}_X$-module.*

Proof. Considering Proposition 22.2.22, the conditions on $\mathscr{F}$ is necessary. To prove the sufficiency, we can assume that $X = \operatorname{Spec}(A)$ is affine, where A is Noetherian, $\mathscr{B} = \widetilde{B}$, where B is an A-algebra of finite type, and $\mathscr{F} = \widetilde{M}$, where M is a B-module and there exists a surjective B-homomorphism $\mathscr{B}^m \to \mathscr{F}$. Then we get a corresponding homomorphism $B^m \to M$, so M is a finitely generated B-module; the kernel P of thie homomorphism is finitely generated since B is Noetherian, and $\mathscr{F}$ is therefore the cokernel of a morphism $\mathscr{B}^n \to \mathscr{B}^m$, so it is coherent (since $\mathscr{B}$ is a coherent sheaf of rings). The same reasoning shows that any quasi-coherent sub-$\mathscr{B}$-module (resp. quotient $\mathscr{B}$-module) of $\mathscr{F}$ is of finite type, whence the second part of the corollary. □

Proposition 22.2.29. *Let X be a locally Noetherian scheme and E be a subset of X. Any point $x \in E$ admits in E a maximal generalization y (i.e. y has no further generalization in Y). In particular, if $E \neq \varnothing$, there exists a maximal element $y \in E$ under generalization.*

Proof. The generalizations of x in X lie in the points of $\mathrm{Spec}(\mathcal{O}_{X,x})$ (Corollary 22.2.10), where $\mathcal{O}_{X,x}$ is a Noetherian local ring. We then know that the lengths of chains of prime ideals in this ring are bounded by $\dim(\mathcal{O}_{X,x})$, and to prove the proposition it suffices to consider a chain of prime ideals belonging to E and having the greatest possible length. □

Proposition 22.2.30. *Let X be a scheme. Then the following conditions are equivalent:*

(i) $X = \mathrm{Spec}(A)$ *is affine and A is Artinian;*

(ii) X is Noetherian and has discrete underlying space;

(iii) X is Noetherian and every point in X is closed (in other words, X is T1).

If these equivalent conditions hold, then X is finite and the ring A is a direct product of finitely many Artinian local rings.

Proof. We know that (i) implies the last asserion. It is clear that (i)⇒(ii)⇒(iii). To see that (iii) implies (i), let us first show that X is then finite; we can indeed reduce to case where X is affine, and we know that a Noetherian ring of which all the prime ideals are maximal is Artinian, hence our assertion. □

Note that a Noetherian scheme can have an underlying space finite without being artinian, as shown by the example of a spectrum discrete valuation ring.

22.3 Product of schemes

Let (X_α) be a family of schemes, and X be the topological space which is the **coproduct** of the underlying spaces of X. Then X is the union of its open subspaces U_α, and for each α we have a embedding $\iota_\alpha : X_\alpha \to X$ with image equal to U_α. If we endow each U_α the sheaf $(\iota_\alpha)_*(\mathcal{O}_{X_\alpha})$, it is clear that X becomes a scheme, which we will call the **coproduct** of the family (X_α), and denote by $\coprod_\alpha X_\alpha$. It is clear that the scheme X satisfies the universal property of coproducts of X_α's: for any scheme Y and morphisms $f_\alpha : X_\alpha \to Y$, there exists a unique morphism $f : X \to Y$ such that $f \circ \iota_\alpha = f_\alpha$. In other words, we have a functorial bijection

$$\mathrm{Hom}(\coprod_\alpha X_\alpha, Y) \to \prod_\alpha \mathrm{Hom}(X_\alpha, Y).$$

This fact can be also stated that $\coprod_\alpha X_\alpha$ represents the covariant functor $\prod_\alpha \mathrm{Hom}(X_\alpha, -)$ on the category of schemes. In particular, if X_α are S-schemes with structural morphisms ψ_α, then X is an S-scheme with structural morphism $\psi : X \to S$ such that $\psi \circ \iota_\alpha = \psi_\alpha$. We usually denote the coproduct of two schemes X and Y by $X \amalg Y$, and it is clear that if $X = \mathrm{Spec}(A)$ and $Y = \mathrm{Spec}(B)$, then $X \amalg Y$ is canonically identified with $\mathrm{Spec}(A \times B)$.

In this section, we shall consider product of schemes, which is far more complicated than coproducts. We will see that fiber products plays a central role of many construction and operations on schemes.

22.3.1 Product of schemes

Let X and Y be S-schemes. Recall that the object $X \times_S Y$ represents by definition the contravariant functor

$$T \mapsto F(T) = \mathrm{Hom}_S(T, X) \times \mathrm{Hom}_S(T, Y)$$

on the category of S-schemes. To prove the existence of $X \times_S Y$, we shall apply the methods used in Proposition 19.3.5. We first verify condition (ii) in Proposition 19.3.5, which means F is a sheaf over the category **Sch**: this is evident since the functors $T \mapsto \mathrm{Hom}_S(T, X)$ and $T \mapsto \mathrm{Hom}_S(T, Y)$ are sheaves, and a projective limit of sheaves over **Sch** is again a sheaf over **Sch**.

This already allows us to bring ourselves back to the case that the scheme S is affine. In fact, let (S_α) is a covering of S by affine open sets. In view of the above fact and of **??**, it suffices to show that each of the functors $F \times_{h_S} h_{S_\alpha}$ is representable. On the other hand, let $\varphi : X \to S$ and $\psi : Y \to S$ be the structural morphisms; it is immediate that when T is a locally ringed S_α-space (hence also an S-space), we have canonical identifies

$$\mathrm{Hom}_S(T, X) \xrightarrow{\sim} \mathrm{Hom}_{S_\alpha}(T, \varphi^{-1}(S_\alpha)), \quad \mathrm{Hom}_S(T, Y) \xrightarrow{\sim} \mathrm{Hom}_{S_\alpha}(T, \psi^{-1}(S_\alpha)).$$

Therefore, in view of **??**, we only need to show that F is representable when it is restricted to the subcategory of locally ringed S_α-spaces.

With these being done, assume that S is affine and consider a covering (X_λ) (resp. (Y_μ)) of X (resp. Y) by affine opens. We shall verify the conditions (i) and (iii) of Proposition 19.3.5 for the subfunctors $F_{\lambda\mu} : T \mapsto \mathrm{Hom}_S(T, X_\lambda) \times \mathrm{Hom}_S(T, Y_\mu)$ of F. Let Z be a locally ringed S-space and (p, q) be an element of $F(Z)$, i.e. $p : Z \to X$ and $q : Z \to Y$ are S-morphisms. These determine by Yoneda Lemma a natural transform $h_Z \to F$ which associates a locally ringed S-space T the map

$$\mathrm{Hom}_S(T, Z) \to F(T), \quad g \mapsto (p \circ g, q \circ g)$$

and every natural transform $h_Z \to F$ is of this form. We now show that the functor

$$T \mapsto F_{\lambda\mu}(T) \times_{F(T)} h_Z(T) \tag{3.1.1}$$

is representable by a locally ringed S-space induced by Z on an open subset of Z. In fact, an element of the right side of (3.1.1) (which is a fiber product of sets) is a triple (u_λ, v_μ, g), where $g : T \to Z$, $u_\lambda : T \to X_\lambda$, and $v_\mu : T \to Y_\mu$ are S-morphisms such that the following diagram commutes:

$$\begin{tikzcd}
T \arrow[dr, "g"] \arrow[drr, bend left, "v_\mu"] \arrow[ddr, bend right, "u_\lambda"'] & & \\
& Z \arrow[r, "q"] \arrow[d, "p"'] & Y \arrow[d] \\
& X \arrow[r] & S
\end{tikzcd}$$

Now this in particular implies that $g(T) \subseteq Z_{\lambda\mu} = p^{-1}(X_\lambda) \cap q^{-1}(Y_\mu)$, and conversely, any S-morphism $g : T \to Z$ verifying this condition corresponds to the unique triple $(p \circ g, q \circ g, g)$, since $p \circ g$ (resp $q \circ g$) can be viewed as a morphism from Z to X_λ (resp. Y_μ). In other word,

we have a canonical bijection

$$F_{\lambda\mu}(T) \times_{F(T)} \mathrm{Hom}_S(T, Z) \xrightarrow{\sim} \mathrm{Hom}_S(T, Z_{\lambda\mu})$$

and the functor (3.1.1) is then represented by the couple $(Z_{\lambda\mu}, (p|_{Z_{\lambda\mu}}, q|_{Z_{\lambda,\mu}}), j_{\lambda\mu})$, where $j_{\lambda\mu} : Z_{\lambda\mu} \to Z$ is the cannical injection. Since the $Z_{\lambda\mu}$ form an open covering of Z, this proves both of the conditions (i) and (iii) of Proposition 19.3.5.

It remains to show that the functors $F_{\lambda\mu}$ are representable, which means we need to construct $X \times_S Y$ when X, Y, and S are affine schemes. This is fairly easy, as we will now show.

Proposition 22.3.1. *Assume that $S = \mathrm{Spec}(A)$, $X = \mathrm{Spec}(B)$, and $Y = \mathrm{Spec}(C)$, where B and C are A-algebras. Then the scheme $Z = \mathrm{Spec}(B \otimes_A C)$, with p, q the S-morphisms corresponding to the canonical A-homomorphisms $B \to B \otimes_A C$ and $C \to B \otimes_A C$, representes the functor F in the category of locally rinfed S-spaces.*

Proof. In fact, in the category of rings, the tensor product $B \otimes_A C$ of two A-algebras B and C is a coproduct in the category of A-algebras, as can be easily verified. □

We then conclude that fiber products exist in the category of schemes. As always, the notation $X \times_S Y$ will be used to denote this product for two S-schemes X and Y. If $S = \mathrm{Spec}(A)$ is an affine scheme, we also write $X \times_A Y$. If $Y = \mathrm{Spec}(B)$ is an affine scheme, in view of Proposition 22.3.1, we use $X \otimes_S B$ to denote this product, and $X \otimes_A B$ if $S = \mathrm{Spec}(A)$ is also affine.

The general notations and results for fiber products in a category can be then used for the product of schemes. In particular, if $p_1 : X \times_X Y \to X$, $p_2 : X \times_S Y \to Y$ are the canonical projections, and $g : T \to X$, $h : T \to Y$ are two S-morphisms, we denote by $(g, h)_S$ the unique S-morphism fits into the following diagram:

$$\begin{tikzcd}
T \arrow[dr, "(g,h)_S"] \arrow[drr, bend left, "h"] \arrow[ddr, bend right, "g"'] & & \\
& X \times_S Y \arrow[r, "p_2"] \arrow[d, "p_1"'] & Y \arrow[d] \\
& X \arrow[r] & S
\end{tikzcd}$$

If $S = \mathrm{Spec}(A)$, $X = \mathrm{Spec}(B)$, $Y = \mathrm{Spec}(C)$, and $T = \mathrm{Spec}(D)$ are all affine, and g, h correspond to homomorphisms $\rho : B \to D$, $\sigma : C \to D$ of A-algebras, then $(g, h)_S$ corresponds to the homomorphism $\tau : B \otimes_A C \to D$ such that

$$\tau(b \otimes c) = \rho(b)\sigma(c).$$

Again, if $S = \mathrm{Spec}(A)$ is affine, we also write $(g, h)_A$ instead of $(g, h)_S$.

Corollary 22.3.2. *Let $Z = X \times_S Y$ be the product of two S-schemes, $p : Z \to X$, $q : Z \to Y$ the canonical projections, φ (resp ψ) the structural morphisms of X (resp. Y). Let U, V be open subsets of X, Y respectively, and W be an open subset of S such that $p(U) \subseteq W$ and $p(V) \subseteq W$. Then the product $U \times_W V$ is canonically identified with the scheme induced by Z on the subset $p^{-1}(V) \cap q^{-1}(W)$ (considered as a U-scheme). Moreover, if $g : T \to X$, $h : T \to Y$ are S-morphisms such that $g(T) \subseteq V$,*

$h(T) \subseteq W$, the U-morphism $(g,h)_S$ is identified with $(g,h)_S$, considered as morphisms from T to $p^{-1}(V) \cap q^{-1}(W)$.

Proof. We first note that, if U is an open set of S and $\varphi : X \to S$, $\psi : Y \to S$ are structural morphisms with images in U, then the fiber product $X \times_S Y$ is identified with $X \times_U Y$. Apply this to V and W, we conclude that $U \times_W V = U \times_W V$. So it suffices to prove that the subscheme $R = p^{-1}(U) \cap q^{-1}(V)$ with its restricted projections to U and V form a product of U and V. For this, we note that if T is an S-scheme, we can identify the S-morphisms $T \to R$ and the S-morphisms $T \to Z$ with image in R. If $g : T \to U$, $h : T \to V$ are two S-morphisms, we can consider them as S-morphisms of T in X and Y respectively, and by hypothesis there is therefore an S-morphism and there is a morphism $f : T \to Z$ such that $g = p \circ f$, $h = q \circ f$. Since $p(f(T)) \subseteq U$ and $q(f(T)) \subseteq V$, we have

$$f(T) \subseteq p^{-1}(U) \cap q^{-1}(V) = W$$

whence our claim. □

Corollary 22.3.3. *Let (X_λ) (resp. (Y_μ)) be a family of S-schemes and X (resp. Y) be their coproduct. Then $X \times_S Y$ is identified with the coproduct of the family $(X_\lambda \times_S Y_\mu)$.*

Proof. In fact, in the notations of Corollary 22.3.2, the underlying space of $X \times_S Y$ is the disjoint union of open sets $p^{-1}(X_\lambda) \cap q^{-1}(Y_\mu)$, and it suffices to apply Corollary 22.3.2. □

Remark 22.3.1. The product of two Noetherian S-schemes need not to be Noetherian, even if they are both spectrum of fields. For example, if k is a nonperfect field of characteristic $p > 0$, the tensor product $A = k^{p^{-\infty}} \otimes_k k^{p^{-\infty}}$ is not a Noetherian ring: in fact, for any integer $n > 0$, there exists $x_n \in k^{p^{-\infty}}$ such that $x_n^{p^n} \in k$ and $x_n^{p^{n-1}} \notin k$. If we consider the element $z_n = 1 \otimes x_n - x_n \otimes 1$ of A, we then have $z_n^{p^n} = 0$, and $z_n^{p^{n-1}} \neq 0$ since 1 and $x_n^{p^{n-1}}$ are linearly independent over k. We then conclude that the nilradical of A is not nilpotent, so A is not Noetherian.

Remark 22.3.2. We should note that the underlying topological space of the fiber product $X \times_S Y$ is not the fiber product of the underlying topological spaces. This can be seen from the tensor product of two fields, which can not be a field.

22.3.2 Base change of schemes

The functor $X \times_S Y$ is covariant in both of its variables, and this follows from the following commutative diagram:

$$\begin{tikzcd} X \times Y \arrow[r, "f\times 1"] \arrow[d] & X' \times Y \arrow[r, "f'\times 1"] \arrow[d] & X'' \times Y \arrow[d] \\ X \arrow[r, "f"] & X' \arrow[r, "f'"] & X'' \end{tikzcd}$$

Proposition 22.3.4. *For any S-scheme X, the first (resp. second) projection $X \times_S S$ (resp. $S \times_S X$) is a functorial isomorphism of $X \times_S S$ (resp. $S \times_S X$) to X, with inverse isomorphism $(1_X, \varphi)_S$ (resp. $(\varphi, 1_X)_S$), where $\varphi : X \to S$ is the structural morphism. We can therefore write*

$$X \times_S S = S \times_S X = X.$$

Proof. It suffices to prove that the triple $(X, 1_X, \varphi)$ form a product of X and S, which is immediate. □

Corollary 22.3.5. *Let X and Y be S-schemes, $\varphi : X \to S$, $\psi : Y \to S$ the structural morphisms. If we identify canonically X with $X \times_S S$ and Y with $S \times_S Y$, the projections $X \times_S Y \to X$ and $X \times_S Y \to Y$ is identified respectively to $1_X \times \psi$ and $\varphi \times 1_Y$.*

We can define similarly the fiber product of S-schemes $X_1, \dots, X_n$, whose existence can be proved by induction on n, which is isomorphic to $(X_1 \times_S \cdots \times_S X_{n-1}) \times_S X_n$. The uniqueness of the product entails, as in any category, its properties of commutativity and associativity. If, for example, p_1, p_2, p_3 denotes the projections of $X_1 \times_S X_2 \times_S X_3$, and if we identify this scheme with $(X_1 \times_S X_2) \times_S X_3$, the projection in $X_1 \times_S X_2$ is identified with $(p_1, p_2)_S$.

Let S, S' be two schemes, $\varphi : S \to S'$ an morphism, making S' an S-scheme. For any S-scheme X, consider the product $X \times_S S'$, and let p and π' the projections to X and S' respectively. Through the morphism π', this product is an S'-scheme, which we may denoted by $X_{(S')}$ or $X_{(\varphi)}$, and the obtained scheme is called the **base change** of X from S to S', or the inverse image of X via φ. We note that if π is the structural morphism of X and θ is the structural morphism of $X \times_S S'$, the following diagram is commutative:

$$\begin{tikzcd} X_{(S')} \arrow[r, "\pi'"] \arrow[d, "p"'] & S' \arrow[d, "\varphi"] \\ X \arrow[r, "\pi"] & S \end{tikzcd}$$

For any S-morphism $f : X \to Y$, we denote by $f_{(S')}$ the S'-morphism $f \times_S 1 : X_{(S')} \to Y_{(S')}$ and call it the inverse image of f by φ. The operation $X_{(S')}$ is clearly a covariant functor on X, from the category $\mathbf{Sch}/S$ to $\mathbf{Sch}/S'$.

Let S, S' be two affine schemes with rings A, A'; a morphism $S' \to S$ corresponds to a homomorphism $A \to A'$. If X is an S-scheme, we then denote by $X_{(A')}$ of $X \otimes_A A'$ by the S'-scheme $X_{(S')}$; if X is also affine with ring B, then $X_{(A')}$ is affine with ring $B_{(A')} = B \otimes_A A'$.

We point out that the scheme $X_{(S')}$ satisfies the following universal property: any S'-scheme T is an S-scheme via the morphism φ, and for any S-morphism $g : T \to X$ there exists a unique S'-morphism $f : T \to X_{(S')}$ such that $g = p \circ f$.

Proposition 22.3.6 (Transitivity). *Let $\varphi' : S'' \to S'$ and $\varphi : S' \to S$ be morphism of schemes. For any S-scheme X, there is a canonical functorial isomorphism of the S''-schemes $(X_{(\varphi)})_{(\varphi')}$ and $X_{(\varphi \circ \varphi')}$.*

Proof. In fact, let T be an S''-scheme, ψ its structural morphism, $g : T \to X$ an S-morphism (T is an S-scheme via the morphism $\varphi \circ \varphi' \circ \psi$). Since T is an S'-scheme with structural morphism $\varphi' \circ \psi$, we can write $g = p \circ g'$, where $g' : T \to X_{(\varphi)}$ is an S'-morphism. Then $g' = p' \circ g''$, where $g'' : T \to (X_{(\varphi)})_{\varphi'}$ is an S''-morphism:

$$\begin{tikzcd} (X_{(\varphi)})_{\varphi'} \arrow[r, "p'"] \arrow[d, "\pi''"] & X_{(\varphi)} \arrow[r, "p"] \arrow[d, "\pi'"] & X \arrow[d, "\pi"] \\ S'' \arrow[r, "\varphi'"] & S' \arrow[r, "\varphi"] & S \end{tikzcd}$$

The claim now follows from the definition of the universal property of $X_{(\varphi \circ \varphi')}$. □

The previous result can also be written as $(X_{(S')})_{(S'')} = X_{(S'')}$, if there is no risk of confusion. Moreover precisely, we have

$$(X \times_S S') \times_{S'} S'' = X \times_S S'';$$

the functorial of the isomorphism in Proposition 22.3.6 also shows the transitive of inverse image of morphisms:

$$(f_{(S')})_{(S'')} = f_{(S'')}$$

for any S-morphism $f : X \to Y$.

Corollary 22.3.7. *If X and Y are S-schemes, there exists a canonical functorial isomorphism of S'-schemes $X_{(S')} \times_{S'} Y_{(S')}$ and $(X \times_S Y)_{S'}$.*

Proof. In fact, we have, the following canonical isomorphisms:

$$(X \times_S S') \times_{S'} (Y \times_S S') = X \times_S (Y \times_S S') = (X \times_S Y) \times_S S'$$

where we use Proposition 22.3.6 and the associativity of fiber product. □

Again, the functorial isomorphism in Corollary 22.3.7 also gives the isomorphism

$$(u_{(S')}, v_{(S')})_{(S')} = ((u, v)_S)_{S'}$$

for any S-morphisms $u : T \to X$, $v : T \to Y$. In other words, the inverse image functor $X_{(S')}$ commutes on the formation of the products; note that it also commutes to the formation of coproducts.

Corollary 22.3.8. *Let Y be an S-scheme, $f : X \to Y$ a morphism making X a Y-scheme (and also an S-scheme). Then the scheme $X_{(S')}$ is canonically identified with the product $X \times_Y Y_{(S')}$, and the projection $X \times_Y Y_{(S')} \to Y_{(S')}$ is identified with $f_{(S')}$.*

Proof. Let $\psi : Y \to S$ be the structural morphism of Y; we have a commutative diagram

$$\begin{tikzcd}
X_{(S')} \arrow[r, "f_{(S')}"] \arrow[d] & Y_{(S')} \arrow[r, "\psi_{(S')}"] \arrow[d] & S' \arrow[d] \\
X \arrow[r, "f"] & Y \arrow[r, "\psi"] & S
\end{tikzcd}$$

Now $Y_{(S')}$ is identified with $S'_{(\psi)}$, and $X_{(S')}$ with $S'_{(\psi \circ f)}$, so by Proposition 22.3.6 and Proposition 22.3.4, we deduce the corollary. □

Example 22.3.9. Let A be a ring, X an A-scheme, and $\mathfrak{a}$ an ideal of A. Then $X_0 = X \otimes_A (A/\mathfrak{a})$ is an $(A/\mathfrak{a})$-scheme, called the scheme obtained from X by **reduction mod** $\mathfrak{a}$.

Proposition 22.3.10. *Let $f : X \to X'$, $g : Y \to Y'$ be two S-morphisms that are monomorphisms of schemes; then $f \times_S g$ is a monomorphism. In particular, for any extension $S' \to S$ of base scheme, the inverse image $f_{(S')} : X_{(S')} \to Y_{(S')}$ is a monomorphism.*

Proof. In fact, if p, q are the projections of $X \times_S Y$, and p', q' that of $X' \times_S Y'$:

$$\begin{tikzcd}
X \times_S Y \arrow[rr, "q"] \arrow[dr, "f \times_S g"] \arrow[dd, "p"'] & & Y \arrow[d, "g"] \\
& X' \times_S Y' \arrow[r, "q'"] \arrow[d, "p'"] & Y' \arrow[d] \\
X \arrow[r, "f"] & X' \arrow[r] & S
\end{tikzcd}$$

then for any two morphisms $u, v : T \to X \times_S Y$, the relation $(f \times_S g) \circ u = (f \times_S g) \circ v$ implies

$$p' \circ (f \times_S g) \circ u = p' \circ (f \times_S g) \circ v$$

so $f \circ p \circ u = f \circ p \circ v$, and since f is a monomorphism, we conclude $p \circ u = p \circ v$. Similarly, since g is a monomorphism, we have $q \circ u = q \circ v$, whence $u = v$. □

For any S-morphism $f : S' \to X$, the morphism $f' = (f, 1_{S'})_S$ is then an S'-morphism from S' to $X' = X_{(S')}$ such that $p \circ f' = f$, $\pi' \circ f' = 1_{S'}$, which is called an ***S'*-section** of X':

$$\begin{tikzcd}
X' \arrow[r, "\pi'"] \arrow[d, "p"'] & S' \arrow[l, bend right, "f'"'] \arrow[dl, "f"] \arrow[d, "\varphi"] \\
X \arrow[r, "\pi"] & S
\end{tikzcd}$$

Conversely if f' is an S'-section, then $f = p \circ f'$ is an S-morphism $S' \to X$. We then deduce the following canonical correspondence

$$\mathrm{Hom}_S(S', X) \xrightarrow{\sim} \mathrm{Hom}_{S'}(S', X') \tag{3.2.1}$$

The morphism f' is called the **graph** of f, and denoted by Γ_f. A particularly important case is $S' = X$ and $f = 1_X$, where corresponding morphism $X \to X \times_S X$ is called the **diagonal morphism** of X, and denoted by Δ_X. Also, if $f : X \to Y$ is a morphism of schemes, we denote by Δ_f the diagonal map from X to $X \times_Y X$.

Example 22.3.11. Since any scheme X can be considered as a $\mathbb{Z}$-scheme, we can consider the X-sections of $X \otimes_{\mathbb{Z}} \mathbb{Z}[T]$ (where T is an indeterminate) corresponding to the $\mathbb{Z}$-morphisms $X \to \mathrm{Spec}(\mathbb{Z}[T])$. We claim that such X-sections correspond to sections of the structural sheaf $\mathscr{O}_X$ of X. In fact, the morphisms $X \to \mathrm{Spec}(\mathbb{Z}[T])$ correspond to ring homomorphisms $\mathbb{Z}[T] \to \Gamma(X, \mathscr{O}_X)$, which in turn are entirely determined by the image of T, and can be an arbitrary element of $\Gamma(X, \mathscr{O}_X)$, whence our assertion.

22.3.3 Tensor product of quasi-coherent sheaves

Let S be a scheme, X, Y be two S-schemes, $Z = X \times_S Y$, and p, q be the projections of Z to X and Y, respectively. Let $\mathscr{F}$ (resp. $\mathscr{G}$) be an $\mathscr{O}_X$-module (resp. an $\mathscr{O}_Y$-module). Then the tensor product $p^*(\mathscr{F}) \otimes_{\mathscr{O}_Z} q^*(\mathscr{G})$ is called the **tensor product of $\mathscr{F}$ and $\mathscr{G}$ over $\mathscr{O}_S$** (or **over *S***)

and denoted by $\mathscr{F} \otimes_{\mathscr{O}_S} \mathscr{G}$ (or $\mathscr{F} \otimes_S \mathscr{G}$). More generaly, if $(X_i)_{1 \leq i \leq n}$ is a finite family of S-schemes and for each i, $\mathscr{F}_i$ is an $\mathscr{O}_X$-module, we can define the tensor product $\mathscr{F}_1 \otimes_S \cdots \otimes_S \mathscr{F}_n$ over the scheme $Z = X_1 \times_S \cdots \times_S X_n$. This is a quasi-coherent $\mathscr{O}_Z$-module if each $\mathscr{F}_i$ is quasi-coherent (Corollary 22.2.20), and is coherent if each $\mathscr{F}_i$ is coherent and Z is locally Noetherian in view of Proposition 19.4.26.

We note that if $X = Y = S$, the above definition coincide with the usual one of tensor product of $\mathscr{O}_S$-modules. Moreover, as $q^*(\mathscr{O}_Y) = \mathscr{O}_{X \times_S Y}$, the product $\mathscr{F} \otimes_S \mathscr{O}_Y$ is canonically identified with $p^*(\mathscr{F})$, and similarly $\mathscr{O}_X \otimes_S \mathscr{G}$ is identified with $q^*(\mathscr{G})$. In particular, if $Y = S$ and $f : X \to Y$ is the structural morphism, then $\mathscr{O}_X \otimes_Y \mathscr{G} = f^*(\mathscr{G})$: the ordinary tensor product and the inverse image therefore appears as a special case of the general tensor product. We also note that if X and Y are fixed, the operation $\mathscr{F} \otimes_S \mathscr{G}$ is a covariant bifunctor and is right exact on $\mathscr{F}$ and $\mathscr{G}$.

Proposition 22.3.12. *Let S, X, Y be affine schemes with rings A, B, C, respectively, where B, C are A-algebras. Let M (resp. B) be a B-module (resp. C-module) and $\mathscr{F} = \widetilde{M}$ (resp. $\mathscr{G} = \widetilde{N}$) the associated quasi-coherent sheaf. Then $\mathscr{F} \otimes_S \mathscr{G}$ is canonically isomorphic to the sheaf associated with the $(B \otimes_A C)$-module $M \otimes_A N$.*

Proof. In fact, in view of Proposition 22.1.13 and Corollary 22.1.9, $\mathscr{F} \otimes_S \mathscr{G}$ is canonically isomorphic to the sheaf associated with the $(B \otimes_A C)$-module

$$(M \otimes_B (B \otimes_A C)) \otimes_{B \otimes_A C} ((B \otimes_A C) \otimes_C N)$$

and due to the canonical isomorphisms between tensor products, the latter is isomorphic to $M \otimes_B (B \otimes_A C) \otimes_C N = (M \otimes_B B) \otimes_A (C \otimes_C N) = M \otimes_A N$. □

Proposition 22.3.13. *Let $f : T \to X$, $g : T \to Y$ be two S-morphisms, and $\mathscr{F}$ (resp. $\mathscr{G}$) be an $\mathscr{O}_X$-module (resp. $\mathscr{O}_Y$-module). Then we have $(f, g)_S^*(\mathscr{F} \otimes_S \mathscr{G}) = f^*(\mathscr{F}) \otimes_{\mathscr{O}_T} g^*(\mathscr{G})$.*

Proof. If p, q are the projections of $X \times_S Y$, the assertion follows from the relations $(f, g)_S^* \circ p^* = f^*$ and $(f, g)_S^* \circ q^* = g^*$, and the fact that the inverse image operation commutes with tensor products. □

Corollary 22.3.14. *Let $f : X \to X'$, $g : Y \to Y'$ be two S-schemes and $\mathscr{F}'$ (resp. $\mathscr{G}'$) be an $\mathscr{O}_{X'}$-module (resp. $\mathscr{O}_{Y'}$-module). Then $(f \times_S g)^*(\mathscr{F}' \otimes_S \mathscr{G}') = f^*(\mathscr{F}') \otimes_S g^*(\mathscr{G}')$.*

Proof. This follows from Proposition 22.3.13 and the fact that $f \times_S g = (f \circ p, g \circ q)_S$, where p, q are the projections of $X \times_S Y$. □

Corollary 22.3.15. *Let X, Y, Z be S-schemes and $\mathscr{F}$ (resp. $\mathscr{G}, \mathscr{H}$) be an $\mathscr{O}_X$-module (resp. $\mathscr{O}_Y$-module, $\mathscr{O}_Z$-module). Then the sheaf $\mathscr{F} \otimes_S \mathscr{G} \otimes_S \mathscr{H}$ is the inverse image of $(\mathscr{F} \otimes_S \mathscr{G} \otimes_S \mathscr{H})$ under the canonical isomorphism $X \times_S Y \times_S Z \to (X \times_S Y) \times_S Z$, and $\mathscr{G} \otimes_S \mathscr{F}$ is the inverse image of $\mathscr{F} \otimes_S \mathscr{G}$ under the canonical isomorphism $X \times_S \to Y \times_S X$.*

Proof. The first isomorphism is $(p_1, p_2)_S \times_S p_3$, where p_1, p_2, p_3 are the projections of $X \times_S Y \times_S Z$, and second one is similarly. □

Corollary 22.3.16. *If X is an S-scheme, any $\mathscr{O}_X$-module $\mathscr{F}$ is the inverse image of $\mathscr{F} \otimes_S \mathscr{O}_S$ under the canonical isomorphism from X to $X \times_S S$.*

Let X be an S-scheme, $\mathscr{F}$ be an $\mathscr{O}_X$-module, and $\varphi : S' \to S$ be an morphism. We denote by $\mathscr{F}_{(\varphi)}$ or $\mathscr{F}_{(S')}$ the sheaf $\mathscr{F} \otimes_S \mathscr{O}_{S'}$ over $X \times_S S' = X_{(\varphi)} = X_{(S')}$, so $\mathscr{F}_{(S')} = p^*(\mathscr{F})$, where p is the projection $X_{(S')} \to X$.

Proposition 22.3.17. *Let $\varphi' : S'' \to S'$ be a morphism. For any $\mathscr{O}_X$-module $\mathscr{F}$ over the S-scheme X, $(\mathscr{F}_{(\varphi)})_{(\varphi')}$ is the inverse image of $\mathscr{F}_{(\varphi\circ\varphi)}$ under the canonical isomorphism $(X_{(\varphi)})_{(\varphi')} \to X_{(\varphi\circ\varphi')}$.*

Proof. This follows from the definition and the associativity of base change, since $(\mathscr{F} \otimes_S \mathscr{O}_{S'}) \otimes_{S'} \mathscr{O}_{S''} = \mathscr{F} \otimes_S \mathscr{O}_{S''}$. □

Proposition 22.3.18. *Let Y be an S-scheme and $f : X \to Y$ be an S-morphism. For any $\mathscr{O}_Y$-module $\mathscr{G}$ and any morphism $S' \to S$, we have $(f_{(S')})^*(\mathscr{G}_{(S')}) = (f^*(\mathscr{G}))_{(S')}$.*

Proof. This follows from the diagram

$$\begin{tikzcd} X_{(S')} \arrow[r, "f_{(S')}"] \arrow[d] & Y_{(S')} \arrow[d] \\ X \arrow[r, "f"] & Y \end{tikzcd}$$

and the functoriality of inverse images. □

Corollary 22.3.19. *Let X, Y be S-schemes and $\mathscr{F}$ (resp. $\mathscr{G}$) be an $\mathscr{O}_X$-module (resp. $\mathscr{O}_Y$-module). For any morphism $S' \to S$, the inverse image of the sheaf $(\mathscr{F}_{(S')}) \otimes_{S'} (\mathscr{G}_{(S')})$ under the canonical isomorphism $(X \times_S Y)_{(S')} \cong (X_{(S')}) \times_{S'} (Y_{(S')})$ is equal to $(\mathscr{F} \otimes_S \mathscr{G})_{(S')}$.*

Proof. If p, q are the projections of $X \times_S Y$, the isomorphism is given by $(p_{(S')}, q_{(S')})'_S$, so the corollary follows from Proposition 22.3.13 and Proposition 22.3.18. □

Proposition 22.3.20. *Let X, Y be two S-schemes and $\mathscr{F}$ (resp. $\mathscr{G}$) be an $\mathscr{O}_X$-module (resp. $\mathscr{O}_Y$-module). Let p, q be the projections of $Z = X \times_S Y$, z be a point of Z, and put $x = p(z)$, $y = q(z)$. Then the stalk $(\mathscr{F} \otimes_S \mathscr{G})_z$ is isomorphic to $(\mathscr{F}_x \otimes_{\mathscr{O}_{X,x}} \mathscr{O}_{Z,z}) \otimes_{\mathscr{O}_{Z,z}} (\mathscr{G}_y \otimes_{\mathscr{O}_{Y,y}} \mathscr{O}_{Z,z}) = \mathscr{F}_x \otimes_{\mathscr{O}_{X,x}} \mathscr{O}_{Z,z} \otimes_{\mathscr{O}_{Y,y}} \mathscr{G}_y$.*

Proof. Since the question is local, we can reduce to the affine case, and the assertion follows from Corollary 22.1.9. □

Corollary 22.3.21. *With the notations in Proposition 22.3.20, if $\mathscr{F}$ and $\mathscr{G}$ are of finite type, then*

$$\operatorname{supp}(\mathscr{F} \otimes_S \mathscr{G}) = p^{-1}(\operatorname{supp}(\mathscr{F})) \cap q^{-1}(\operatorname{supp}(\mathscr{G})).$$

Proof. As $p^*(\mathscr{F})$ and $q^*(\mathscr{G})$ are of finite type over $\mathscr{O}_Z$, in view of Proposition 22.3.20 and Proposition 10.4.37, we can reduce to the case $\mathscr{G} = \mathscr{O}_Y$, and the assertion then follows from the formula $\operatorname{supp}(p^{-1}(\mathscr{F})) = p^{-1}(\operatorname{supp}(\mathscr{F}))$. □

22.3.4 Scheme valued points

Let X be a scheme; for any scheme T, we denote by $X(T)$ the set $\operatorname{Hom}(T, X)$ of morphisms from T to X, and the elements of this set will be called **points of X with values in T**. The operation $T \mapsto X(T)$ is then a contravariant functor from the category of schemes to that of sets (in one word, we identify the scheme X with the induced functor h_X on **Sch**). Moreover,

any morphism $g : X \to Y$ of schemes defines a natural transform $X(T) \to Y(T)$, which send $v \in X(T)$ to $g \circ v \in Y(T)$. The product of two S-schemes X and Y is then defined by the canonical isomorphism

$$(X \times_S Y)(T) \xrightarrow{\sim} X(T) \times_{S(T)} Y(T) \tag{3.4.1}$$

where the maps $X(T) \to S(T)$ and $Y(T) \to S(T)$ corresponds to the structural morphisms $X \to S$ and $Y \to S$.

If we are given a scheme S and consider S-schemes and S-morphisms, we denote by $X(T)_S$ the set $\mathrm{Hom}_S(T, X)$ of S-morphisms $T \to X$, and omit the index S if there is no risk of confusion. We also say the elements of $X(T)_S$ are the (S-)points of the S-scheme X with values in the S-scheme T. In particular, an S-section of X is none other than a point of X with values in S. The formula (3.4.1) is then written as

$$(X \times_S Y)(T)_S = X(T)_S \times Y(T)_S;$$

more generally, if Z is an S-scheme, X, Y, T are Z-schemes, we have

$$(X \times_Z Y)(T)_S = X(T)_S \times_{Z(T)_S} Y(T)_S.$$

We remark that for any morphism $S' \to S$, the set $X(S')_S = \mathrm{Hom}_S(S', X)$ is identified with the set $\mathrm{Hom}_{S'}(S', X')$, where $X' = X \times_S S'$, which is the set of S'-sections of X'.

In T (resp. S) is an affine scheme with ring B (resp. A), we replace T (resp. S) by B (resp. A) in the above notations, and we then refer points of X with values in the ring B, or points of the A-scheme X with values in the A-algebra B for the elements $X(B)$ of $X(B)_A$, respectively. We also call $X(T)_A$ the set of points of the A-scheme X with values in the A-scheme T.

Consider in particular the case where T is a local scheme $\mathrm{Spec}(A)$, where A is a local ring; the elements $X(A)$ corresponds to local homomorphisms $\mathscr{O}_{X,x} \to A$ for $x \in X$ (Corollary 22.2.13); we say the point x of the underlying topological space X is the **locality** of the point of X with values in A to which it corresponds (of course, several distinct points of X with values in A can have the same locality), or that the point of X with values in A which corresponds to x is **localizaed in x**.

Even more particularly, a point of X with values in a field K correspond to a point $x \in X$ and a field extension $\kappa(x) \to K$. If X is an S-scheme, saying that $S' = \mathrm{Spec}(K)$ is an S-scheme means K is an extension of the residue field $\kappa(s)$ for an point $s \in S$; an element of $X(K)_S$, which is called **a point of X lying over s with values in K**, corresponds then to a $\kappa(s)$-homomorphism $\kappa(x) \to K$, where x is a point of the topological space X lying over s (hence $\kappa(x)$ is an extension of $\kappa(s)$).

The points of X with values in an algebraically closed field K are called **geometric points** of the scheme X;[2] the field K is called the **value field** of the geometric point. If X is an S-scheme and s is an point of S, a **geometric point of X lying over s** is then a geometric point of X localizaed in a point of X lying over s. We then have a map $X(K) \to X$, which send a geometric point with values in K to the point it locates.

If $S = \mathrm{Spec}(k)$ is the spectrum of a field k and X is an S-scheme, the S-points of X with val-

[2]This terminology is also sometimes used when K is only separably closed, but at that time we will explicitly clarify which convention we adapt.

ues in k is identified with the S-sections of X, or with the points x of X such that the canonical homomorphism $k \to \kappa(x)$ is an isomorphism since only at such a point there exists a homomorphism $\kappa(x) \to k$ such that the composition $k \to \kappa(x) \to k$ is the identity. Such points are called the **rational points** over k of the k-scheme X. Note that if k' is an extension of k, the points of X with values in k' correspond to the points of $X' = X_{(k')}$ rational over k' (cf. (3.2.1)).

The example $X = \mathrm{Spec}(K)$, where K is an nontrivial extension of k, shows that there do not necessarily exist in X rational points on k, even if X is nonempty. Still assuming that X is a k-scheme. For any point $x \in X$, there is always an extensions k' of k for which there is a point x' of $X' = X_{(k')}$ rational over k' and whose image by the canonical projection $X' \to X$ is x: it suffices to take for k' an extension of $\kappa(x)$, the k-monomorphism $\kappa(x) \to k'$ giving the sought point x'. When we thus passes from a point x to a rational point $x' \in X'$ over k' and above x, we say that we "make x rational".

Proposition 22.3.22. *Let $S = \mathrm{Spec}(k)$ be the specturm of a field k, and X be an S-scheme. Then the points of X rational over k are closed in X.*

Proof. In fact, it suffices to show that the point x is closed in any open affine open set containing x, so we may assume that $X = \mathrm{Spec}(A)$ is affine. In this case, since the composition homomorphism $k \to A \to \kappa(x)$ is an isomorphism (we know that $\kappa(x) = k$), we conclude in particular that $A/\mathfrak{p}_x \to k$ is an integral extension, which implies that $A/\mathfrak{p}_x$ is a field (Proposition 13.1.62). □

Proposition 22.3.23. *Let $(X_i)_{1\leq i\leq n}$ be S-schemes, s a point of X, and x_i a point of X_i lying over s for each i. For there to be a point y of the scheme $Y = X_1 \times_S \cdots \times_S X_n$ whose projections on X_i is x_i, it is necessary and sufficient that the x_i are over the same point s of S.*

Proof. This condition is clearly necessary. Now let s be an element of S and x_i a point of X_i lying over s. Then there exist $\kappa(s)$-homomorphisms $\kappa(x_i) \to K$ where K is a common field. The composition $\kappa(s) \to \kappa(x_i) \to K$ are all identical, so the morphisms $\mathrm{Spec}(K) \to X_i$ corresponding to $\kappa(x_i) \to K$ are S-morphisms, and we conclude that they define a unique morphism $\mathrm{Spec}(K) \to Y$. If y is the corresponding point of Y, it is clear that its projection into each of the X_i is x_i. □

In other words, if we denote by (X) the set underlying X, we see that we have a canonical surjective map $(X \times_S Y) \to (X) \times_{(S)} (Y)$; we have already pointed that this maps is not injective in general; that is, there can be multiple points distinct in $X \times_S Y$ having same projections to X and Y.

Corollary 22.3.24. *Let $f : X \to Y$ be an S-morphism, $f_{(S')} : X_{(S')} \to Y_{(S')}$ the S'-morphism induced by a base change $S' \to S$. Let p (resp. q) be the projection $X_{(S')} \to X$ (resp. $Y_{(S')} \to Y$); for any subset V of X, we have*

$$q^{-1}(f(M)) = f_{(S')}(p^{-1}(M)).$$

Proof. By Corollary 22.3.8, $X_{(S')}$ is identified with the product $X \times_Y Y_{(S')}$ and we have the following commutative diagram

$$\begin{tikzcd} X_{(S')} \arrow[r, "f_{(S')}"] \arrow[d, "p"'] & Y_{(S')} \arrow[d, "q"] \\ X \arrow[r, "f"] & Y \end{tikzcd}$$

By Proposition 22.3.23, the relation $q(y') = f(x)$ for $x \in V$, $y' \in Y_{(S')}$ is equivalent to the existence of a point $x' \in X_{(S')}$ such that $p(x') = x$ and $f_{(S')}(x') = y'$, whence the corollary. □

Proposition 22.3.25. *Let X, Y be S-schemes and $x \in X$, $y \in Y$ two points that are over the same point $s \in S$. The set of points $X \times_S Y$ having projections x and y is in canonical one-to-one correspondence with the set of types of the composition extension of $\kappa(x)$ and $\kappa(y)$, considered as extensions of $\kappa(s)$.*

Proof. Let p (resp. q) be the projection of $X \times_S Y$ to X (resp. Y) and let E be the subspace $p^{-1}(x) \cap q^{-1}(y)$ of the underlying topological space of $X \times_S Y$. We first note that since x and y are lying over s, the morphisms $\operatorname{Spec}(\kappa(x)) \to S$ and $\operatorname{Spec}(\kappa(y)) \to S$ factor through $\operatorname{Spec}(\kappa(s))$:

$$\begin{tikzcd}
 & \operatorname{Spec}(\kappa(x)) \arrow[d] & \\
\operatorname{Spec}(\kappa(y)) \arrow[r] & \operatorname{Spec}(\kappa(s)) \arrow[r] & S
\end{tikzcd}$$

since $\operatorname{Spec}(\kappa(s)) \to S$ is a monomorphism by Corollary 22.2.16, it follows immediately that we have

$$P = \operatorname{Spec}(\kappa(x)) \times_S \operatorname{Spec}(\kappa(y)) = \operatorname{Spec}(\kappa(x)) \times_{\operatorname{Spec}(\kappa(s))} \operatorname{Spec}(\kappa(y)) = \operatorname{Spec}(\kappa(x) \otimes_{\kappa(s)} \kappa(y)).$$

Let $i : \operatorname{Spec}(\kappa(x)) \to X$ and $j : \operatorname{Spec}(\kappa(y)) \to Y$ be the canonical morphisms, we put $\alpha = i \times_S j : P \to E$ to be the map on the underlying topological space. On the other hand, any point $z \in E$ defines two $\kappa(s)$-homomorphisms $\kappa(x) \to \kappa(z)$ and $\kappa(y) \to \kappa(z)$, hence a $\kappa(s)$-homomorphism $\kappa(x) \otimes_{\kappa(s)} \kappa(y) \to \kappa(z)$, which corresponds to a morphism $\operatorname{Spec}(\kappa(z)) \to P$; we take $\beta(z)$ to be the image of this morphism, which defines a map $\beta : E \to P$.

To verify that $\alpha \circ \beta$ and $\beta \circ \alpha$ are identity maps, we need the following commutative diagram

$$\begin{tikzcd}
\operatorname{Spec}(\kappa(z)) \arrow[dr] \arrow[drr, bend left] \arrow[ddr, bend right] & & & \\
 & P \arrow[r] \arrow[d] \arrow[dr, "\alpha"] & \operatorname{Spec}(\kappa(y)) \arrow[dr, "j"] & \\
 & \operatorname{Spec}(\kappa(x)) \arrow[dr, "i"'] & E \arrow[r] \arrow[d] & Y \arrow[d] \\
 & & X \arrow[r] & S
\end{tikzcd}$$

for $z \in E$. By the uniqueness part of the universal property of fiber products, the canonical morphism $\operatorname{Spec}(\kappa(z)) \to E$ induced by $\operatorname{Spec}(\kappa(z)) \to X$ and $\operatorname{Spec}(\kappa(z)) \to Y$ is given by the composition $\operatorname{Spec}(\kappa(z)) \to P \to E$, and also equal to the canonical morphism $\operatorname{Spec}(\kappa(z)) \to E$ of the scheme $X \times_S Y$ at z (Corollary 22.2.15). This means the image of $\beta(z)$ under α is exactly the image of the canonical morphism $\operatorname{Spec}(\kappa(z)) \to E$, which is just z; this shows $\alpha \circ \beta = 1_E$. As for $\beta \circ \alpha$, we just note that if $z = \alpha(\mathfrak{p})$ for some $\mathfrak{p} \in P$ (a prime ideal), then the morphism α induces a field extensins $\kappa(z) \to \kappa(\mathfrak{p})$, which corresponds to morphism $\operatorname{Spec}(\kappa(\mathfrak{p})) \to \operatorname{Spec}(\kappa(z))$. Again by the uniqueness part of the fiber product P, we conclude that the canonical morphism $\operatorname{Spec}(\kappa(\mathfrak{p})) \to P$ factors through $\operatorname{Spec}(\kappa(z))$, which means $\beta(z) = \mathfrak{p}$, so $\beta \circ \alpha = 1_P$. Finally, we recall that the set P corresponds to composition fields of $\kappa(x)$ and $\kappa(y)$ over $\kappa(s)$. □

22.3.5 Surjective morphisms

Let $\mathcal{P}$ be a property for morphisms of schemes. We consider the following conditions:

(i) If $f : X \to X'$ and $g : Y \to Y'$ are S-morphisms satisfying $\mathcal{P}$, then $f \times_S g$ also satisfies $\mathcal{P}$.

(ii) If $f : X \to Y$ is an S-morphism satisfying $\mathcal{P}$ and $S' \to S$ is a morphism, then $f_{(S')} : X_{(S')} \to Y_{(S')}$ also satisfies $\mathcal{P}$.

Since $f_{(S')} = f \times_S 1_{S'}$, we see if any identity morphism satisfies $\mathcal{P}$, then (i) implies (ii). On the other hand, since $f \times_S g$ is the following composition

$$X \times_S Y \xrightarrow{f \times 1_Y} X' \times_S Y \xrightarrow{1_{X'} \times g} X' \times_S Y'$$

it is clear that if the composition of two morphisms satisfying $\mathcal{P}$ still satisfies $\mathcal{P}$, then (ii) implies (i) (in this case we say $\mathcal{P}$ is stable under composition). In general, a property $\mathcal{P}$ is called **stable under base change** if it satisfies the condition (ii). For example Proposition 22.3.10 just says that being a monomorphism is stable under base change. On the other hand, if $\mathcal{P}$ is an arbitrary property of morphisms, we say a morphism $f : X \to S$ **satisfies $\mathcal{P}$ universally** (or is **universally $\mathcal{P}$**), if for any morphism $S' \to S$ the inverse image $f_{(S')}$ satisfies $\mathcal{P}$.

Our first application of the above definition is that surjectivity is stable under base change:

Proposition 22.3.26. *Surjective morphisms of schemes are stable under base change.*

Proof. Note that it is clear that surjectivity is stable under composition, in fact we have the both conditions (i) and (ii) described above. But condition (ii) follows from Corollary 22.3.24 by setting $V = X$. □

Proposition 22.3.27. *For a morphism $f : X \to Y$ of schemes to be surjective, it is necessary and sufficient that for any field K and any morphism* $\mathrm{Spec}(K) \to Y$*, there exists an extension K' of K and a morphism* $\mathrm{Spec}(K') \to X$ *fitting into the following diagram*

$$\begin{tikzcd} \mathrm{Spec}(K') \arrow[r] \arrow[d] & X \arrow[d, "f"] \\ \mathrm{Spec}(K) \arrow[r] & Y \end{tikzcd}$$

Proof. The condition is sufficient, since for any $y \in Y$, we can apply the canonical morphism $\mathrm{Spec}(\kappa(y)) \to Y$ to get a morphism $\mathrm{Spec}(K) \to X$, which gives a inverse image of y in X. Conversely, suppose that f is surjective, and let $y \in T$ be the image of $\mathrm{Spec}(K)$ in Y; there exists $x \in X$ such that $f(x) = y$. Consider the monomorphism $\kappa(y) \to \kappa(x)$ corresponding to f, and take an extension K' of $\kappa(y)$ containing $\kappa(x)$ and K; the morphism $\mathrm{Spec}(K') \to X$ corresponding to $\kappa(x) \to K'$ then satisfies the requirement. □

Corollary 22.3.28. *For a morphism $f : X \to Y$ to be surjective, it is necessary and sufficient that, for any field K, there exist an algebraically closed extension K' of K such that the map $X(K') \to Y(K')$ corresponding to f is surjective.*

Proof. In view of Proposition 22.3.27, this condition is sufficient. Conversely, suppose that f is surjective and let K be a field. If p is the characteristic of K, let us take for K' an algebraically

closed extension of K having over the prime field P a transcendence basis of strictly larger cardinality to the cardinals of all the transcendence bases on P of the residual fields of X and Y having characteristic p. It then remains to see, with the same notations as in Proposition 22.3.27, that any monomorphism $u : \kappa(y) \to K'$ factors into

$$\kappa(y) \xrightarrow{w} \kappa(x) \xrightarrow{v} K'$$

where $w = f^x$. Now, let L a purely transcendental extension of P contained in $\kappa(y)$ and over which $\kappa(y)$ is algebraic; if B is a transcendence basis of L over P, we can complete $w(B)$ into a transcendence basis B' of $\kappa(x)$ on P, and then (due to the assumption made on the trancendence bases of K') define a monomorphism $v_1 : P(B') \to K'$ such that $v_1 \circ (w|_L)$ coincides with $u|_L$. There is also an isomorphism $v_2 = u \circ w^{-1}$ from $w(\kappa(y))$ to $u(\kappa(y))$ such that v_2 and v_1 coincide in $w(L)$; as $w(\kappa(y))$ and $P(B' - w(B))$ are linearly disjoint on $w(L)$, we can extend v_1 and v_2 into a monomorphism v_0 of $M = P(B')(w(\kappa(y)))$ in K'; as K' is algebraically closed and $\kappa(x)$ is algebraic over M, we can finally extend v_0 into the monomorphism $v : \kappa(x) \to K'$, which completes the proof. □

22.3.6 Radical morphisms

Proposition 22.3.29. *Let $f : X \to Y$ be a morphism of schemes. The following conditions are equivalent:*

(i) f is universally injective.

(ii) The map f is injective and for any $x \in X$, the extension $f^x : \kappa(f(x)) \to \kappa(x)$ is purely inseparable.

(iii) For any field K, the map $X(K) \to Y(K)$ corresponding to f is injective.

(iv) For any field K, there exists an algebraically closed extension K' of K such that the map $X(K') \to X(K')$ corresponding to f is injective.

(v) The diagonal morphism $\Delta_f : X \to X \times_Y X$ is surjective.

*The morphism f is called **radical** if it satisfies the above equivalent conditions.*

Proof. It is clear that (i) implies f is injective; on the other hand, if $\kappa(x)$ is not a purely inseparable extension of $\kappa(f(x))$, there exist two distinct $\kappa(f(x))$-monomorphisms $\kappa(x) \to K$ into an algebraically closed extension K of $\kappa(x)$; hence we get two distinct morphisms g_1, g_2 of $\mathrm{Spec}(K)$ to X, whose compositions $f \circ g_1$, $f \circ g_2$ equal to the same morphism $\mathrm{Spec}(K) \to Y$. If we set $Y' = \mathrm{Spec}(K)$, there then would be two distinct Y'-sections of $X_{(Y')}$; since K is a field, the Y'-sections of $X_{(Y')}$ correspond one-to-one to their images (the rational points of $X_{(Y')}$ over K), so $f_{(Y')} : X_{(Y')} \to Y'$ would not be injective, contrary to the assumption.

To show that (ii) implies (iii), we note that by Corollary 22.2.15, (iii) signifies that for any $y \in Y$ and a monomorphism $\kappa(y) \to K$ to a field K, there do not exist two distinct $\kappa(y)$-monomorphisms $\kappa(x_1) \to K$, $\kappa(x_2) \to K$, where x_1, x_2 are both lying over y. Now (ii) implis that if we have two such monomorphisms, they come from the same point x since f is injective; moreover, since $\kappa(x)$ is a purely inseparable extension of $\kappa(y)$, the two monomorphisms $\kappa(x) \to K$ are necessarily equal.

It is clear that (iii) implies (iv). Conversely, suppose that (iv) holds; let K be a field and K' be an algebraically closed extension of K; then the diagram

$$\begin{tikzcd} X(K) \arrow[r, "\alpha"] \arrow[d, "\varphi"] & Y(K) \arrow[d, "\varphi'"] \\ X(K') \arrow[r, "\alpha'"] & Y(K') \end{tikzcd} \tag{3.6.1}$$

is commutative. Since the homomorphism $K \to K'$ is injective, φ is injective by Corollary 22.2.15, and by hypothesis we can choose K' such that α' is also injective. Then α is injective, which shows (iii).

To see that (iv) and (v) are equivalent, we note that, for the morphism Δ_f to be surjective, it is necessary and sufficient that, in view of Corollary 22.3.28, for any field K, there exists an algebraically closed extension K' of K such that the diagonal map

$$X(K') \to (X \times_Y X)(K') = X(K') \times_{Y(K')} X(K')$$

corresponding to Δ_f is surjective. But by the definition of this fiber product, this signifies that the map $X(K') \to Y(K')$ is injective, whence our claim.

Finally, we prove that (iii) implies (i). If (iii) is satisfied, then for any base change $Y' \to Y$, the map

$$(X \times_Y Y')(K) \to Y'(K)$$

is still injective, as we immediately verify by noting that $(X \times_Y Y')(K) = X(K) \times_{Y(K)} Y'(K)$ and that $X(K) \to Y(K)$ is injective. Therefore, it suffices to prove that if $X(K) \to Y(K)$ is injective for any field K, then f is injective. Now if x_1 and x_2 are two points of X such that $f(x_1) = f(x_2) = y$, there then exists a field extension K of $\kappa(y)$ and $\kappa(y)$-monomorphisms $\kappa(x_1) \to K$, $\kappa(x_2) \to K$; the corresponding morphisms u_1, u_2 of $\operatorname{Spec}(K)$ to X are then such that $f \circ u_1 = f \circ u_2$, and by hypothesis this implies $u_1 = u_2$, so $x_1 = x_2$. □

Remark 22.3.3. We then obtain examples of injective morphisms (and even bijective) of schemes but not universally injective: it suffices to take a morphism $\operatorname{Spec}(K) \to \operatorname{Spec}(k)$, where K is a separable extension of k distinct from k.

Corollary 22.3.30. *A monomorphism of schemes $f : X \to Y$ is radical. In particular, if A is a ring, S is a multiplicative subset of A, then the canonical morphism* $\operatorname{Spec}(S^{-1}A) \to \operatorname{Spec}(A)$ *is radical.*

Proof. The first assertion follows from Proposition 22.3.29(iii), and the second from the fact that $\operatorname{Spec}(S^{-1}A) \to \operatorname{Spec}(A)$ is a monomorphism. □

Corollary 22.3.31. *Let $f : X \to Y$ be a radical morphism, $g : Y' \to Y$ a morphism, and $X' = X_{(Y')}$. Then the radical morphism $f_{(Y')}$ is a bijection from the underlying space X' to $g^{-1}(f(X))$. Moreover, for any field K, the set $X'(K)$ is identified with the inverse image in $Y'(K)$ under the map $Y'(K) \to Y(K)$ (corresponding to g) of the subset $X(K)$ of $Y(K)$.*

Proof. The first assertion follows from Proposition 22.3.29(ii) and Corollary 22.3.24; the second one follows from the commutative diagram (3.6.1). □

Proposition 22.3.32. *Let $f : X \to Y$ and $g : Y \to Z$ be two morphism of schemes.*

(a) *If f and g are radical, so is $g \circ f$.*

(b) *Conversely, if $g \circ f$ is radical, so is f.*

Proof. It suffices to apply the functors X, Y, Z on any field K, and use the characterization of Proposition 22.3.29(iii); the verification boils down to set-theoretic issues, which are straightforward. □

Proposition 22.3.33. *Radical morphisms are stable under base changes. In particular, if $f : X \to X'$ and $g : y \to Y'$ are radical S-morphisms, then so is $f \times_S g$.*

Proof. Since radical is equivalently to universally injective, the first assertion is clear. The second one follows from the first one since radical morphisms are stable under composition by Proposition 22.3.32. □

22.3.7 Fibers of morphisms

Proposition 22.3.34. *Let $f : X \to Y$ be a morphism, y be a point of Y, and $\mathfrak{a}_y$ be an ideal of $\mathscr{O}_{Y,y}$. Put $Y' = \operatorname{Spec}(\mathscr{O}_{Y,y}/\mathfrak{a}_y)$, $X' = X \times_Y Y'$, and let $p : X' \to X$ be the canonical projection. Then p is a homeomorphism from X' onto the subspace $f^{-1}(Y')$ of X (where we identify Y' are a subspace of Y, cf. Corollary 22.2.10). Moreover, for any $x' \in X'$, the homomorphism $p^{\#}_{x'} : \mathscr{O}_{X,p(x')} \to \mathscr{O}_{X',x'}$ is surjective with kernel $\mathfrak{a}_y\mathscr{O}_{X,x}$.*

Proof. The morphism $\operatorname{Spec}(\mathscr{O}_{Y,y}/\mathfrak{a}_y) \to Y$ is radical (Proposition 22.3.29), so we conclude from Corollary 22.3.31 that p identifies the space $X' = X \times_Y \operatorname{Spec}(\mathscr{O}_{Y,y}/\mathfrak{a}_y)$ with $f^{-1}(Y')$. It remains to show that p is a homeomorphism and identify its morphism on stalks. Since this question is local, we may assume that $X = \operatorname{Spec}(B)$, $Y = \operatorname{Spec}(A)$, where B is an A-algebra. Then the morphism p corresponds to the homomorphism $1 \otimes \rho : B \to B \otimes_A A'$, where $\rho : A \to A' = A_{\mathfrak{p}_y}/\mathfrak{a}_y$ is the canonical homomorphism. Now any element of $B \otimes_A A'$ is of the form

$$\sum_i b_i \otimes \rho(a_i)/\rho(s) = \rho\Big(\sum_i a_i b_i \otimes 1\Big)(1 \otimes \rho(s))^{-1}$$

where $s \notin \mathfrak{p}_y$, so we can apply Proposition 10.4.20. The assertion on the homomorphism $p^{\#}_{x'}$ also follows from the equality. □

We will mainly use Proposition 22.3.34 for the case $\mathfrak{a}_y = \mathfrak{m}_y$ is the maximal ideal of $\mathscr{O}_{Y,y}$. If there is no confusion, we denote by X_y the $\kappa(y)$-scheme obtained by transporting of scheme structure from $X' = X \otimes_S \kappa(s)$ to $f^{-1}(y)$ via the projection p, and this is always the scheme that will be involved when we speak of the **fiber** $f^{-1}(y)$ of the morphism f as a scheme.

Let X, Y be two S-schemes and $f : X \to Y$ an S-morphism. By the transitivity of base change, we have the canonical isomorphism

$$X_s = X \times_Y Y_s$$

for any $s \in S$; the morphism $f_s : X_s \to Y_s$ induced by f by the base change $Y_s \to Y$ is such that, for any $y \in Y_s$, the fiber $f_s^{-1}(y)$ is identified with the $\kappa(y)$-scheme $f^{-1}(y)$, since the residue field of Y_s at y is the same as that of Y at y, in view of Proposition 22.3.34

Proposition 22.3.35 (Transitivity of Fibers). *Let $f : X \to Y$, $g : Y' \to Y$ be two morphisms; put $X' = X_{(Y')}$ and $f' = f_{(Y')}$. For any $y' \in Y'$, if $y = g(y')$, then the scheme $X'_{y'}$ is canonically isomorphic to $X_y \otimes_{\kappa(y)} \kappa(y')$.*

Proof. In fact, by the transitivity of base change, we have canonical isomorphisms

$$(X \otimes_Y \kappa(y)) \otimes_{\kappa(y)} \kappa(y') \cong X \times_Y \operatorname{Spec}(\kappa(y')) \cong (X \times_Y Y') \otimes_{Y'} \kappa(y')$$

The left one is $X_y \otimes_{\kappa(y)} \kappa(y')$, and the right one is $X'_{y'} \otimes_{Y'} \kappa(y')$, so our assertion follows. □

Proposition 22.3.36. *Let $f : X \to Y$ be a monomorphism of schemes. Then for each $y \in Y$, the fiber X_y is a $\kappa(y)$-scheme which is either empty or $\kappa(y)$-isomorphic to* $\operatorname{Spec}(\kappa(y))$.

Proof. By Proposition 22.3.34, X_y is reduced to a point, and hence affine. The morphism $f_y : X_y \to \operatorname{Spec}(\kappa(y))$ induced by f under base change is still a monomorphism by Proposition 22.3.10. If A is the ring of X_y, this signifies that the homomorphism $A \otimes_{\kappa(y)} A \to A$ which maps $a \times a'$ to aa' is bijective. This clearly implies that $A = \kappa(y)$, since otherwise there exist an element $a \in A$ not contained in $\kappa(y)$ and the image $a \otimes 1$ and $1 \otimes a$ are distinct, but both mapped to a. □

Proposition 22.3.37. *Let $f : X \to Y$ be an S-morphism of S-schemes, $g : S' \to S$ a surjective morphism, and $f' = f_{(S')} : X' = X_{(S')} \to Y' = Y_{(S')}$. Consider the following properties:*

(a) surjective;

(b) injective;

(c) dominant;

(d) finite fiber (as sets);

Then if $\mathcal{P}$ denotes one of the properties above and if f' satisfies $\mathcal{P}$, then so does f.

Proof. Since the projection $Y' \to Y$ is surjective by Proposition 22.3.26, we can, by virtue of Corollary 22.3.8, limiting ourselves to the case where $Y = S$, $Y' = S'$. For any $y' \in Y'$, let $y = g(y')$; we have the transitivity relation $X'_{y'} \cong X_y \otimes_{\kappa(y)} \kappa(y')$ (Proposition 22.3.35). Since the morphism $\operatorname{Spec}(\kappa(y')) \to \operatorname{Spec}(\kappa(y))$ is surjective, so is the projection $X'_{y'} \to X_y$ (Proposition 22.3.26). Thus, if $X'_{y'}$ is nonempty (resp. a singleton, resp. a finite set), the same holds for X_y. Since $S' \to S$ is surjective, this proves (a), (b), and (d). On the other hand, if f' is dominant, so is the composition $g \circ f' = f \circ g'$; but since $g' : X' \to X$ is surjective by Proposition 22.3.26, this implies f is dominant. □

22.3.8 Universally open and universally closed morphisms

Following the usual terminology, we say a morphism $f : X \to Y$ is **universally open** (resp. **universally closed**, resp. a **universal embedding,** resp. a **universal homeomorphism**) if for any base change $Y' \to Y$, the morphism $f_{(Y')} : X_{(Y')} \to Y'$ is open (resp. closed, resp. an embedding, resp. a homeomorphism).

Proposition 22.3.38.

(i) *The composition of two universally open morphisms (resp. universally closed morphisms, resp. two universal embeddings, resp. two universal homeomorphisms) is universally open (resp. universally closed, resp. a universal embedding, resp. a universal homeomorphism).*

(ii) *If $f : X \to X'$, $g : Y \to Y'$ are two universally open (resp. universally closed, resp. two universal embeddings, resp. two universal homeomorphisms) S-morphisms, so is the product $f \times_S g$.*

(iii) *If $f : X \to Y$ is a universally open (resp. universally closed, resp. a universal embedding, resp. a universal homeomorphism) S-morphism, so is $f_{(S')} : X_{(S')} \to Y_{(S')}$ for any base change $S' \to S$.*

(iv) *Let $f : X \to Y$, $g : Y \to Z$ be two morphism such that f is surjective; if $g \circ f$ is universally open (resp. universally closed, resp. a universal embedding, resp. a universal homeomorphism), so is g.*

(v) *Let (U_α) be an open cover of Y. For a morphism $f : X \to Y$ to be universally open (resp. universally closed, resp. a universal embedding, resp. a universal homeomorphism), it is necessary and sufficient that, for each α, the restriction $f_\alpha : f^{-1}(U_\alpha) \to U_\alpha$ is universally open (resp. closed).*

Proof. The assertion (i) follows from definiton, and so does (iii). We have already remareked that (i) and (iii) together imply (ii), since identity morphisms satisfies all the properties mentioned above. To prove (iv), we note that for any morphism $Z' \to Z$, the morphism $f_{(Z')} \to X_{(Z')}$ is surjective, so it suffices to prove that if $g \circ f$ is open (resp. closed, resp. an embedding, resp. a homeomorphism) and f is surjective, then so is g. For the case where $g \circ f$ is open or closed, the fact that g is open or closed result from **??**; for the other two cases, we can limit ourselves to the case $g(f(X)) = g(Y) = Z$, so that $g \circ f$ is a homeomorphism from X to Z. As f is surjective, g is necessarily bijective, and as it is open by the first two cases already shown, g is then a homeomorphism from Y to Z.

Finally, the necessity in (v) follows from (iii) and Corollary 22.3.2. Conversely, suppose the condition in (v) and let $g : Y' \to Y$ be a morphism; then $g^{-1}(U_\alpha) = U'_\alpha$ form an open cover of Y' and if $f' = f_{(Y')}$, the restriction $f'^{-1}(U'_\alpha) \to U'_\alpha$ of f' is none other than $(f_\alpha)_{(U'_\alpha)}$ (Corollary 22.3.2). We can then reduce to proving that f is open (resp. closed, resp. an embedding, resp. a homeomorphism) if each f_α is, which is immediate. □

We recall that openness of a map is a local property, i.e., a map $f : X \to Y$ is open if and only if it is open at every point of X. Simialrly, the property of universally open morphisms is also local. To justify this, we define a morphism $f : X \to Y$ is **universally open at a point** $x \in X$ if for any base change $Y' \to Y$ the morphism $f_{(Y')} : X_{(Y')} \to Y_{(Y')}$ is open at any point x' of X' lying over x.

Proposition 22.3.39. *Let $f : X \to Y$, $g : Y \to Z$ be two morphisms of schemes, x a point of X, and $y = f(x)$.*

(a) *If f is universally open at x and g is universally open at y, then $g \circ f$ is universally open at x. Conversely, if $g \circ f$ is universally open at x, then g is universally open at y.*

(b) *If $f : X \to Y$ is an S-morphism universally open at a point $x \in X$, then for any base change $S' \to S$, the morphism $f_{(S')} : X_{(S')} \to Y_{(S')}$ is universally open at any point of $X_{(S')}$ lying over x.*

Proof. Assertion (b) is an immediate concequence of the definition of universally openness at a point and transitivity of base change. Also, it follows from Corollary 22.3.24 that to prove (a), we may drop the "universally" condition and prove the assertion for openness, which follows from **??**. □

Recall that openness is a local property for maps: a continuous map $f : X \to Y$ is open if and only if it is open at every point of X. Inspired by this, for a morphism $f : X \to Y$ of schemes, we may say f is universally open at a point $x \in X$ if for any base change $Y' \to Y$, the morphism $f_{(Y')} : X' \to Y'$ is open at any point $x' \in X'$ lying over x (where $X' = X_{(Y')}$).

Proposition 22.3.40. *Let $f : X \to Y$ and $g : Y \to Z$ be morphisms of schemes, x be a point of X, and $y = f(x)$.*

(a) If f is universally open at a point x and g is universally open at y, then $g \circ f$ is universally open at x. Conversely, if $g \circ f$ is universally open at x, g is universally open at y.

(b) If f is an S-morphism universally open at a point x, then for any base change $S' \to S$, the morphism $f_{(S')} : X_{(S')} \to Y_{(S')}$ is universally open at any point of $X_{(S')}$ lying over x.

Proof. In fact, (b) is a immediate concequence of (a) and the transitivity of base changes. To prove (a), it suffices to drop the "universal" condition and the result then follows from **??**. □

Proposition 22.3.41. *Let X, Y be two schemes, $f : X \to Y$ be a morphism, and x be a point of X. Let (Y_i) be a locally finite covering of Y by closed subschemes, and suppose that for each i such that $f(x) \in Y_i$, the restriction $f_i : f^{-1}(Y_i) \to Y_i$ of f is an open morphism (resp. universally open) at the point x. Then f is open (resp. universally open) at the point x.*

Proof. The assertion about openness is just **??**. For the universal part, consider a morphism $g : Y' \to Y$ and in Y' the closed subschemes $Y'_i = g^{-1}(Y_i)$ (Proposition 22.4.14), which underlying spaces form a locally finite covering of Y'. If $f' = f_{(Y')} : X_{(Y')} \to Y'$ is the base change of f, the restriction $f'_i : f'^{-1}(Y_i) \to Y'_i$ of f' equals to $(f_i)_{(Y')}$, so we can apply **??** to f'. □

Proposition 22.3.42. *Let $f : X \to Y$ be a morphism of schemes, $(X_i)_{1\le i\le n}$ (resp. $(Y_i)_{1\le i\le n}$) be a finite family of closed subschemes of X (resp. Y), and $j_i : X_i \to X$ (resp. $h_i : Y_i \to Y$) be the canonical injections. Suppose that $(X_i)_{1\le i\le n}$ covers X and for each i there exists a morphism $f_i : X_i \to Y_i$ fitting into the following diagram*

$$\begin{tikzcd} X_i \arrow[r, "f_i"] \arrow[d, "j_i"'] & Y_i \arrow[d, "h_i"] \\ X \arrow[r, "f"] & Y \end{tikzcd}$$

Then for f to be closed (resp. universally closed), it is necessary and sufficient that each f_i is.

Proof. If f is closed, then each f_i is closed since Y_i are closed in Y. Conversely, if the f_i are closed, for any closed subset F of X, we have $f_i(F \cap X_i) = f(F \cap X_i)$ and it closed in Y_i, hence in Y, and as $f(F)$ is the union of $f(F \cap X_i)$, it is therefore closed in Y.

For the case of universally closed morphisms, the condition is necessary because j_i is a closed immersion (hence universally closed, cf. Corollary 22.4.12), and if f is universally closed, so is $f \circ j_i = h_i \circ f_i$. But as h_i is a closed immersion, hence separated (Proposition 22.5.25), it follows that f_i is universally closed (Proposition 22.5.23).

Conversely, suppose that each f_i is universally closed, and consider the scheme Z that is the coproduct of that X_i. Let $u : Z \to X$ be the induced morphism by the j_i's. The restriction of $f \circ u$ to X_i is equal to $f \circ j_i = h_i \circ f$, hence universally closed (Corollary 22.4.12 and Proposition 22.3.38(i)); we then deduce from Corollary 22.3.3 that $f \circ u$ is universally closed. But since u is surjective by hypotheses, we conclude that f is universally closed (Proposition 22.3.38(iv)). □

Remark 22.3.4. If X only have finitely many irreducible components, then we deduce from Proposition 22.3.42 that, to verify a morphism $f : X \to Y$ is closed (resp. universally closed), we can reduce ourselves to doing it for dominant morphisms of integral schemes. In fact, let $(X_i)_{1\leq i\leq n}$ be the reduced subschemes of X with underlying spaces the irreducible components of X (Proposition 22.4.40), which are then integral. Let Y_i be the unique reduced closed subscheme of Y with underlying space $\overline{f(X_i)}$ (Proposition 22.4.40), which iss irreducible (Proposition 4.1.6). If $j_i : X_i \to X$ (resp. $h_i : Y_i \to Y$) is the canonical injection, there then exists a dominant morphism $f_i : X_i \to Y_i$ such that $f \circ g_i = h_i \circ f_i$ (Proposition 22.4.44); we are then in the case of Proposition 22.3.42, so f is closed (resp. universally closed) if and only if each f_i is.

Proposition 22.3.43. *Let X, Y be two S-schemes and $f : X \to Y$ be an S-morphism. For f to be universally closed, it suffices that, for any base change $S' \to S$ where $S' = S \otimes_{\mathbb{Z}} \mathbb{Z}[(T_\lambda)_{\lambda\in I}]$ (denoted by $S[(T_\lambda)_{\lambda\in I}]$), the morphism $f_{(S')} : X_{(S')} \to Y_{(S')}$ is closed.*

Proof. We note that if (S_α) is an open cover of S and Y_α is the inverse image of S_α in Y, it suffices to prove that the restricted morphism $f_\alpha : f^{-1}(Y_\alpha) \to Y_\alpha$ is closed (Proposition 22.3.38(v)). Now the inverse image of S_α in S' is $S_\alpha[(T_\lambda)_{\lambda\in I}] = S'_\alpha$ and $(f_\alpha)_{(S')}$ is the restriction $(f_{(S')})^{-1}(Y'_\alpha) \to Y'_\alpha$ of $f_{(S')}$, where Y'_α is the inverse image of S'_α in $Y_{(S')}$. If the proposition is proved for S_α and f_α, it is then true for S and f. We can then assume that S is affine.

Now let (U_β) be an open covering of Y; for f to be universally closed, it suffices to prove that $f_\beta : f^{-1}(U_\beta) \to U_\beta$ is universally closed for each β (Proposition 22.3.38(v)). Again, the morphism $(f_\beta)_{(S')}$ is the restriction $(f_{(S')})^{-1}(U'_\beta) \to U'_\beta$ of $f_{(S')}$, where $U'_\beta = U_\beta \times_S S'$ is the inverse image of U_β in $Y_{(S')}$. If the proposition is proved for U_β and f_β, it then holds for Y and f. Therefore, we can further assume that Y is affine.

Let us first show that if $f_{(S')}$ is closed for any base change $S' \to S$, then f is universally closed. In fact, any Y-scheme Y' can be considered as an S-scheme, and as the morphism $Y \to S$ is separated (recall that Y and S are assumed to be affine), $X \times_Y Y'$ (resp. $Y \times_Y Y' = Y'$) is identified with a closed subscheme of $X \times_S Y'$ (resp. $Y \times_S Y'$) (Proposition 22.4.11). In the following commutative diagram

$$\begin{tikzcd} X \times_Y Y' \arrow[r, "f\times 1_{Y'}"] \arrow[d] & Y \times_Y Y' = Y' \arrow[d] \\ X \times_S Y' \arrow[r, "f_{(Y')}"] & Y \times_S Y \end{tikzcd}$$

the vertical morphisms are closed immersions, so if $f_{(Y')}$ is a closed morphism, so is $f \times 1_{Y'}$.

It remains to prove that $f_{(S')}$ is closed for arbitrary base change $S' \to S$ if this is ture for $S' = S[(T_\lambda)]$. Now by hypotheses S is affine, and if (S'_γ) is an open covering of S', we see in the same manner as before that for $f_{(S')}$ to be closed, it suffices to prove that $f_{(S'_\gamma)}$ is closed. We can then assume S' to be affine. If $S = \operatorname{Spec}(A)$, we have $S' = \operatorname{Spec}(A')$, where A' is an A-algebra. Let $(t_\lambda)_{\lambda\in I}$ be a generator for A', which means there is a surjective A-homomorphism

$A[(T_\lambda)] \to A'$ identifying A' with $A[(T_\lambda)]/\mathfrak{b}$, where $\mathfrak{b}$ is an ideal. If $S'' = \mathrm{Spec}(A[(T_\lambda)])$, S' is then a closed subscheme of S'', and $X_{(S')}$ (resp. $Y_{(S')}$) is identified with a closed subscheme of $X_{(S'')}$ (resp. $Y_{(S'')}$). The morphism $f_{(S')}$ is the restriction of $f_{(S'')}$ on $X_{(S')}$, and since $f_{(S'')}$ is closed by hypotheses, we conclude that $f_{(S')}$ is closed. This completes the proof. □

22.4 Subschemes and immersions

22.4.1 Subschemes

Proposition 22.4.1. *Let X be a scheme and $\mathscr{I}$ be a quasi-coherent ideal of $\mathscr{O}_X$. The support Y of the sheaf $\mathscr{O}_X/\mathscr{I}$ is then closed, and if $\mathscr{O}_Y$ is the sheaf induced on Y by $\mathscr{O}_Y/\mathscr{I}$, $(Y, \mathscr{O}_Y)$ is a scheme.*

Proof. Since the problem is local, it suffices to consider the affine case and show that Y is closed and $(X, \mathscr{O}_Y)$ is an affine scheme. In fact, if $X = \mathrm{Spec}(A)$, we have $\mathscr{O}_X = \widetilde{A}$ and $\mathscr{I} = \widetilde{\mathfrak{a}}$, where $\mathfrak{a}$ is an ideal of A (Theorem 22.1.20); Y is then equal to the closed subset $V(\mathfrak{a})$ of X and is identified with the spectrum of $B = A/\mathfrak{a}$ (Proposition 10.4.44). Moreover, if $\rho : A \to B = A/\mathfrak{a}$ is the canonical homomorphism, the direct image ${}^a\rho_*(\widetilde{B})$ is canonically identified with the sheaf $\widetilde{A}/\widetilde{\mathfrak{a}} = \mathscr{O}_X/\mathscr{I}$ (Corollary 22.1.6 and Proposition 22.1.11). These complete the proof. □

We say $(Y, \mathscr{O}_Y)$ is the **subscheme of** $(X, \mathscr{O}_X)$ **defined by the quasi-coherent ideal** $\mathscr{I}$. More generally, we say a locally ringed space $(Y, \mathscr{O}_Y)$ is a **subscheme** of a scheme $(X, \mathscr{O}_X)$ if Y is a locally closed subspace of X and if U denote the largest open subset of X containing Y such that Y is open in U (in other words, the complement of $\overline{Y} - Y$, so $U = (X - \overline{Y}) \cup Y$), then $(Y, \mathscr{O}_Y)$ is a subscheme of $(U, \mathscr{O}_X|_U)$ defined by a quasi-coherent ideal of $\mathscr{O}_X|_U$. We say the subscheme $(Y, \mathscr{O}_Y)$ of $(X, \mathscr{O}_X)$ is **closed** if Y is closed in X (in this case $U = X$). It follows from this definition and Proposition 22.4.1 that closed subschemes of X are in one-to-one correspondence with quasi-coherent ideals of $\mathscr{O}_X$, since if two such ideals $\mathscr{I}$, $\mathscr{J}$ have the same support (closed) Y and the sheaf induced by $\mathscr{O}_X/\mathscr{I}$ and $\mathscr{O}_X/\mathscr{J}$ on Y are identical, then $\mathscr{I} = \mathscr{J}$.

Let $(Y, \mathscr{O}_Y)$ be a subscheme of X, U the largest open subset of X containing Y such that Y is closed in U, V an open subset of X contained in U; then $V \cap Y$ is closed in V. Moreover, if Y is defined by the quasi-coherent ideal $\mathscr{I}$ of $\mathscr{O}_X|_U$, then $\mathscr{I}|_V$ is a quasi-coherent ideal of $\mathscr{O}_X|_V$, and it is immediate that the scheme induced by Y over $Y \cap V$ is the closed subscheme of V defined by the ideal $\mathscr{I}|_V$.

In particular, the scheme induced by X over an open subset of X is a subscheme of X; such schemes are called **open subschemes** of X. One should note that a subscheme of X can have the underlying space being an open set U of X without being induced on this open subset by X: it is induced over U by X only if it is defined by the ideal 0 of $\mathscr{O}_X|_U$, and there are in general quasi-coherent ideals $\mathscr{I}$ of $\mathscr{O}_X|_U$ such that $(\mathscr{O}_X|_U)/\mathscr{I}$ have support U but is nonzero.

Proposition 22.4.2. *Let $(Y, \mathscr{O}_Y)$ be a locally ringed space such that Y is a subspace of X and there exists a covering (V_α) of Y by open sets of X such that for each α, $Y \cap V_\alpha$ is closed in V_α and the locally ringed space $(Y_\cap V_\alpha, \mathscr{O}_Y|_{Y\cap V_\alpha})$ is a closed subscheme of the scheme induced over V_α by X. Then $(Y, \mathscr{O}_Y)$ is a subscheme of X.*

Proof. The hypothesis implies that Y is locally closed in X and the largest open set U containing Y and in which Y is closed contains the V_α. We are then reduced to the case $U = X$ and Y is closed in X. We define a quasi-coherent ideal $\mathscr{I}$ of $\mathscr{O}_X$ by letting $\mathscr{I}_{V_\alpha}$ to be the sheaf of ideal

of $\mathcal{O}_X|_{V_\alpha}$ that defines the closed subscheme $(Y \cap V_\alpha, \mathcal{O}_Y|_{Y\cap V_\alpha})$ and for any open set W of X not meeting Y, $\mathcal{I}_W = \mathcal{O}_X|_W$. It is immediately verified that there exists a unique sheaf of ideals $\mathcal{I}$ satisfying these conditions and that it defines the closed subscheme $(Y, \mathcal{O}_Y)$. □

Proposition 22.4.3. *A (closed) subscheme of a (closed) subscheme of X is canonically identified with a (closed) subscheme of X.*

Proof. Since a locally closed subset of a locally closed subset of X is still locally closed in X, it is clear by Proposition 22.4.2 that the question is local and we may assume that X is affine. The proposition then follows from the identification $A/\mathfrak{b}$ and $(A/\mathfrak{a})/(\mathfrak{b}/\mathfrak{a})$ where $\mathfrak{a}, \mathfrak{b}$ are ideals of the ring A such that $\mathfrak{a} \subseteq \mathfrak{b}$. □

Let Y be a subscheme of X and denote by $\iota : Y \to X$ the canonical injection of the underlying space; we know the inverse image $\iota^*(\mathcal{O}_X)$ is the restriction $\mathcal{O}_X|_Y$. If for any $y \in Y$, we denote by ι_y the canonical homomorphism $\mathcal{O}_{X,y} \to \mathcal{O}_{Y,y}$, these homomorphisms are then the restrictions to the stalks of $\mathcal{O}_X$ at the points of Y of a surjective homomorphism of sheaves of rings $\iota^\# : \mathcal{O}_X|_Y \to \mathcal{O}_Y$: it suffices indeed to check it locally on Y, so we can assume that X is affine and Y is a closed subscheme; in this case, if $\mathcal{I}$ is the quasi-coherent ideal of $\mathcal{O}_X$ which defines Y, the ι_y's are nothing but the restrictions to the stalks of the canonical homomorphism $\mathcal{O}_X|_Y \to (\mathcal{O}_X/\mathcal{I})|_Y$. We have therefore defined a monomorphism $j_Y = (\iota, \iota^\#)$ of locally ringed spaces, which is called the **canonical injection morphism**. If $f : X \to Z$ is another morphism of schemes, we say the composition

$$Y \xrightarrow{j_Y} X \xrightarrow{f} Z$$

is the **restriction** of f to the subscheme Y of X.

A subscheme Y of a scheme X is considered as an X-scheme via the canonical injection $j_Y : Y \to X$. Two subschemes Y, Z of X that are X-isomorphic are then necessary identical. In fact, if $u : Y \to Z$ is an X-isomorphism, the relation $j_Y = j_Z \circ u$ shows the underlying spaces of Y and Z are identical. Moreover if $U \supseteq Y$ is an open subset of X such that $Y = Z$ are closed in U, and $\mathcal{I}, \mathcal{J}$ are the ideals of U defining respectively Y and Z, for each $x \in Y$ we then have a commutative diagram

$$\begin{tikzcd} \mathcal{O}_{X,x}/\mathcal{J}_x \arrow[rr, "u_x^\#"] & & \mathcal{O}_{X,x}/\mathcal{I}_x \\ & \mathcal{O}_{X,x} \arrow[ul] \arrow[ur] & \end{tikzcd}$$

Since u is an isomorphism, this implies $\mathcal{I}_x = \mathcal{J}_x$, so $Y = Z$ and $u = 1_Y$.

According to the general definitions, we say a morphism $f : Z \to X$ is **dominated by the canonical injection** $j_Y : Y \to X$ of a subscheme Y of X, if f factors through j_Y:

$$Z \xrightarrow{g} Y \xrightarrow{j_Y} X$$

where g is a morphism of schemes. Since j_Y is a monomorphism, the morphism g is unique.

Proposition 22.4.4. *Let Y be a subscheme of a scheme X and $j : Y \to X$ be the cannical injection. For a morphism $f : Z \to X$ to be dominated by the injection j, it is necessary and sufficient that $f(Z) \subseteq Y$*

and for each $z \in Z$, the homomorphism $f_z^\# : \mathcal{O}_{X,f(z)} \to \mathcal{O}_{Z,z}$ factors through $\mathcal{O}_{Y,f(z)}$ (or equivalently, the kernel of $\mathcal{O}_{X,f(z)} \to \mathcal{O}_{Z,z}$ is contained in that of $\mathcal{O}_{X,f(z)} \to \mathcal{O}_{Y,f(z)}$).

Proof. The condition is cleraly necessary. For the sufficiency, we may assume that Y is a closed subscheme of X, and replace X by an open subset U such that Y is closed in U. Y is then defined by a quasi-coherent ideal $\mathcal{I}$ of $\mathcal{O}_X$. Let $\mathcal{J}$ be the kernel of the homomorphism $f^*(\mathcal{O}_X) \to \mathcal{O}_Z$. In view of the properties of the functor f^*, the hypothesis implies tht for each $z \in Z$ we have $(f^*(\mathcal{I}))_z \subseteq \mathcal{J}_z$, and concequently $f^*(\mathcal{I}) \subseteq \mathcal{J}$. Therefore the homomorphism $f^*(\mathcal{O}_X) \to \mathcal{O}_Z$ factors into

$$f^*(\mathcal{O}_X) \longrightarrow f^*(\mathcal{O}_X)/f^*(\mathcal{I}) = f^*(\mathcal{O}_X/\mathcal{I}) \xrightarrow{\theta_z} \mathcal{O}_Z$$

the first arrow being the canonical homomorphism. Let g be the continuous map of Z in Y coincide with f; it is clear that $g^*(\mathcal{O}_Y) = f^*(\mathcal{O}_X/\mathcal{I})$; on the other hand, for any $z \in Z$, θ_z is obviously a local homomorphism, so $(g, \theta) : Z \to Y$ is a morphism of schemes which satisfies $f = j \circ g$, whence the proposition. □

Corollary 22.4.5. *Let Y and Z be subschemes of X. For the canonical injection $Z \to X$ to be dominated by the injection $Y \to X$, it is necessary and sufficient that Z is a subscheme of Y.*

Due to this corollary, for two subschemes Y, Z of X we write $Y \preceq Z$ if Y is a subscheme of Z. It is clear that this defines an order relation on the set of subschemes of X, since two subschemes Y and Z are identical if $Y \preceq Z$ and $Z \preceq Y$.

22.4.2 Immersions of schemes

We say a morphism $f : Y \to X$ is an **immersion** (resp. a **closed immersion**, resp. an **open immersion**) if it is factorized into

$$Y \xrightarrow{g} Z \xrightarrow{j} X$$

where g is an isomorphism, Z is a subscheme (resp. a closed subscheme, resp. an open subscheme) of X, and j is the canonical injection. The subscheme Z and the isomorphism g are then uniquely determined since two X-isomorphic subschemes are identical. We say $f = i \circ g$ is the **canonical factorization** of the immersion f, and the subscheme Z and the isomorphism g is called **associated** with f. It is clera that an immersion is a monomorphism of schemes (since j is a monomorphism), and a fortiori a radical morphism (Corollary 22.3.30). Also, it is clear from Proposition 22.4.3 that the composition of two immersions (resp. two open immersions, resp. two closed immersions) is an immersion (resp. an open immersion, resp. a closed immersion).

Again, one should note that an immersion $f : Y \to X$ such that $f(Y)$ is a open subset of X, in other words which is an open morphism, is not necessarily an open immersion.

Example 22.4.6. Let X be an affine scheme. Then from the definition of closed subschemes, we see that for a morphism $f : Y \to X$ to be a closed immersion, it is necessary and sufficient that Y is an affine scheme and $\Gamma(f) : \Gamma(X, \mathcal{O}_X) \to \Gamma(Y, \mathcal{O}_Y)$ is surjective.

Lemma 22.4.7. *Let $f : Y \to X$ be a morphism of schemes such that $f(Y)$ is closed and f is a homeomorphism onto $f(Y)$. Then for each point $x \in X$, there exists an affine open neighborhood U of x such that $f^{-1}(U)$ is an affine open of Y.*

Proof. Since $f(Y)$ is closed in X, the lemma is trivial if $x \notin f(Y)$, since it suffices to choose an affine open neighborhood of x disjoint from $f(Y)$. If $x \in f(Y)$, there exists a unique point $y \in Y$ such that $f(y) = x$. Let W be an affine open neighborhood of x in X and V an affine open neighborhood of y in Y such that $f(V) \subseteq W$. By hypothesis $f(V)$ is an open neighborhood of x in $f(Y)$, so there exists an open neighborhood $U' \subseteq W$ of x such that $U' \cap f(Y) = f(V)$. Let U be an open neighborhood of x contained in U' and is of the form $D(s)$, where $s \in A = \Gamma(W, \mathcal{O}_X)$ (recall that W is chosen to be affine); in view of Proposition 10.4.18(b), $f^{-1}(U) \subseteq V$ is of the form $D(t)$, where t is the image of s in $B = \Gamma(V, \mathcal{O}_Y|_V)$, hence proves the lemma. □

Lemma 22.4.8. *Let $f : Y \to X$ be a morphism of schemes and (U_λ) be an affine open covering of X such that for each λ, $f^{-1}(U_\lambda)$ is an affine open of Y. Then for any quasi-coherent $\mathcal{O}_Y$-module $\mathcal{F}$, the direct image $f_*(\mathcal{F})$ is a quasi-coherent $\mathcal{O}_X$-module.*

Proof. For each λ, put $V_\lambda = f^{-1}(U_\lambda)$, and let $f_\lambda : V_\lambda \to U_\lambda$ be the restriction of f to V_λ. Then the restriction $f_*(\mathcal{F})$ to U_λ is equal to $(f_\lambda)_*(\mathcal{F}_\lambda)$, where $\mathcal{F}_\lambda = \mathcal{F}|_{U_\lambda}$. But since U_λ and V_λ are affine by hypothesis, we see $(f_\lambda)_*(\mathcal{F}_\lambda)$ is quasi-coherent by Proposition 22.1.11. This proves the lemma. □

Proposition 22.4.9. *Let $f : Y \to X$ be a morphism of schemes.*

(a) For f to be an open immersion, it is necessary and sufficient that f is a homeomorphism onto an open subset of X and for each $y \in Y$, the homomorphism $f_y^\# : \mathcal{O}_{X,f(y)} \to \mathcal{O}_{Y,y}$ is bijective.

(b) For f to be an immersion (resp. a closed immersion), it is necessary and sufficient that f is a homeomorphism onto a locally closed (resp. closed) subset of X and for each $y \in Y$, the homomorphism $f_y^\# : \mathcal{O}_{X,f(y)} \to \mathcal{O}_{Y,y}$ is surjective.

Proof. In the two cases, the conditions are clearly necessary, so we only need to prove the sufficiency. If the conditions in (a) holds, it is clear that $f^\#$ induces an isomorphism of $\mathcal{O}_Y$ to $f^*(\mathcal{O}_X)$, and $f^*(\mathcal{O}_X)$ is the sheaf defined by the transport by structure by means of f^* from the induced sheaf $\mathcal{O}_X|_{f(Y)}$, hence the conclusion.

Suppose then the conditions in (b) holds. Let U_0 be the largest open set of X such that $Z = f(Y)$ is closed in U_0; by replacing X by the subscheme induced by X over U_0, we may assume that $Z = f(Y)$ is closed in X. By Lemma 22.4.7 and Lemma 22.4.8, the sheaf $f_*(\mathcal{O}_Y)$ is a quasi-coherent $\mathcal{O}_X$-module. We have an exact sequence

$$0 \longrightarrow \mathcal{I} \longrightarrow \mathcal{O}_X \xrightarrow{f^\#} f_*(\mathcal{O}_Y) \longrightarrow 0$$

where two terms are quasi-coherent $\mathcal{O}_X$-modules; we then deduce that (Corollary 22.2.20) $\mathcal{I}$ is a quasi-coherent ideal of $\mathcal{O}_X$, and $f^\#$ factors into

$$\mathcal{O}_X \longrightarrow \mathcal{O}_X/\mathcal{I} \xrightarrow{\theta} f_*(\mathcal{O}_Y)$$

where the first arrow is the canonical homomorphism and θ is an isomorphism. If $\mathcal{O}_Z = (\mathcal{O}_X/\mathcal{I})|_Z$, $(Z, \mathcal{O}_Z)$ is then a closed subscheme of $(X, \mathcal{O}_X)$ and f factors through the canonical injection $j_Z : Z \to X$. Since the corresponding morphism $Y \to Z$ is just (f_0, θ_0), where f_0 is the map f considered as a homeomorphism from Y to Z and θ_0 is the restriction of θ to $\mathcal{O}_Z$, it is clear that f is a closed immersion, which completes the proof. □

Remark 22.4.1. It may happen that $f : Y \to X$ is a closed immersion and for all $y \in Y$, $f_y^\# : \mathcal{O}_{X,f(y)} \to \mathcal{O}_{Y,y}$ is bijective, without f being an open immersion (that is, $f(Y)$ is not necessarily opened in X). For example, let $X = \mathrm{Spec}(A)$ be an affine scheme and $x \in X$ be a closed point of X that is not isolated. Then if $Y = \mathrm{Spec}(A/\mathfrak{m}_x)$, the canonical morphism $Y \to X$ is a closed immersion satisfying the desired property, since the subspace $\{x\}$ is not open in X.

Corollary 22.4.10. *Let $f : Y \to X$ be a morphism of schemes.*

(a) Let (V_λ) be a covering of $f(Y)$ by open subsets of X. Then for f to be an immersion (an open immersion), it is necessary and sufficient that for each λ, the restriction $f^{-1}(V_\lambda) \to V_\lambda$ of f is an immersion (an open immersion).

(b) Let (U_λ) be an open covering of X. Then for f to be a closed immersion, it is necessary and sufficient that for each λ, the restriction $f^{-1}(U_\lambda) \to U_\lambda$ of f is a closed immersion.

Proof. In the case (a), $f_y^\#$ is surjective (resp. bijective) for every point $y \in Y$, and in case (b) it is surjective for every point $y \in Y$; it then suffices to verify that in case (a) f is a homeomorphism of Y onto a locally closed (resp. open) subset of X and in case (b), a homeomorphism onto a closed subset of X. Now, the hypothesis imply that f is clearly injective and maps each neighborhood of $y \in Y$ to a neighborhood of $f(y)$ in $f(Y)$. In case (a), $f(Y) \cap V_\lambda$ is locally closed (resp. open) in the union of the V_λ, and a fortiori in X; in case (b), $f(Y) \cap U_\lambda$ is closed in U_λ, hence closed in X since $X = \bigcup_\lambda U_\lambda$. □

Remark 22.4.2. We can generalize the notions of this part to any ringed spaces. We define a **ringed subspace** of a ringed space $(X, \mathcal{O}_X)$ to be a ringed space of the form $(Y, (\mathcal{O}_U/\mathcal{I})|_Y)$, where U is an open of X, $\mathcal{I}$ an ideal of $\mathcal{O}_U$ and Y the support of the sheaf of rings $\mathcal{O}_U/\mathcal{I}$ (support which is no longer necessarily closed in U). We can define the canonical injection $Y \to X$, and the definitions and results of Proposition 22.4.4 are valid without modification. We then define the notion of immersion (resp. of closed immersion) in the same manner. The characterizations of open (resp. closed) immersions given in Proposition 22.4.9 still hold (observing that if $f(Y)$ is closed in X, $f_*(\mathcal{O}_Y)$ has support $f(Y)$). The result of Proposition 22.4.9 can therefore be stated by saying that if a scheme Y is a ringed subspace of a scheme X, then Y is a subscheme of X.

22.4.3 Inverse image of subschemes

Proposition 22.4.11. *Let $f : X' \to X$ and $g : Y' \to Y$ be two S-morphisms. Let p, q be the projections of $X \times_S Y$.*

(a) If f and g are immersions (resp. open immersions, resp. closed immersions), then $f \times_S g$ is an immersion (resp. an open immersion, resp. a closed immersion).

(b) If X' (resp. Y') is identified with a subscheme of X (resp. Y) via the immersion f (resp. g), then $f \times_S g$ identifies the underlying space of $X' \times_S Y'$ with the subspace $p^{-1}(X') \cap q^{-1}(Y')$ of the underlying space of $X \times_S Y$.

Proof. We can restrict ourselves to the case where X' and Y' are subschemas and f and g are the canonical injection morphisms. The proposition has already been established for the subschemes induced on the open sets (Corollary 22.3.2); as any subscheme is a closed subscheme of an open scheme, we are reduced in case X' and Y' are closed subschemes.

We can further assume that S is affine. In fact, let (S_λ) be an affine open cover of S, φ and ψ be the structural morphisms of X and Y, and let $X_\lambda = \varphi^{-1}(S_\lambda)$, $Y_\lambda = \psi^{-1}(S_\lambda)$. The restriction X'_λ (resp. Y'_λ) of X' (resp Y') to $X_\lambda \cap X'$ (resp. $Y_\lambda \cap Y'$) is a closed subscheme of X_λ (resp. Y_λ), the schemes X_λ, Y_λ, X'_λ, Y'_λ can then be considered as S_λ-schemes and the product $X_\lambda \times_S Y_\lambda$ and $X_\lambda \times_{S\lambda} Y_\lambda$ (resp. $X'_\lambda \times_S Y'_\lambda$ and $X'_\lambda \times_{S_\lambda} Y'_\lambda$) are identified (Corollary 22.3.2). If the proposition is true when S is affine, the restriction of $f \times_S g$ to the $X'_\lambda \times_S Y'_\lambda$ will therefore be an immersion. As the product $X'_\lambda \times_S Y'_\mu$ (resp. $X_\lambda \times_S Y_\mu$) is identified with $(X'_\lambda \cap X'_\mu) \times_S (Y'_\lambda \cap Y'_\mu)$ (resp. $(X_\lambda \cap X_\mu) \times_S (Y_\lambda \cap Y_\mu)$), the restriction of $f \times_S g$ to $X'_\lambda \times_S Y'_\mu$ is also an immersion; it follows from Corollary 22.4.10 that $f \times_S g$ is an immersion.

Secondly, let's prove that we can also assume that X and Y are affine. In fact, let (U_i) (resp. (V_j)) be an affine open cover of X (resp. Y), and let X'_i (resp. Y'_j) be the restriction of X' (resp. Y') to $X' \cap U_i$ (resp. $Y' \cap V_j$), which is a closed subscheme of U_i (resp. V_j). Then $U_i \times_S V_j$ is identified with the restriction of $X \times_S Y$ to $p^{-1}(U_i) \cap q^{-1}(V_j)$ by Corollary 22.3.2, and similarly, if $p' : X' \times_S Y' \to X'$ and $q' : X' \times_S Y' \to Y'$ are the canonical projections, the product $X'_i \times_S Y'_j$ is identified with the restriction of $X' \times_S Y'$ to $p'^{-1}(X'_i) \cap q'^{-1}(Y'_j)$. Put $h = f \times_S g$, then since $X'_i = f^{-1}(U_i)$, $Y'_j = g^{-1}(V_j)$, we have

$$p'^{-1}(X'_i) \cap q'^{-1}(Y'_j) = h^{-1}(p^{-1}(U_i) \cap q^{-1}(V_j)) = h^{-1}(U_i \times_S V_j).$$

Again, by the same reasoning and using Corollary 22.4.10, we can show that h is an immersion.

Suppose then that X, Y, and S are affine, with rings B, C, and A, respectively. Then B and C are A-algebras, X' and Y' are affine subschemes with rings quotients B', C' of B and C, respectively. Moreover, f and g are induced by ring homomorphisms $\rho : B \to B'$ and $\sigma : C \to C'$. With these, we see $X \times_S Y$ (resp. $X' \times_S Y'$) is the affine scheme with ring $B \otimes_A C$ (resp. $B' \otimes_A C'$), and $f \times_S g$ corresponds to the ring homomorphism $\rho \otimes \sigma : B \otimes_A C \to B' \otimes_A C'$. Since this homomorphism is surjective, $f \times_S g$ is an immersion. Moreover, if $\mathfrak{b}$ (resp. $\mathfrak{c}$) is the kernel of ρ (resp. σ), the kernel of $\rho \otimes \sigma$ is $u(\mathfrak{b}) + v(\mathfrak{c})$, where u (resp. v) is the homormorphism $b \mapsto b \otimes 1$ (resp. $c \mapsto 1 \otimes c$). As p corresponds to the ring homomorphism u and q corresponds to v, this kernel corresponds, in the spectrum $\mathrm{Spec}(B \otimes_A C)$, to the closed subset $p^{-1}(X') \cap q^{-1}(Y')$, which proves the demonstration. □

Corollary 22.4.12. *If $f : X \to Y$ is an immersion (resp. an open immersion, resp. a closed immersion) and an S-morphism, then $f_{(S')}$ is an immersion (resp. an open immersion, resp. a closed immersion) for any extension $S' \to S$ of base schemes.*

Proof. This follows from the observation that the identity morphism is an immersion (resp. an open immersion, resp. a closed immersion). □

Corollary 22.4.13. *An immersion (resp. a closed immersion, resp. an open immersion) is a universally embedding (resp. universally closed, resp. universally open).*

Proposition 22.4.14. *Let $f : X \to Y$ be a morphism, Y' a subscheme (resp. a closed subscheme, resp. an open subscheme) of Y, and $j : Y' \to Y$ the canonical injection.*

(a) The projection $p : X \times_Y Y' \to X$ is an immersion (resp. a closed immersion, resp. an open immersion), and the subscheme of X associated with p has underlying space $f^{-1}(Y')$. Moreover, if j' is the canonical injection of this subscheme, for a morphism $h : Z \to X$ to be such that $f \circ h : Z \to Y$ is dominated by j, it is necessary and sufficient that h is dominated by j'.

(b) *If Z is a closed subscheme defined by a quasi-coherent ideal $\mathscr{K}$ of $\mathscr{O}_Y$, the inverse image of Z by f is defined by the quasi-coherent ideal $f^*(\mathscr{K})\mathscr{O}_X$.*

Proof. As $p = 1_X \times_Y j$, the first assertion in (a) follows from Proposition 22.4.11. The second one is a special case of Corollary 22.3.31. Finally, if we have $f \circ h = j \circ h'$, where $h' : Z \to Y'$ is a morphism, it follows from the universal property of product that we have $h = p \circ u$, where $u : Z \to X \times_Y Y'$ is a morphism, whence assertion (a).

To prove (b), since the question is local on X and Y, we may assume that X and Y are affine. It then suffices to note that if A is an B-algebra and $\mathfrak{b}$ is an ideal of B, we have $A \otimes_B (B/\mathfrak{b}) = A/\mathfrak{b}A$, and apply Proposition 22.1.13. □

We say the subscheme of X thus defined is the **inverse image** of the subscheme Y' of Y by the morphism f. We say the morphism $f \times 1_{Y'} : f^{-1}(Y') \to Y'$ is the restriction of f to $f^{-1}(Y')$. When we speak of $f^{-1}(Y')$ as a subscheme of X, it is always this subscheme that will be involved.

Example 22.4.15. If the scheme $f^{-1}(Y')$ and X are identical, $j' : f^{-1}(Y') \to X$ is then the identity and any morphism $h : Z \to X$ is dominated by j'; hence the morphism $f : X \to Y$ factors into

$$X \xrightarrow{g} Y' \xrightarrow{j} Y$$

Example 22.4.16. If y is a closed point of Y and $Y' = \operatorname{Spec}(\kappa(y))$ is the smallest closed subscheme of Y having $\{y\}$ as underlying space, the closed subscheme $f^{-1}(Y')$ is then canonically isomorphic to the **fiber** $f^{-1}(y)$.

Corollary 22.4.17. *Retain the hypotheses of Proposition 22.4.14(b). Let X' be a closed subscheme of X defined by a quasi-coherent ideal $\mathscr{I}$ of $\mathscr{O}_X$ and $i : X' \to X$ be the canonical injection. For the restriction $f \circ i$ of f to X' is dominated by the injection $j : Y' \to Y$, it is necessary and sufficient that $f^*(\mathscr{K})\mathscr{O}_X \subseteq \mathscr{I}$.*

Proof. This follows from Proposition 22.4.14(b) and (a). □

Corollary 22.4.18. *Let $f : X \to Y$, $g : Y \to Z$ be two morphisms, and $h = g \circ f$ be their composition. For any subscheme Z' of Z, the subscheme $f^{-1}(g^{-1}(Z'))$ and $h^{-1}(Z')$ of X are identical.*

Proof. This follows from the transitivity of products and Proposition 22.4.14. □

Corollary 22.4.19. *Let X', X'' be two subschemes of X and $j' : X' \to X$, $j'' : X'' \to X$ be the canonical injections. Then $j'^{-1}(X'')$ and $j''^{-1}(X')$ are both equal to the infimum $\inf(X', X'')$ of X' and X'' for the ordered relation on subschemes, and is canonically isomorphic to $X' \times_S X''$.*

Proof. This follows from Proposition 22.4.14, Proposition 22.4.3, and the universal property of products. □

Corollary 22.4.20. *Let $f : X \to Y$ be a morphism and Y', Y'' be two subschemes of Y. Then we have $f^{-1}(\inf(Y', Y'')) = \inf(f^{-1}(Y'), f^{-1}(Y''))$.*

Proof. In fact, we have the canonical isomorphism of $(X \times_Y Y') \times_X (X \times_Y Y'')$ and $X \times_Y (Y' \times_Y Y'')$. □

22.4.4 Local immersions and local isomorphisms

Let $f : X \to Y$ be a morphism of schemes. We say f is a **local immersion** (resp. a **local isomorphism**) **at a point** $x \in X$ if there exists an open neighborhood U of x in X and an open neighborhood V of $f(x)$ in Y such that the restriction of f to U is a closed immersion (resp. an open immersion) into V. We say f is a local immersion (resp. a local isomorphism) if f is a local immersion (resp. a local isomorphism) at every point of X.

An immersion (resp. closed immersion) $f : X \to Y$ can then be characterized as a local immersion such that f is a homeomorphism onto a subset of Y (resp. a closed subset of Y). An open immersion f can be characterized as an injective local isomorphism.

Proposition 22.4.21. *Let X be an irreducible scheme, $f : X \to Y$ be a injective dominant morphism. If f is a local immersion, then it is an immersion and $f(X)$ is open in Y.*

Proof. In fact, let $x \in X$ and U be an open neighborhood of x in X, V an open neighborhood of $f(x)$ in Y such that $f|_Y$ is a closed immersion into V. As U is dense in X, $f(U)$ is also dense in Y by hypothesis, hence $f(U) = V$ and f is a homeomorphism from U to V. The hypothesis f is injective implies $f^{-1}(V) = U$, whence the proposition. □

Proposition 22.4.22. *Let $f : X \to X'$, $g : Y \to Y'$ be two S-schemes.*

(a) The composition of two local immersions (resp. local isomorphisms) is a local immersion (resp. a local isomorphism).

(b) If f and g are local immersions (resp. local isomorphisms), so is the product $f \times_S g$.

(c) If f is a local immersion (resp. a local isomorphism), so is $f_{(S')}$ for any extension $S' \to S$ of base schemes.

Proof. It suffices to prove (a) and (b). Now (a) follows from the transitivity of closed immersions (resp. open immersions) and the fact that if f is a homeomorphism of X to a closed subset Y, then for any open set $U \subseteq X$, $f(U)$ is open in $f(X)$, so there exists an open subset V of Y such that $f(U) = V \cap f(X)$, and $f(U)$ is therefore closed in V.

To prove (b), let p, q be the projections of $X \times_S Y$ and p', q' that of $X' \times_S Y'$. There exist by hypotheses open neighborhoods U, U', V, V' of $x = p(z)$, $x' = p'(z')$, $y = q(z)$, $y' = q'(z')$, respectively, such that $f|_U$ and $g|_V$ are closed immersions (resp. open immersions) onto U' and V', respectively. As the underlying space of $U \times_S V$ is $p^{-1}(U) \cap q^{-1}(V)$ and that of $U' \times_S V'$ is $p'^{-1}(U') \cap q'^{-1}(V')$, which are neighborhoods of z and z', respectively (Corollary 22.3.2), the claim follows by Corollary 22.4.12. □

Remark 22.4.3. A local isomorphism is clearly flat and universally open, and therefore is universally generalizing.

Proposition 22.4.23. *Let X be an irreducible scheme, Y an integral scheme, and $f : X \to Y$ be a morphism.*

(a) If f is dominant, then for any $x \in X$, the homomorphism $f_x^\# : \mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x}$ is injective.

(b) If f is dominant and a local immersion, then f is a local isomorphism (and therefore X is integral).

Proof. Let ξ and η be the generic points of X and Y, respectively. If f is dominant, we then have $f(\xi) = \eta$; moreover $\mathscr{O}_{Y,\eta}$ is a field since Y is reduced, so $f_\xi^\# : \mathscr{O}_{Y,\eta} \to \mathscr{O}_{X,\xi}$ is a monomorphism. For any point $x \in X$, and any affine neighborhood U of $y = f(x)$, there exists an affine neighborhood V of x contained in $f^{-1}(U)$. The open set U (resp. V) contains η (resp. ξ), and the ring $\Gamma(U, \mathscr{O}_Y)$ is integral with fraction field $\mathscr{O}_{Y,\eta}$. If $\rho : \Gamma(U, \mathscr{O}_Y) \to \Gamma(V, \mathscr{O}_X)$ is the homomorphism corresponding to f, the composition

$$\Gamma(U, \mathscr{O}_Y) \xrightarrow{\rho} \Gamma(V, \mathscr{O}_X) \longrightarrow \mathscr{O}_{X,\xi}$$

is then the restriction of $f_\xi^\#$ to $\Gamma(U, \mathscr{O}_Y)$, so the homomorphism ρ. We now deduce that $f_x^\#$ is injective: in fact the hypotheses that X is irreducible implies that $\Gamma(V, \mathscr{O}_X)$ has a unique minimal $\mathfrak{n}$, which is its nilradical; the homomorphism $f_x^\#$ just send an element u/s (where $u, s \in \Gamma(U, \mathscr{O}_Y)$ and $s \neq 0$) to the element $\rho(u)/\rho(s) \in \mathscr{O}_{X,x}$, which is zero only if there exists $t \notin \mathfrak{p}_x$ such that $t\rho(u) = 0 \in \mathfrak{n}$. But as $t \notin \mathfrak{n}$, this then implies $\rho(u) \in \mathfrak{n}$, so $\rho(u)$ is nilpotent and since ρ is injective, this shows that u is nilpotent, which means $u = 0$ for $\Gamma(U, \mathscr{O}_Y)$ being integral.

To prove the second assertion, let f be dominant and a local immersion. We see $f(Y)$ is open in Y by Proposition 22.4.21. Since $f_x^\#$ is surjective for every point $x \in X$ (Proposition 22.4.9), it follows that $\mathfrak{f}_x^\#$ is an isomorphism by (a), and this shows f is a local isomorphism, again by Proposition 22.4.9 . □

Proposition 22.4.24. *Let Y be a reduced scheme such that the family of irreducible components of Y is locally finite. Let $j : X \to Y$ be an immersion. For j to be a local isomorphism at a point $x \in X$, it is necessary and sufficient that the homomorphism $j_x^\# : \mathscr{O}_{Y,j(x)} \to \mathscr{O}_{X,x}$ is flat.*

Proof. Since the question is local on Y, we may assume that Y is affine, that j is a closed immersion, and that all irreducible components of Y contain $j(x)$ (hence are finite in number), and we prove that j is an isomorphism in this case. If $Y = \operatorname{Spec}(A)$, and if $\mathfrak{p}$ is the prime ideal of A corresponding to $j(x)$, the morphism $\operatorname{Spec}(A_\mathfrak{p}) \to \operatorname{Spec}(A)$ is then dominant since $\mathfrak{p}$ contains the minimal ideals of A (it is contaiend in every irreducible component of $\operatorname{Spec}(A)$). As A is reduced, the homomorphism $A \to A_\mathfrak{p}$ is injective (Corollary 10.4.19). If $\mathscr{O}$ is the ideal of $\mathscr{O}_Y$ defining the closed subscheme of Y associated with j, we have $\mathscr{I} = \widetilde{\mathfrak{a}}$, where $\mathfrak{a}$ is an ideal of A, and it is identified with a subset of $\mathfrak{a}_\mathfrak{p}$. If j is flat at x, then $(A/\mathfrak{a})_\mathfrak{p}$ is a flat $A_\mathfrak{p}$-module, and since the homomorphism $A_\mathfrak{p} \to (A/\mathfrak{a})_\mathfrak{p}$ is local, it is faithfully flat (Proposition 7.3.15). By Proposition 7.3.15 this implies $\mathfrak{a}_\mathfrak{p} = 0$, hence $\mathfrak{a} = 0$ and the claim follows. □

22.4.5 Nilradical and associated reduced scheme

Proposition 22.4.25. *Let $(X, \mathscr{O}_X)$ be a scheme and $\mathscr{B}$ be a quasi-coherent $\mathscr{O}_X$-algebra. There exist a unique quasi-coherent ideal $\mathscr{N}$ of $\mathscr{B}$ such that for each point $x \in X$, the stalk $\mathscr{N}_x$ is the nilradical of the ring $\mathscr{B}_x$. If $X = \operatorname{Spec}(A)$ is affine and $\mathscr{B} = \widetilde{B}$, where B is an A-algebra, then $\mathscr{N} = \widetilde{\mathfrak{n}}$, where $\mathfrak{n}$ is the nilradical of B.*

Proof. Since the question is loca, we may assume that $X = \operatorname{Spec}(A)$ is affine and $\mathscr{B} = \widetilde{B}$. We know that $\widetilde{\mathfrak{n}}$ is a quasi-coherent $\mathscr{O}_X$-module and for each point $x \in X$, the stalk $\mathfrak{n}_x$ is an ideal of the fraction ring B_x. It suffices to show that the nilradical of B_x is contained in $\mathfrak{n}_x$, the opposite inclusion being evident. Now, let z/s be a nilpotent element in B_x, where $z \in B$ and $s \notin \mathfrak{p}_x$. By

hypotheses, there exist $k \geq 0$ such that $(z/s)^k = 0$, which means there exists $t \notin \mathfrak{p}_x$ such that $tz^k = 0$. We then conclude that $(tz)^k = 0$, so $z/s = (tz)/(ts)$ is indeed in $\mathfrak{n}_x$. □

The quasi-coherent ideal $\mathscr{N}$ is called the **nilradical** of the $\mathscr{O}_X$-algebra $\mathscr{B}$. In particular, we denote by $\mathscr{N}_X$ the nilradical of $\mathscr{O}_X$.

Corollary 22.4.26. *Let X be a scheme. Then the closed subscheme of X defined by the quasi-coherent ideal $\mathscr{N}_X$ is the unique reduced subscheme of X with underlying space X. It is also the smallest subscheme of X having X as underlying space.*

Proof. Since the structural sheaf of the closed subscheme Y defined by $\mathscr{N}_X$ is $\mathscr{O}_X/\mathscr{N}_X$, it is immediate that Y is reduced and has X as underlying space, since $\mathscr{N}_x \neq \mathscr{O}_{X,x}$ for each $x \in X$. To prove the second claim, let Z be a subscheme of X with X as underlying space. Then Z is closed in X, so let $\mathscr{I}$ be the ideal defining it. We can assume that X is affine, so $\mathscr{I} = \widetilde{\mathfrak{a}}$ where $\mathfrak{a}$ is an ideal of A. Then for each $x \in X$ we have $\mathfrak{a} \subseteq \mathfrak{p}_x$, so $\mathfrak{a} \subseteq \mathfrak{n}$, where $\mathfrak{n}$ is the nilradical of A. This shows Y is the smallest subscheme of X with underlying space X, and if Z is distinct from Y, we necessarily have $\mathscr{I}_x \neq \mathscr{N}_x$ for some $x \in X$, and concequently Z is not reduced. □

The reduced scheme defined by $\mathscr{N}_X$ on X is called the **reduced scheme associated with X**, and denoted by X_{red}. To say that a schema X is reduced therefore means that $X_{\text{red}} = X$. Clearly, we have a canonical closed immersion $X_{\text{red}} \to X$, which is also a universal homeomorphism.

Proposition 22.4.27. *For the spectrum of a ring A to be reduced (resp. integral), it is necessary and sufficient that A is reduced (resp. integral).*

Proof. In fact, the condition $\mathscr{N} = 0$ is necessary and sufficient for $\operatorname{Spec}(A)$ to be reduced, and the integral conditions follows from Corollary 10.4.8. □

Proposition 22.4.28. *A scheme X is integral if and only if for each open subset U of X, the ring $\Gamma(U, \mathscr{O}_X)$ is integral.*

Proof. We first assume that $\Gamma(U, \mathscr{O}_X)$ is integral for any open set U. It is clear that X is reduced. If X is not irreducible, then one can find two nonempty disjoint open subsets U_1 and U_2. Then $\Gamma(U_1 \cup U_2, \mathscr{O}_X) = \Gamma(U_1, \mathscr{O}_X) \times \Gamma(U_2, \mathscr{O}_X)$, which is not an integral domain. Thus X is an integral scheme.

Conversely, suppose that X is reduced and irreducible. Let $U \subseteq X$ be an open subset, and suppose that there are elements $f, g \in \Gamma(U, \mathscr{O}_X)$ with $fg = 0$. Let

$$Y = \{x \in U : f_x \in \mathfrak{m}_x\}, \quad Z = \{x \in U : g_x \in \mathfrak{m}_x\};$$

then Y and Z are closed subsets, and $Y \cup Z = U$. Since X is irreducible, so U is irreducible, and one of Y or Z is equal to U, say $Y = U$. But then the restriction of f to any open affine subset of U will be contained in every point of that subset, hence nilpotent and thus zero. This shows that $\Gamma(U, \mathscr{O}_X)$ is integral. □

Proposition 22.4.29. *Let X be a scheme and x a point of X.*

(a) For x to belong to a unique irreducible component of X, it is necessary and sufficient that the nilradical of $\mathscr{O}_{X,x}$ is prime.

(b) *If the nilradical of $\mathcal{O}_{X,x}$ is prime and the family of irreducible components of X is locally finite, there exists an open neighborhood U of x that is irreducible.*

(c) *For X to be the coproduct of its irreducible components, it is necessary and sufficient that the family of irreducible components of X is locally finite and for each $x \in X$, the nilradical of $\mathcal{O}_{X,x}$ is prime.*

Proof. To check that whether x belongs to distinct irreducible components of X, we may assume that $X = \operatorname{Spec}(A)$ is affine (Proposition 4.1.13). Then this signifies that $\mathfrak{p}_x$ contains two distinct minimal prime ideals of A, and equivalently $\mathfrak{m}_x$ contains two distinct minimal prime ideals of $\mathcal{O}_{X,x}$, which is a contradiction if and only if the nilradical of $\mathcal{O}_{X,x}$ is prime.

Now assume the conditions in (a). As the family of irreducible components of X is locally finite, the union of those of these components which do not contain x is closed, so its complement U is open and contained in the unique irreducible component of X containing x, and therefore irreducible (Proposition 4.1.1). The assertion in (c) follows from (b) and Proposition 4.1.22. □

Proposition 22.4.30. *For a scheme X to be locally integral, it is necessary and sufficient that the family of irreducible components is locally finite and for each point $x \in X$, the local ring $\mathcal{O}_{X,x}$ is integral. In this case, X is the coproduct of its irreducible components, which are integral subschemes.*

Proof. As the localizations of integral domains are integral, for a locally integral scheme X, its local rings $\mathcal{O}_{X,x}$ are inegral. The set of the irreducible components of X is locally finite since each $x \in X$ admits an irreducible open neighborhoods; moreover, the irreducible components of X are all open and disjoint, so X is the coproduct of its irreducible components (Proposition 4.1.22). Conversely, if X satisfies these conditions, then X is the coproduct of its irreducible components, which are open and integral. It follows immediately that X is locally integral. □

Corollary 22.4.31. *Let X be a scheme whose set of irreducible components is locally finite (for example if X is locally Noetherian). Then for X to be integral, it is necessary and sufficient that it is connected and for each $x \in X$, the local ring $\mathcal{O}_{X,x}$ is integral. In particular, a locally integral and connected scheme is integral.*

Proposition 22.4.32. *Let X be a locally Noetherian scheme and let $x \in X$ be a point such that the nilradical $\mathcal{N}_x$ of $\mathcal{O}_{X,x}$ is prime (resp. such that $\mathcal{O}_{X,x}$ is reduced, resp. such that $\mathcal{O}_{X,x}$ is integral). Then there exist an open neighborhood U of x that is irreducible (resp. reduced, resp. integral).*

Proof. It suffices to consider the case where $\mathcal{N}_x$ is prime and where $\mathcal{N}_x = 0$, the third one is the conjunction of the first two cases. If $\mathcal{N}_X$ is prime, the claim follows from Proposition 22.4.29. If $\mathcal{N}_x = 0$, we then have $\mathcal{N}_y = 0$ for y in a neighborhood of x, since $\mathcal{N}$ is quasi-coherent, hence coherent since X is locally Noetherian and $\mathcal{N}$ is of finite type, and the conclusion follows from Proposition 19.4.6. □

Proposition 22.4.33. *For a Noetherian scheme X, the nilradical $\mathcal{N}_X$ of $\mathcal{O}_X$ is nilpotent.*

Proof. Since X is quasi-compact, We can cover X by a finite number of affine open sets U_i, and it suffices to prove that there exist integers n_i such that $(\mathcal{N}_X|_{U_i})^{n_i} = 0$. If n is the largest of the n_i, we will then have $\mathcal{N}_X^n = 0$. We are therefore reduced to the case where $X = \operatorname{Spec}(A)$ is affine, A being a Noetherian ring. It then suffices to observe that the nilradical of A is nilpotent. □

Corollary 22.4.34. *A Noetherian sheme X is affine if and only if X_{red} is affine.*

Proof. If X is affine it is clear that X_{red} is affine, regardless of X being Noetherian. Conversely, assume that X_{red} is affine and X is Noetherian. Then by Proposition 22.4.33, the nilradical $\mathcal{N}$ of $\mathcal{O}_X$ is nilpotent. For any quasi-coherent sheaf $\mathcal{F}$ on X, consider the follows exact sequence (where $k \geq 0$)

$$0 \longrightarrow \mathcal{N}^k\mathcal{F} \longrightarrow \mathcal{N}^{k-1}\mathcal{F} \longrightarrow \mathcal{N}^{k-1}\mathcal{F}/\mathcal{N}^k\mathcal{F} \longrightarrow 0$$

Since $\mathcal{N}^{k-1}\mathcal{F}/\mathcal{N}^k\mathcal{F}$ is an $\mathcal{O}_X/\mathcal{N}$-module and $(X, \mathcal{O}_X/\mathcal{N})$ is affine, by Serre's criterion we have $H^1(X, \mathcal{N}^{k-1}\mathcal{F}/\mathcal{N}^k\mathcal{F}) = 0$, so

$$H^1(X, \mathcal{N}^k\mathcal{F}) = 0 \Rightarrow H^1(X, \mathcal{N}^{k-1}\mathcal{F}) = 0.$$

Since $\mathcal{N}$ is nilpotent, this shows $H^1(X, \mathcal{F}) = 0$, so $(X, \mathcal{O}_X)$ is affine, by Serre's criterion again. □

Let $f : X \to Y$ be a morphism of schemes; let $i : X_{\mathrm{red}} \to X$ and $j : Y_{\mathrm{red}} \to Y$ be the canonical injections. The homomorphism $f_x^\# : \mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x}$ maps nilpotent elements of $\mathcal{O}_{Y,f(x)}$ into nilpotent elements of $\mathcal{O}_{X,x}$, so $f^*(\mathcal{N}_Y)\mathcal{O}_X \subseteq \mathcal{N}_X$. It then follows from Proposition 22.4.4 that $f \circ i$ factors through j, so we get an induced morphism $f_{\mathrm{red}} : X_{\mathrm{red}} \to Y_{\mathrm{red}}$ and a commutative diagram

$$\begin{tikzcd} X_{\mathrm{red}} \arrow[r, "f_{\mathrm{red}}"] \arrow[d, "i"'] & Y_{\mathrm{red}} \arrow[d, "j"] \\ X \arrow[r, "f"] & Y \end{tikzcd} \tag{4.5.1}$$

In particular, if X is reduced, then the morphism f factors into

$$X \xrightarrow{f_{\mathrm{red}}} Y_{\mathrm{red}} \xrightarrow{j} Y$$

or in other words, f is dominated by the canonical injection j. We also conclude that Y_{red} satisfies the universal property that any morphism from a reduced scheme to Y factors through Y_{red}.

For two morphisms $f : X \to Y$, $g : Y \to Z$, it follows from the uniqueness of factorization that we have

$$(g \circ f)_{\mathrm{red}} = g_{\mathrm{red}} \circ f_{\mathrm{red}};$$

we can equivalently say that the operation $X \mapsto X_{\mathrm{red}}$ is a covariant functor on the category of schemes.

Proposition 22.4.35. *If X and Y are S-schemes, the schemes $X_{\mathrm{red}} \times_{S_{\mathrm{red}}} Y_{\mathrm{red}}$ and $X_{\mathrm{red}} \times_S Y_{\mathrm{red}}$ are identical, and are canonically identified with a subscheme of $X \times_S Y$ having the same underlying space as this product.*

Proof. The fact that $X_{\mathrm{red}} \times_S Y_{\mathrm{red}}$ is identified with a subscheme of $X \times_S Y$ follows from the fact that if $f : X' \to X$ and $g : Y' \to Y$ are surjective S-immersions, then $f \times_S g : X' \times_S Y' \to X \times_S Y$ is a surjective immersion (Proposition 22.4.11 and Proposition 22.3.26). On the other hand, if $\varphi : X_{\mathrm{red}} \to S$ and $\psi : Y_{\mathrm{red}} \to S$ are the structural morphisms, it is clear that they factors through S_{red}, and as $S_{\mathrm{red}} \to S$ is a monomorphism, the second assertion follows. □

Corollary 22.4.36. *The schemes* $(X \times_S Y)_{\mathrm{red}}$ *and* $(X_{\mathrm{red}} \times_{S_{\mathrm{red}}} Y_{\mathrm{red}})_{\mathrm{red}}$ *are canonically identified.*

We note that if X and Y are reduced S-schemes, it is not necessarily that case that $X \times_S Y$ is reduced, since the tensor product of two reduced algebras (even two fields) may not be reduced.

Corollary 22.4.37. *For any morphism* $f : X \to Y$ *of schemes, the diagram (4.5.1) factors into*

$$\begin{tikzcd} X_{\mathrm{red}} = (X \times_Y Y_{\mathrm{red}})_{\mathrm{red}} \arrow[r] & X \times_Y Y_{\mathrm{red}} \arrow[r] \arrow[d] & Y_{\mathrm{red}} \arrow[d] \\ & X \arrow[r, "f"] & Y \end{tikzcd} \tag{4.5.2}$$

Proof. For this, we only need to note that $(X \times_Y Y_{\mathrm{red}})_{\mathrm{red}} = (X_{\mathrm{red}} \times_{Y_{\mathrm{red}}} Y_{\mathrm{red}})_{\mathrm{red}} = X_{\mathrm{red}}$. □

Proposition 22.4.38. *Let* X *and* Y *be two schemes. Consider the following properties for a morphism* $f : X \to Y$*:*

(i) surjective;

(ii) injective;

(iii) open at the point x *(resp. open);*

(iv) closed;

(v) a homeomorphism onto its image;

(vi) universally open at a point x *(resp. universally open);*

(vii) universally closed;

(viii) a universal embedding;

(ix) a universal homeomorphism;

(x) radical;

(xi) generalizing at a point x *(resp. generalizing);*

(xii) universally generalizing at a point x *(resp. universally generalizing).*

Then, if $\mathcal{P}$ *denote one of the above properties, for* f *to possess the property* $\mathcal{P}$*, it is necessary and sufficient that* f_{red} *possess* $\mathcal{P}$*.*

Proof. The proposition is evident for the properties (i), (ii), (iii), (iv), (v), (xi), which only depend on the map of the underlying spaces. For (x), the proposition follows from the fact that the fibers of f and f_{red} at a point $y \in Y$ have the same underlying space and the residue field at a point of X (resp. Y) is the same for X_{red} and Y_{red}. For the properties (vi), (vii), (viii), (ix) and (xii), if f possesses one of these properties, the same is true of f_{red} due to Corollary 22.4.37 and that the morphism $X_{\mathrm{red}} \to X \times_Y Y_{\mathrm{red}}$ is a universal homeomorphism. Conversely, if f_{red} possesses one of these properties, it suffices to note that for any morphism $Y' \to Y$ we have $(X_{\mathrm{red}} \times_{Y_{\mathrm{red}}} Y'_{\mathrm{red}})_{\mathrm{red}} = (X \times_Y Y')_{\mathrm{red}}$, so the morphism

$$(f_{(Y')})_{\mathrm{red}} : (X \times_Y Y')_{\mathrm{red}} \to Y'_{\mathrm{red}}$$

possesses the "nonuniversal" version of the same property, and by what we have already seen, $f_{(Y')}$ then has the corresponding property. □

Proposition 22.4.39. *Let X and Y be two schemes and x be a point of X. Consider the following properties for a morphism $f : X \to Y$:*

(i) a monomorphism;

(ii) an immersion;

(iii) an open immersion;

(iv) a closed immersion;

(v) a local immersion at the point x;

(vi) a local isomorphism at the point x;

(vii) birational.

Then, if f possesses one of the above properties, f_{red} also possesses that property.

Proof. For the properties (ii) to (vii), the result follows from the observation that $(f_{\mathrm{red}})^{\#}_x : \mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x}$ is surjective (resp. bijective) if $f^{\#}_x : \mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x}$ is surjective (resp. bijective) (Proposition 22.4.9). For (i) it suffices to note that a monomorphism is universal (Proposition 22.3.10), the diagram (4.5.2), and the fact that $X_{\mathrm{red}} \to X \times_Y Y_{\mathrm{red}}$ is a closed immersion, hence a monomorphism. □

Note that if f_{red} is an immersion, it is not necessarily true that f is. For example, let $Y = \mathrm{Spec}(k)$ where k is a field and $X = \mathrm{Spec}(A)$, where $A = k[T]/(T^2)$. Then the canonical injection $\rho : k \to k[T]/(T^2)$ corresponds to a morphism $f : X \to Y$. It is clear that f is not an immersion (in fact any nonzero immersion into Y is automatically closed); but $A_{\mathrm{red}} = k$ so f_{red} is an isomorphism.

Remark 22.4.4. To say that an immersion $f : Y \to X$ is surjective means it is closed and that the subscheme of X associated with f is defined by an ideal $\mathcal{I}$ contained in the nilradical $\mathcal{N}_X$. In this case, we say f is a nilimmersion; f is then a homeomorphism from Y to X, and f_{red} is an isomorphism from Y_{red} to X_{red}. We say the nilimmersion f is **nilpotent** (resp. **locally nilpotent**) if the ideal $\mathcal{I}$ is nilpotent (resp. locally nilpotent, i.e. that every $x \in X$ has an open neighborhood U such that $\mathcal{I}|_U$ is nilpotent). More precisely, we say f is **nilpotent of order n** if $\mathcal{I}^{n+1} = 0$. If Y is a subscheme of X and f is the canonical immersion, we say X is an **infinitesimal neighborhood** (resp. an **infinitesimal neighborhood of order n**) of Y if f is nilpotent (resp. nilpotent of order n).

22.4.6 Reduced scheme structure on closed subsets

Proposition 22.4.40. *For any locally closed subspace Y of the underlying space of a scheme X, there exists a unique reduced subscheme of X with underlying space Y.*

Proof. The uniqueness is immediate from Corollary 22.4.26, so we only need to construct a reduced scheme structure on Y. If X is affine with ring A and Y is closed in X, the proposition is immediate: $I(Y)$ is the largest ideal $\mathfrak{a} \subseteq A$ such that $V(\mathfrak{a}) = Y$, and is radical, hence the ring $A/I(Y)$ is reduced, and we can take the scheme structure $(Y, \widetilde{A/I(Y)})$ on Y.

In the general case, for any affine open $U \subseteq X$ such that $U \cap Y$ is closed in U, consider the closed subscheme Y_U of U defined by the quasi-coherent ideal associated with the ideal $I(U \cap Y)$ of $\Gamma(U, \mathcal{O}_X|_U)$, which is reduced. If V is an open affine of X contained in U, then Y_V is induced by Y_U on $V \cap Y$ since this induced scheme is a closed subscheme of V which is reduced and has $V \cap Y$ as underlying space; the uniqueness of Y_V therefore entails our assertion. □

Corollary 22.4.41. *Let X be a scheme and Y be a locally closed subset of X. Then any point $x \in Y$ admits a maximal generalization y (i.e. y has no further generalization in Y). In particular, if $Y \neq \varnothing$, there exist a maximal element $y \in Y$ under generalization.*

Proof. It suffices to give Y a subscheme structure of X and take y to be the generic point of the irreducible components of Y containing x. □

Example 22.4.42. Let X be a scheme and x be a closed point of X. Let U be an open neighborhood of x. Then $Z = (X - U) \cup \{x\}$ is a closed subset of X, so we can consider the reduced scheme structure on it. Let $\mathcal{I}$ be the corresponding quasi-coherent ideal of $\mathcal{O}_X$, we want to determine the stalk $\mathcal{I}_x$. For this, we can assume that $X = \operatorname{Spec}(A)$ is affine and $X - U = V(\mathfrak{a})$, where $\mathfrak{a}$ is an ideal of A. Then the point x corresponds to a maximal ideal $\mathfrak{m}$ of A such that $\mathfrak{a} \not\subseteq \mathfrak{m}$, and $Z = V(\mathfrak{a}) \cup \{x\} = V(\mathfrak{a} \cap \mathfrak{m})$. By definition, $\mathcal{I}$ is the quasi-coherent ideal on X associated with $I(Z) = \sqrt{\mathfrak{a} \cap \mathfrak{m}}$, and therefore

$$\mathcal{I}_x = (\sqrt{\mathfrak{a} \cap \mathfrak{m}})_{\mathfrak{m}} = \sqrt{(\mathfrak{a} \cap \mathfrak{m})_{\mathfrak{m}}},$$

which is the intersection of prime ideals $\mathfrak{p}$ containing $\mathfrak{a} \cap \mathfrak{m}$ and contained in $\mathfrak{m}$. But if a prime ideal $\mathfrak{p} \subseteq \mathfrak{m}$ of A contains $\mathfrak{a} \cap \mathfrak{m}$, then by Proposition 10.1.5 we have $\mathfrak{p} \supset \mathfrak{a}$ or $\mathfrak{p} \supset \mathfrak{m}$. If $\mathfrak{p} \neq \mathfrak{m}$, then this implies $\mathfrak{p} \supset \mathfrak{a}$ and therefore $\mathfrak{m} \supset \mathfrak{p} \supset \mathfrak{a}$, which is a contradiction (since x is not contained in $X - U = V(\mathfrak{a})$). From this, we conclude that $\mathcal{I}_x = \mathfrak{m}_x$.

Example 22.4.43. Let X be a reduced locally Noetherian scheme and X' be a reduced closed subscheme of X with underlying space an irreducible component of X. Then X' is defined by a quasi-coherent ideal $\mathcal{I}$ of $\mathcal{O}_X$. Let x be the generic point of X'; we claim that $\mathcal{I}_x = 0$. For this, we can assume that $X = \operatorname{Spec}(A)$ is affine, where A is a reduced Noetherian ring, so $\mathcal{I} = \tilde{\mathfrak{p}}$ where $\mathfrak{p}$ is a minimal prime ideal of A. By definition the stalk of $\mathcal{I}$ at x is indeitified with $\mathfrak{p}A_{\mathfrak{p}}$, which is the maximal ideal of $A_{\mathfrak{p}} = \mathcal{O}_{X,x}$. But since A is reduced and $\mathfrak{p}$ is minimal, $A_{\mathfrak{p}}$ is a reduced Artinian local ring, whence a field, and we then conclude that $\mathfrak{p}A_p = 0$, so $\mathcal{I}_x = 0$.

Proposition 22.4.44. *Let X be a reduced scheme, $f : X \to Y$ be a morphism, and Z be a closed subscheme of Y containing $f(X)$. Then f factors into*

$$X \xrightarrow{g} Z \xrightarrow{j} Y$$

where j is the canonical injection.

Proof. The hypotheses implies that the closed subscheme $f^{-1}(Z)$ of X has underlying space X (Proposition 22.4.14). As X is reduced, this subscheme coincides with X by Corollary 22.4.26, and the proposition then follows from Proposition 22.4.14. □

Corollary 22.4.45. *Let X be a reduced subscheme of a scheme Y. If Z is the reduced closed subscheme of Y with underlying space $\overline{X}$, then X is an open subscheme of Z.*

Proof. Since X is locally closed, there is an open set U of Y such that $X = U \cap \overline{X}$. By Proposition 22.4.44, X is then a reduced subscheme of Z, with underlying space open in Z. Since the scheme structure induced by Z is also reduced, we conclude that X is induced by Z, in view of the uniqueness part of Proposition 22.4.40. □

Corollary 22.4.46. *Let $f : X \to Y$ be morphism and X' (resp. Y') be a closed subscheme of X (resp. Y) defined by a quasi-coherent ideal $\mathscr{I}$ (resp. $\mathscr{K}$) of $\mathscr{O}_X$ (resp. $\mathscr{O}_Y$). Suppose that X' is reduced and $f(X') \subseteq Y'$, then we have $f^*(\mathscr{K})\mathscr{O}_X \subseteq \mathscr{I}$.*

Proof. The restriction of f to X' factors into $X' \to Y' \to Y$ by Proposition 22.4.44, so it suffices to use Corollary 22.4.17. □

22.5 Separated schemes and morphisms

22.5.1 Diagonal and graph of a morphism

Let X be an S-scheme; recall that the diagonal morphism $X \to X \times_S X$, denoted by $\Delta_{X/S}$ or Δ_X, is the S-morphism $(1_X, 1_X)_S$, which means Δ_X is the unique S-morphism such that

$$p_1 \circ \Delta_X = p_2 \circ \Delta_X = 1_X,$$

where p_1, p_2 are the canonical projections of $X \times_S X$. If $f : T \to X$ and $g : T \to Y$ are two S-morphisms, we verify that

$$(f, g)_S = (f \times_S g) \circ \Delta_{T/S}.$$

If $\varphi : X \to S$ is the structural morphism of X, we also write Δ_φ for $\Delta_{X/S}$.

Proposition 22.5.1. *Let X, Y be S-schemes. If we identify $(X \times_S Y) \times_S (X \times_S Y)$ and $(X \times_S X) \times_S (Y \times_S Y)$, the morphism $\Delta_{X \times Y}$ is identified with $\Delta_X \times \Delta_Y$.*

Proof. In fact, if p_1, q_1 are the canonical projections $X \times_S X \to X$, $Y \times_S Y \to Y$, the projection $(X \times_S Y) \times_S (X \times_S Y) \to X \times_S Y$ is identified with $p_1 \times q_1$, and we have

$$(p_1 \times q_1) \circ (\Delta_X \times \Delta_Y) = (p_1 \circ \Delta_X) \times (q_1 \circ \Delta_Y) = 1_{X \times Y}$$

similar for the projection to the second factor. □

Corollary 22.5.2. *For any extension $S' \to S$ of base schemes, $\Delta_{X_{(S')}}$ is identified with $(\Delta_X)_{(S')}$.*

Proof. It suffices to remark that $(X \times_S X)_{(S')}$ is identified with $X_{(S')} \times_{S'} X_{(S')}$ canonically. □

Proposition 22.5.3. *Let X, Y be S-schemes and $S \to T$ be a morphism. Let $\varphi : X \to S$, $\psi : Y \to S$ be the structural morphisms, p, q the projection of $X \times_S Y$, and $\pi = \varphi \circ p = \psi \circ q$ the structural morphism $X \times_S Y \to S$. Then the diagram*

$$\begin{tikzcd} X \times_S Y \arrow[r, "(p,q)_T"] \arrow[d, "\pi"'] & X \times_T Y \arrow[d, "\varphi \times_T \psi"] \\ S \arrow[r, "\Delta_{S/T}"] & S \times_T S \end{tikzcd} \tag{5.1.1}$$

commutes and cartesian.

Proof. By the definition of products, we may prove the proposition in the category of sets, and replace X, Y, S by $X(Z)_T$, $Y(Z)_T$, $S(Z)_T$, where Z is an arbitrary T-scheme, and it is then immediate. □

Corollary 22.5.4. *If $f : X \to Y$ is an S-morphism, the diagram*

$$\begin{tikzcd} X \arrow[r, "\Gamma_f"] \arrow[d, "f"'] & X \times_S Y \arrow[d, "f \times_S 1_Y"] \\ Y \arrow[r, "\Delta_Y"] & Y \times_S Y \end{tikzcd} \tag{5.1.2}$$

is commutative and cartesian.

Proof. It suffcies to apply Proposition 22.5.3 with S replaced by Y and T by S, and note that $X \times_Y Y = X$. □

Proposition 22.5.5. *For a morphism $f : X \to Y$ of schemes to be a monomorphism, it is necessary and sufficient that $\Delta_{X/Y}$ is an isomorphism from X to $X \times_Y X$.*

Proof. In fact, f is a monomorphism means for any Y-scheme Z, the corresponding map $X(Z)_Y \to Y(Z)_Y$ is an injection, and as $Y(Z)_Y$ is reduced to a singleton, this means $X(Z)_Y$ is either empty or a singleton. But this is equivalent to saying that $X(Z)_Y \times X(Z)_Y$ is canonically isomorphic to $X(Z)_Y$ via the diagonal map, where the first set is $(X \times_Y X)(Z)_Y$, and this means $\Delta_{X/Y}$ is an isomorphism. □

Proposition 22.5.6. *The diagonal morphism is an immersion from X to $X \times_S X$, and the corresponding subscheme of $X \times_S X$ is called the **diagonal** of $X \times_S X$.*

Proof. Let p_1, p_2 be the projections of $X \times_S X$. As the continuous maps p_1 and Δ_X are such that $p_1 \circ \Delta_X = 1_X$, Δ_X is a homeomorphism from X onto $\Delta_X(X)$. Simialrly, the composition of the homomorphisms $\mathcal{O}_{X,x} \to \mathcal{O}_{\Delta_X(X),x} \to \mathcal{O}_{X,x}$ corresponding to p_1 and Δ_X is the identity, so the homomorphism corresponding to Δ_X on stalks are surjective. The proposition then follows from Proposition 22.4.9 . □

Corollary 22.5.7. *With the hypotheses of Proposition 22.5.3, the morphisms $(p, q)_T$ is an immersion.*

Proof. This follows from Proposition 22.5.3 and Corollary 22.4.12. □

Corollary 22.5.8. *Let X and Y be S-schemes and $f : X \to Y$ be an S-morphism. Then the graph morphism $\Gamma_f : X \to X \times_S Y$ of f is an immersion.*

Proof. This follows from the diagram (5.1.2) and Corollary 22.4.12. □

The subscheme of $X \times_S Y$ associated with the immersion Γ_f is called the **graph** of the morphism f; the subschemes of $X \times_S Y$ which are graphs of morphisms $X \to Y$ are characterized by the fact that the restriction of the projection $p_1 : X \times_S Y \to X$ to such a subscheme G is an isomorphism g from G to X: in fact, if this is the case, G is then the graph of the morphism $p_2 \circ g^{-1}$, where $p_2 : X \times_S Y \to Y$ is the second projection.

In particular, if $X = S$, the S-morphisms $S \to Y$, which are none other than the S-sections of Y, are equal to their graph morphisms; the subschemes of Y which are graphs of S-sections (in other words, those which are isomorphic to S by the restriction of the structural morphism $Y \to S$) are then called the **images of these sections**, or, by abuse of language, the S-sections of Y.

Proposition 22.5.9. *If $f : X \to Y$ is an S-morphism, the diagram*

$$\begin{tikzcd} X \arrow[r, "\Delta_X"] \arrow[d, "f"'] & X \times_S X \arrow[d, "f \times_S f"] \\ Y \arrow[r, "\Delta_Y"] & Y \times_S Y \end{tikzcd} \tag{5.1.3}$$

is commutative (in other words, Δ_X is a functorial morphism on the category of schemes).

Proof. The morphisms $\Delta_Y \circ f$ satisfies the condition that

$$p_1 \circ (\Delta_Y \circ f) = p_2 \circ (\Delta_Y \circ f) = f$$

where p_1, p_2 are the projections of $Y \times_S Y$. Similarly, if q_1, q_2 are the projections of $X \times_S X$,

$$\begin{aligned} p_1 \circ (f \times_S f) \circ \Delta_X &= f \circ q_1 \circ \Delta_X = f, \\ p_2 \circ (f \times_S f) \circ \Delta_X &= f \circ q_2 \circ \Delta_X = f. \end{aligned}$$

It then follows from the universal property of products that $\Delta_Y \circ f = (f \times_S f) \circ \Delta_X$. □

Corollary 22.5.10. *If X is a subscheme of Y, the diagonal $\Delta_X(X)$ is identified with a subscheme of $\Delta_Y(Y)$ whose the underlying space is identified with*

$$\Delta_Y(Y) \cap p_1^{-1}(X) = \Delta_Y(Y) \cap p_2^{-1}(X)$$

where p_1, p_2 are the projections of $Y \times_S Y$.

Proof. Apply Proposition 22.5.9 to the immersion $f : X \to Y$, we see $(f \times_S f)$ is an immersion which identifies $X \times_S X$ with the subspace $p_1^{-1}(X) \cap p_2^{-1}(X)$ of $Y \times_S Y$ (Proposition 22.4.11). Moreover, if $z \in \Delta_Y \cap p_1^{-1}(X)$, we have $z = \Delta_Y(y)$ and $y = p_1(z) \in X$, so $y = f(y)$, and $z = \Delta_Y(f(y))$ belongs to $\Delta_X(X)$ in view of the diagram (5.1.3). □

Proposition 22.5.11. *Let $u_1 : X \to Y$, $u_2 : X \to Y$ be two S-morphisms. Then the kernel* $\ker(u_1, u_2)$ *is canonically isomorphic to the inverse image in X of the diagonal $\Delta_Y(Y)$ under the morphism $(u_1, u_2)_S : X \to Y \times_S Y$.*

Proof. Let $Z \to X$ be the inverse image of $\Delta_Y(Y)$ under the morphism $(u_1, u_2)_S$. Then if $f : T \to X$ is an S-morphism such that $u_1 \circ f = u_2 \circ f$, then

$$p_1 \circ (u_1, u_2)_S \circ f = u_1 \circ f = u_2 \circ f = p_1 \circ \Delta_Y \circ u_2 \circ f,$$
$$p_2 \circ (u_1, u_2)_S \circ f = u_2 \circ f = p_2 \circ \Delta_Y \circ u_2 \circ f$$

where p_1, p_2 are the projections of $Y \times_S Y$. We conclude that $(u_1, u_2)_S \circ f = \Delta_Y \circ u_2 \circ f$, and by the definition of Z, the morphism f factors uniquely through Z, which proves our claim. □

Corollary 22.5.12. *For a point $x \in X$ to belong to* $\ker(u_1, u_2)$*, it is necessary and sufficient that $u_1(x) = u_2(x) = y$ and the homomorphisms $\kappa(y) \to \kappa(x)$ corresponding to u_1 and u_2 are equal.*

Proof. In fact, if $j : Z \to X$ is the kernel of u_1 and u_2, to say $x \in Z$ signifies that the canonical morphism $h : \mathrm{Spec}(\kappa(x)) \to X$ factors into $h = j \circ g$, where g is a morphism from $\mathrm{Spec}(\kappa(x))$ to Z. This is equivalent to $u_1 \circ h = u_2 \circ h$, and by Corollary 22.2.15 to that $u_1(x) = u_2(x)$ and the field extensions $\kappa(y) \to \kappa(x)$ corresponding to u_1 and u_2 are equal. □

Proposition 22.5.13. *Let X and Y be S-schemes and $f : X \to Y$, $g : X \to Y$ be S-morphisms. Then we have the following commutative diagram*

$$\begin{tikzcd}
\ker(f,g) \arrow[r] \arrow[d] & X \arrow[r, "g"] \arrow[d, "\Gamma_g"] & Y \arrow[d, "\Delta_Y"] \\
X \arrow[r, "\Gamma_f"] \arrow[d, "f"'] & X \times_S Y \arrow[r, "g \times_S \mathbf{1}_Y"] \arrow[d, "f \times_S \mathbf{1}_Y"] & Y \times_S Y \\
Y \arrow[r, "\Delta_Y"] & Y \times_S Y &
\end{tikzcd}$$

where all squares are cartesian.

Proof. The fact that $\ker(f, g)$ is identified with the kernel of Γ_f and Γ_g can be deduced from by applying the projection $X \times_S Y \to Y$, or by Yoneda since this is clearly true for sets. The other two small squares are cartesian by Corollary 22.5.4, so the claim follows from the transitivity of products. □

Proposition 22.5.14. *Let $\mathcal{P}$ be a property for morphisms of schemes and consider the following conditions:*

(i) If $j : X \to Y$ is an immersion and $g : Y \to Z$ is a morphism possessing the property $\mathcal{P}$, then $g \circ j$ possesses the property $\mathcal{P}$.

(ii) If $f : X \to X'$ and $g : y \to Y'$ are two S-morphisms possessing the property $\mathcal{P}$, then $f \times_S g$ possesses the property $\mathcal{P}$.

(iii) If the composition $g \circ f$ of two morphisms $f : X \to Y$, $g : Y \to Z$ possesses the property $\mathcal{P}$, then f possesses the property $\mathcal{P}$.

Then (iii) is a concequence of (i) and (ii).

Proof. The morphism f factors into

$$X \xrightarrow{\Gamma_f} X \times_Z Y \xrightarrow{p_2} Y$$

where p_2 is the projection. On the other hand, p_2 is idnetified with $(g \circ f) \times_Z 1_Y$, and by (ii) it possesses the property $\mathcal{P}$; as Γ_f is an immersion, it then follows from (i) that f possesses $\mathcal{P}$. □

Proposition 22.5.15. *Let $f : X \to Y$ and $g : Y \to Z$ be two morphisms. Consider the following properties for a morphism:*

(i) a monomorphism;

(ii) an immersion;

(iii) a local immersion;

(iv) a universal embedding;

(v) radical.

Then, if $g \circ f$ possesses one of these properties, so does f.

Proof. The properties (i) and (v) have only been put for memory, because for (i) this is a property valid for any category, and for (v), the proposition has already been proven in Proposition 22.3.29.

An immersion has each of these properties, and the composition of two morphisms having one (determined) of these properties also possesses it; moreover, all the above properties are stable under products. Thus the claim follows from Proposition 22.5.14. □

Corollary 22.5.16. *Let $j : X \to Y$ and $g : X \to Z$ be two S-morphisms. If j possesses one of the properties in Proposition 22.5.15, so does $(j, g)_S$.*

Proof. In fact, if $p : Y \times_S Z \to Y$ is the projection, we have $j = p \circ (j, g)_S$, and it suffices to apply Proposition 22.5.15. □

22.5.2 Separated morphisms and schemes

A morphism $f : X \to Y$ of schemes is called **separated** if the diagonal morphism $\Delta_f : X \to X \times_Y X$ is a closed immersion. In this case, X is said to be a **separated Y-scheme**, or **separated over Y**. A scheme X is called **separated** if it is separated over $\mathbb{Z}$. In view of Proposition 22.5.6, for X to be separated over Y, it is necessary and sufficient that the diagonal is a closed subscheme of $X \times_Y X$.

Proposition 22.5.17. *Any morphism of affine schemes is separated. In particular, any affine scheme is separated.*

Proof. If $f : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is a morphism of affine schemes, where B is an A-algebra, the diagonal morphism corresponds to the ring homomorphism $B \otimes_A B \to B$ given by $b \otimes b' \mapsto bb'$. Since this is surjective, we conclude that Δ_f is a closed immersion, so f is separated. □

Proposition 22.5.18. *Let X, Y be S-schemes and $S \to T$ be a separated morphism. Then the canonical immersion $X \times_S Y \to X \times_T Y$ in (5.1.1) is closed.*

Proof. In fact, in the diagram (5.1.1), the diagonal $\Delta_{S/T}$ is a closed immersion, so its base change $\varphi \times_T \psi : X \times_S Y \to X \times_T Y$ is also closed. □

Corollary 22.5.19. *Let X, Y be S-schemes and $f : X \to Y$ be an S-morphism. If Y is spearated over S, the graph morphism $\Gamma_f : X \to X \times_S Y$ is a closed immersion. In particular, any S-section of Y is a closed immersion.*

Proof. This follows from (5.1.2) and Corollary 22.4.12. □

Proposition 22.5.20. *Let Y be a separated S-scheme. Then for any S-morphisms $u_1 : X \to Y$, $u_2 : X \to Y$, the kernel of u_1 and u_2 is a closed subscheme of X.*

Proof. Recall that by Proposition 22.5.11 the kernel is the inverse image of $\Delta_Y(Y)$ under the morphism $(u_1, u_2)_S$. Since $\Delta_Y(Y)$ is closed, it follows from Corollary 22.4.12 that its inverse image is also closed. □

Corollary 22.5.21. *Let S be an integral scheme, η its generic point, and X a separated S-scheme. If two S-sections u, v of X satisfy $u(\eta) = v(\eta)$, then $u = v$.*

Proof. In fact, if $x = u(\eta) = v(\eta)$, the corresponding homomorphisms $\kappa(x) \to \kappa(\eta)$ are necessarily identical, since their composition with the homomorphism $\kappa(\eta) \to \kappa(x)$ corresponding to the structural morphism $X \to S$ is the idnetity on $\kappa(\eta)$. We then deduce from Corollary 22.5.12 that $\eta \in \ker(u_1, u_2)$, and by hypothesis $\ker(u_1, u_2)$ is a closed subscheme of S (Proposition 22.5.20). As S is reduced and η is its generic point, the unique closed subscheme of S containing η is S (Corollary 22.4.26), so $u = v$. □

Proposition 22.5.22. *Let $\mathcal{P}$ be a property of morphisms of schemes, and consider the following properties:*

(i) If $j : X \to Y$ is a closed immersion and $g : Y \to Z$ is a morphism possessing the property $\mathcal{P}$, then $g \circ j$ possesses the property $\mathcal{P}$.

(ii) If $f : X \to X'$ and $g : Y \to Y'$ are two S-morphisms possessing the property $\mathcal{P}$, then $f \times_S g$ possesses the property $\mathcal{P}$.

(iii) If the composition $g \circ f$ of two morphisms $f : X \to Y$ and $g : Y \to Z$ possesses the property $\mathcal{P}$ and if g is separated, then f possesses the property $\mathcal{P}$.

(iv) If $f : X \to Y$ possesses the property $\mathcal{P}$, so does f_{red}.

Then, (iii) and (iv) are concequences of (i) and (ii).

Proof. For the property (iii), the demonstration is similar to Proposition 22.5.14, with the fact that Γ_f is a closed immersion by Corollary 22.5.19. On the other hand, in the commutative diagram

$$\begin{tikzcd} X_{\mathrm{red}} \arrow[r, "f_{\mathrm{red}}"] \arrow[d] & Y_{\mathrm{red}} \arrow[d] \\ X \arrow[r, "f"] & Y \end{tikzcd}$$

the vertical morphisms are closed immersions, so we see that (iv) is a consequence of (i) and (iii), observing that a closed immersion is separated in view of the definition and Proposition 22.5.5. □

Proposition 22.5.23. *Let $f : X \to Y$ be a morphism and $g : Y \to Z$ be a separated morphism. Suppose that $g \circ f$ possesses one of the following properties:*

(i) universally closed;

(ii) a closed immersion;

Then f possesses the same property.

Proof. In fact, these properties satisfy the conditions (i) and (ii) in Proposition 22.5.22. □

Corollary 22.5.24. *Let Z be a separated S-scheme and $f : X \to Y$, $g : X \to Z$ be two S-morphisms. If f is universally closed (resp. a closed immersion), so is $(f, g)_S : X \to Y \times_S Z$.*

Proof. The morphism j factors into

$$X \xrightarrow{(f,g)_S} Y \times_S Z \xrightarrow{p} Y$$

and the projection $p : Y \times_S Z \to Y$ is a separate morphism by Proposition 22.5.25 (which do not use Corollary 22.5.24), so it suffices to apply Proposition 22.5.23. □

Remark 22.5.1. From the diagram in Proposition 22.5.13, we conclude that a morphism $Y \to S$ is separated if and only if the following equivalent conditions holds:

(i) The diagonal morphism $\Delta_{Y/S}$ is a closed immersion.

(ii) For every S-scheme X and for any two S-morphisms $f, g : X \to Y$, the kernel $\ker(f, g)$ is a closed subscheme of X.

(iii) For every S-scheme X and for any S-morphism $f : X \to Y$, the graph morphism Γ_f is a closed immersion.

Also, if the conclusion in Proposition 22.5.23 holds for the morphisms $\Delta_Y : Y \to Y \times_S Y$ and $p_2 : Y \times_S Y \to Y$, then Δ_Y is a closed immersion so Y is separated over S.

22.5.3 Criterion of separated morphisms

Proposition 22.5.25 (Propoerties of Seperated Morphisms).

(i) Any radical morphism (and in particular any monomorphism, hence any immersion) is a separated morphism.

(ii) The composition of two separated morphisms is separated.

(iii) If $f : X \to X'$ and $g : Y \to Y'$ are two separated S-morphisms, $f \times_S g$ is separated.

(iv) If $f : X \to Y$ is a separated S-morphism, the S'-morphism $f_{(S')}$ is separated for any base change $S' \to S$.

(v) If the composition $g \circ f$ of two morphisms is separated, then f is separated.

(vi) For a morphism f to be separated, it is necessary and sufficient that f_{red} is separated.

Proof. Recall that for a radical morphism the diagonal morphism is surjective (Proposition 22.3.29), so it is separated. If $f : X \to Y$, $g : Y \to Z$ are two morphisms, the diagram

$$\begin{tikzcd} X \arrow[rr, "\Delta_{X/Z}"] \arrow[dr, "\Delta_{X/Y}"'] & & X \times_Z X \\ & X \times_Y X \arrow[ur, "j"'] & \end{tikzcd}$$

where j is the canonical immersion in (5.1.1), is commutative. If f and g are separated, $\Delta_{X/Y}$ is a closed immersion and j is a closed immersion by Proposition 22.5.18, so $\Delta_{X/Z}$ is closed, which proves (ii). With (i) and (ii), conditions (iii) and (iv) are equivalent, and it suffices to prove (iv). Now by transitivity, $X_{(S')} \times_{Y_{(S')}} X_{(S')}$ is identified with $(X \times_Y X) \times_Y Y_{(S')}$, and the diagonal morphism $\Delta_{X_{(S')}}$ is identified with $\Delta_X \times_Y 1_{Y_{(S')}}$. The assertion then follows from Corollary 22.4.12.

To prove (v), consider the factorization

$$X \xrightarrow{\Gamma_f} X \times_Z Y \xrightarrow{p_2} Y$$

of f, and note that $p_2 = (g \circ f) \times_Z 1_Y$; the hypothesis that $g \circ f$ is separated implies p_2 is separated by (iii), and as Γ_f is an immersion, Γ_f is separated by (i), hence f is separated by (ii). Finally, for (vi), we recall that the schemes $X_{\mathrm{red}} \times_{Y_{\mathrm{red}}} X_{\mathrm{red}}$ and $X_{\mathrm{red}} \times_Y X_{\mathrm{red}}$ is canonically identified (Proposition 22.4.35); if $j : X_{\mathrm{red}} \to X$ is the canonical injection, the diagram

$$\begin{tikzcd} X_{\mathrm{red}} \arrow[r, "\Delta_{X_{\mathrm{red}}}"] \arrow[d, "j"'] & X_{\mathrm{red}} \times_Y X_{\mathrm{red}} \arrow[d, "j \times_Y j"] \\ X \arrow[r, "\Delta_X"] & X \times_Y X \end{tikzcd}$$

is commutative, and the assertion follows from the fact that the vertical morphisms are homeomorphisms. □

Corollary 22.5.26. *If $f : X \to Y$ is separated, the restriction of f to any subscheme of X is separated.*

Proof. This follows from Proposition 22.5.25(i) and (iii). □

Corollary 22.5.27. *If X and Y are S-schemes and Y is separated over S, $X \times_S Y$ is separated over X.*

Proof. This is a particular case of Proposition 22.5.25(iv). □

Proposition 22.5.28. *Let X be a scheme and suppose that $(X_i)_{1 \leq i \leq n}$ is a finite covering of X by closed subsets. Let $f : X \to Y$ be a morphism and for each i let Y_i be a closed subset of Y such that $f(X_i) \subseteq Y_i$. Consider the reduced subscheme structures on each X_i and Y_i and let $f_i : X_i \to Y_i$ be the restriction of f on X_i. Then for f to be separated, it is necessary and sufficient that each f_i is separated.*

Proof. The necessity follows from Proposition 22.5.25(i), (ii) and (v). Conversely, if each f_i is separated, then the restriction $X_i \to Y$ of f is separated (Proposition 22.5.25). If p_1, p_2 are the projections of $X \times_Y X$, the subspace $\Delta_{X_i}(X_i)$ is identified with the subspace $\Delta_X(X) \cap p_1^{-1}(X_i)$ of $X \times_Y X$ (Corollary 22.5.10). This subspace is closed in $X \times_Y X$ by hypothesis, and their union is $\Delta_X(X)$, so Δ_X is closed and f is separated. □

Suppose in particular that X_i are the irreducible components of X; then we can suppose that each Y_i is a irreducible closed subset of Y (Proposition 4.1.6); Proposition 22.5.28 then enable us to reduce the separation problem to integral schemes.

Proposition 22.5.29. *Let (Y_λ) be an open covering of a scheme Y. For a morphism $f : X \to Y$ to be separated, it is necessary and sufficient that each of the restriction $f_\lambda : f^{-1}(Y_\lambda) \to Y_\lambda$ is separated.*

Proof. If we set $X_\lambda = f^{-1}(Y_\lambda)$ and identify $X_\lambda \times_Y X_\lambda$ and $X_\lambda \times_{Y_\lambda} X_\lambda$, the $X_\lambda \times_Y X_\lambda$ form an open covering of $X \times_Y X$. If $Y_{\lambda\mu} = Y_\lambda \cap Y_\mu$ and $X_{\lambda\mu} = X_\lambda \cap X_\mu = f^{-1}(Y_{\lambda\mu})$, then $X_\lambda \times_Y X_\mu$ is identified with $X_{\lambda\mu} \times_{Y_{\lambda\mu}} X_{\lambda\mu}$ by Corollary 22.3.2, hence with $X_{\lambda\mu} \times_Y X_{\lambda\mu}$, and finally to an open subset of $X_\lambda \times_Y X_\lambda$, which establishes our assertion (Corollary 22.4.10). □

Proposition 22.5.29 allows, by taking a covering of Y byopen affines, to reduce the study of separated morphisms to separated morphisms with values in affine schemes.

Proposition 22.5.30. *Let Y be an affine scheme, X be a scheme, and (U_α) be an affine open covering of X. For a morphism $f : X \to Y$ to be separated, it ie necessary and sufficient that, for any couple of indices (α, β), the intersection $U_\alpha \cap U_\beta$ is affine, and the ring $\Gamma(U_\alpha \cap U_\beta, \mathcal{O}_X)$ is generated by the images of $\Gamma(U_\alpha, \mathcal{O}_X)$ and $\Gamma(U_\beta, \mathcal{O}_X)$.*

Proof. The open sets $U_\alpha \times_Y U_\beta$ form an open cover of $X \times_Y X$ (Corollary 22.3.2). Let p, q be the projections of $X \times_Y X$, we have

$$\Delta_X^{-1}(U_\alpha \times_Y U_\beta) = \Delta_X^{-1}(p^{-1}(U_\alpha) \cap q^{-1}(U_\beta)) = U_\alpha \cap U_\beta.$$

It therefore amounts to show that the restriction of Δ_X to $U_\alpha \cap U_\beta$ is a closed immersion into $U_\alpha \times_Y U_\beta$. But this restriction is just $(j_\alpha, j_\beta)_Y$, where j_α (resp. j_β) is the canonical injection of $U_\alpha \cap U_\beta$ to U_α (resp. to U_β). As $U_\alpha \times_Y U_\beta$ is an affine scheme with ring isomorphic to $\Gamma(U_\alpha, \mathcal{O}_X) \otimes_{\Gamma(Y,\mathcal{O}_Y)} \Gamma(U_\beta, \mathcal{O}_X)$, we see that $U_\alpha \cap U_\beta$ is a closed subscheme of $U_\alpha \times_Y U_\beta$ if and only if it is affine and the ring homomorphism

$$\Gamma(U_\alpha, \mathcal{O}_X) \otimes_{\Gamma(Y,\mathcal{O}_Y)} \Gamma(U_\beta, \mathcal{O}_X) \to \Gamma(U_\alpha \cap U_\beta, \mathcal{O}_X), \quad h_\alpha \otimes h_\beta \to h_\alpha h_\beta$$

is surjective (Example 22.4.6), which proves our assertion. □

Corollary 22.5.31. *Let Y be an affine scheme. For a morphism $f : X \to Y$ to be separated, it is necessary and sufficient that X is separated.*

Proof. In fact, the criterion in Proposition 22.5.30 does not depend on f. □

Corollary 22.5.32. *For a morphism $f : X \to Y$ to be separated, it is necessary that for any open affine subscheme U that is separated, the open subscheme $f^{-1}(U)$ is separated, and it suffices that this ture for every affine open subset $U \subseteq Y$.*

Proof. The necessity follows from Proposition 22.5.28 and Proposition 22.5.25(ii). The sufficiency follows from Proposition 22.5.29 and Corollary 22.5.31. □

Proposition 22.5.33. *Let Y be a separated scheme and $f : X \to Y$ be a morphism. For any affine open U of X and any affine open V of Y, $U \cap f^{-1}(V)$ is affine.*

Proof. Let p_1, p_2 be the projections of $X \times_{\mathbb{Z}} Y$. Using the universal property of Γ_f, the subspace $U \cap f^{-1}(V)$ can be characterized by

$$\Gamma_f(U \cap f^{-1}(V)) = \Gamma_f(X) \cap p_1^{-1}(U) \cap p_2^{-1}(V)$$

Now $p_1^{-1}(U) \cap p_2^{-1}(V)$ is idnetified with the product $U \times_{\mathbb{Z}} V$, and therefore is affine; as $\Gamma_f(X)$ is closed in $X \times_{\mathbb{Z}} Y$ (Corollary 22.5.19), $\Gamma_f(X) \cap p_1^{-1}(U) \cap p_2^{-1}(V)$ is closed in $U \times_{\mathbb{Z}} V$, hence also affine. The assertion then follows from the fact that Γ_f is a closed immersion and Example 22.4.6. □

Example 22.5.34. The scheme in Example 22.2.8 is separated. In fact, for the covering (X_1, X_2) of X by affine opens, $X_1 \cap X_2 = U_{12}$ is affine and $\Gamma(U_{12}, \mathcal{O}_X)$, the fraction ring of the form $f(s)/s^m$ where $f \in K[s]$, is generated by $K[s]$ and $1/s$, so the conditions in Proposition 22.5.30 are satisfied.

With the same choice of X_1, X_2, U_{12} and U_{21} as in Example 22.2.8, take this time for u_{12} the isomorphism which sends $f(s)$ to $f(t)$; this time we obtain by gluing together a non-separated integral scheme X, because the first condition of Proposition 22.5.30 holds, but the second fails. It is immediate here that $\Gamma(X, \mathcal{O}_X) \to \Gamma(X_1, \mathcal{O}_X) = K[s]$ is an isomorphism; the inverse isomorphism defines a morphism $f : X \to \operatorname{Spec}(K[s])$ which is surjective, and for any $y \in \operatorname{Spec}(K[s])$ such that $\mathfrak{p}_y \neq (0)$, $f^{-1}(y)$ is reduced to a singleton, but for $\mathfrak{p}_y = (0)$, $f^{-1}(y)$ consists of two distinct points (we say that X is the "affine line on K, where the point 0 is doubled").

We can also give examples where neither of the two conditions of Proposition 22.5.30 does not hold. Note first that in the prime spectrum Y of the ring of polynomials $A = K[s, t]$ in two indeterminates over a field K, the open set $U = D(s) \cup D(t)$ is not an affine open set. Indeed, if z is a section of $\mathcal{O}_Y$ over U, there exist two integers $m, n \geq 0$ such that $s^m z$ and $t^n z$ are the restrictions to U of polynomials in s and t (Theorem 22.1.20), which is obviously only possible if the section z extends into a section over the entire space Y, identified with a polynomial in s and t. If U were affine, the canonical injection $U \to Y$ would therefore be an isomorphism by Theorem 22.1.16, which is absurd since $U \neq Y$.

This being so, let us take two affine schemes Y_1, Y_2, with rings $A_1 = K[x_1, t_1]$, $A_2 = K[s_2, t_2]$. Let $U_{12} = D(s_1) \cup D(t_1)$, $U_{21} = D(s_2) \cup D(t_2)$, and let u_{12} be the restriction to U_{21} of the isomorphism $Y_2 \to Y_1$ corresponding to the isomorphism of rints, which sends $f(s_1, t_1)$ to $f(s_2, t_2)$. We thus obtain an example where none of the conditions of Theorem 22.1.16 is satisfied (the integral scheme thus obtained is called "affine plane over K, where point 0 is doubled").

22.6 Finiteness conditions for morphisms

We study, in this section, various "finiteness conditions" for a morphism $f : X \to Y$ of schemes. There are basically two notions of "global finiteness" on X: quasi-compactness and quasi-separateness. On the other hand, there is two notions of "local finiteness" on X: locally of finite type and locally of finite presentation. By combining these local notions with the previous global notions, we obtain the notions of morphism of finite type and of morphism of finite presentation.

22.6.1 Quasi-compact and quasi-separated morphisms

We say a morphism $f : X \to Y$ is **quasi-compact** is for any quasi-compact open subset U of Y, the inverse image $f^{-1}(U)$ is quasi-compact. It is clear that this condition is purely topological, and if X is Noetherian, then any morphism $f : X \to Y$ is quasi-compact. We say a Y-scheme X is **quasi-compact over Y** if its structural morphism is quasi-compact.

If $\mathcal{B}$ is a base of Y formed by quasi-compact open sets (for example, affine opens), for a morphism f to be quasi-compact, it is necessary and sufficient that for any open set $V \in \mathcal{B}$, $f^{-1}(V)$, since any quasi-compact open set of Y is a finite union of open sets in $\mathcal{B}$.

If $f : X \to Y$ is a quasi-compact morphism, it is clear that for any open set V of Y, the restriction $f^{-1}(V) \to V$ of f is quasi-compact. Conversely, if (U_α) is an open covering of Y and $f : X \to Y$ is a morphism such that the restriction $f^{-1}(U_\alpha) \to U_\alpha$ is quasi-compact, then f is quasi-compact, since there exist a basis of quasi-compact open sets for Y, each set of which is contained in at least one of the U_α. We conclude that if $f : X \to Y$ is an S-morphism of S-schemes, and if there is an open covering (S_λ) of S such that the restrictions $\varphi^{-1}(S_\lambda) \to \psi^{-1}(S_\lambda)$ of f (where $\varphi : X \to S$ and $\psi : Y \to S$ are the structural morphisms) are quasi-compact morphisms, then f is quasi-compact.

Proposition 22.6.1. *Let Y be a separated scheme. Then for a morphism $f : X \to Y$ to be quasi-compact, it is necessary and sufficient that X is quasi-compact.*

Proof. If X is quasi-compact, it is a union of finitely many affine opens U_i, and for any affine open V of Y, $U_i \cap f^{-1}(V)$ is an affine open by Proposition 22.5.33, hence quasi-compact; therefore $f^{-1}(V)$ is quasi-compact. Conversely, if f is a quasi-compact morphism, then since Y is quasi-compact open in Y, we see $X = f^{-1}(Y)$ is also quasi-compact. □

Example 22.6.2. A closed immersion is quasi-compact since a closed subset of a quasi-compact set is again quasi-compact. However, open immersions are in general not quasi-compact: the standard example is the affine scheme $X = \mathrm{Spec}(k[x_1, x_2, \dots])$ and consider $U = X - \{0\}$, where 0 is the point of X corresponding to the maximal ideal $(x_1, x_2, \dots)$. The canonical injection $j : U \to X$ is not quasi-compact because U is not quasi-compact. To see this, consider the covering $(D(x_i))_{i\in\mathbb{N}}$ of U; for any finite subset J of $\mathbb{N}$, the family $(D(x_i))_{i\in J}$ can not cover U simply because the prime ideal $\mathfrak{p}_J$ generated by x_i with $i \in J$ is contained in U but not in the union of the $D(x_i)$ for $i \in J$.

We say a morphism $f : X \to Y$ of schemes is **quasi-separated** (of X is an **Y-scheme quasi-separated over Y**) if the diagonal morphism $\Delta_f : X \to X \times_Y X$ is quasi-compact. A scheme X is called **quasi-separated** if it is quasi-separated over $\mathbb{Z}$. Since a closed immersion is quasi-compact, we see any separated morphism is quasi-separated. In particular, any separated scheme is quasi-separated.

Proposition 22.6.3 (Properties of Quasi-Compact Morphisms).

(i) An immersion $j : X \to Y$ is quasi-compact if it is closed, or Y is locally Noetherian, or X is Noetherian.

(ii) The composition of two quasi-compact morphisms is quasi-compact.

(iii) If $f : X \to Y$ is a quasi-compact S-morphism, $f_{(S')} : X_{(S')} \to Y_{(S')}$ is quasi-compact for any base change $g : S' \to S$.

(iv) If $f : X \to X'$ and $g : Y \to Y'$ is two quasi-compact S-morphisms, then $f \times_S g$ is quasi-compact.

(v) If the composition $g \circ f$ of two morphisms $f : X \to Y$, $g : Y \to Z$ is quasi-compact, and if f is quasi-separated or if X is locally Noetherian, then f is quasi-compact.

(vi) For a morphism f to be quasi-compact, it is necessary and sufficient that f_{red} is quasi-compact.

Proof. Assertion (vi) is evident, since the quasi-compactness for a morphism only depends on the map of the underlying spaces. Also, (ii) follows from the definition of quasi-compactness.

The assertion in (i) is clear if j is closed; if j is an immersion and Y is locally Noetherian, any quasi-compact open V of Y is Noetherian, so $j^{-1}(V) = X \cap V \subseteq V$ is quasi-compact (here we identify X as a subscheme of Y). If X is Noetherian, then any morphism from X is quasi-compact.

To prove (iii), we can assume that $S = Y$ by the transitivity of products; put $f' = f_{(S')}$, and let U' be a quasi-compact open subset of S'. For any $s' \in U'$, let T be an affine open neighborhood of $g(s')$ in S, and let W be an affine open neighborhood of s' contained in $U' \cap g^{-1}(T)$; it suffices to show that $f'^{-1}(W)$ is quasi-compact, or in other words, we only need to show that if S and S' are affine, then $X \times_S S'$ is quasi-compact. This is true because by hypothesis X is a finite union of affine opens V_j, and $X \times_S S'$ is then the union of the affine schemes $V_j \times_S S'$, hence quasi-compact. With (ii) and (iii), asserion (iv) then follows.

We now prove (v) in the case where X is locally Noetherian. Put $h = g \circ f$ and let U be a quasi-compact open of Y; $g(U)$ is then quasi-compact in Z (not necessarily open), so it is contained in a finite union of quasi-compact opens V_j, and $f^{-1}(U)$ is contained in the union of the $h^{-1}(V_j)$, which are all quasi-compact by hypothesis. We then conclude that $f^{-1}(U)$ is a Noetherian space (Proposition 4.1.15), and a fortiori quasi-compact.

To prove (v) in the case that g is quasi-separated, recall that f factors into

$$X \xrightarrow{\Gamma_f} X \times_Z Y \xrightarrow{p_2} Y$$

where p_2 is identified with $(g \circ f) \times_Z 1_Y$, and if $g \circ f$ is quasi-compact, so is p_2 by (iii). Finally, we have the following cartesian square (Corollary 22.5.4)

$$\begin{tikzcd} X \arrow[r, "\Gamma_f"] \arrow[d, "f"'] & X \times_Z Y \arrow[d, "f \times 1_Y"] \\ Y \arrow[r, "\Delta_g"] & Y \times_Z Y \end{tikzcd}$$

as by hypothesis Δ_g is quasi-compact, Γ_f is also quasi-compact, and by (ii) we conclude that f is quasi-compact. □

Proposition 22.6.4. *Let $f : X \to Y$, $g : Y \to Z$ be two morphisms. If $g \circ f$ is quasi-compact and f is surjective, then g is quasi-compact.*

Proof. If fact, if V is a quasi-compact open of Z, $f^{-1}(g^{-1}(V))$ is quasi-compact by hypothesis, and we have $g^{-1}(V) = f(f^{-1}(g^{-1}(V)))$ since f is surjective, so $g^{-1}(V)$ is quasi-compact. □

Proposition 22.6.5. *Let f be a quasi-compact morphism of schemes.*

(a) The following conditions are equivalent:

(i) *f is dominant;*

(ii) *for any maximal point $y \in Y$, $f^{-1}(y) \neq \varnothing$.*

(iii) *for any maximal point $y \in Y$, $f^{-1}(y)$ contains a maximal point of X.*

(b) *If f is dominant, for any generalizing morphism $g : Y' \to Y$, the morphism $f_{(Y')} : X_{(Y')} \to Y'$ is quasi-compact and dominant.*

Proof. It is clear that (iii)⇒(ii)⇒(i). Suppose that f is dominant and consider an affine open neighborhood U of y; $f^{-1}(U)$ is quasi-compact, hence a union of finitely many affine opens V_i, and by hypothesis y belongs to the closure of $f(V_i)$ in U. We can evidently suppose that X and Y are reduced. As the closure in X of an irreducible component of V_i is an irreducible component of X (Corollary 4.1.10), we can replace X by V_i, Y by the closed reduced subscheme $\overline{f(V_i)} \cap U$ of U, and we are thus reduced to proving the proposition when $X = \operatorname{Spec}(B)$ and $Y = \operatorname{Spec}(A)$ are affine and reduced. Since f is dominant, A is then a subring of B (Proposition 10.4.18); the proposition then follows from the fact that any minimal prime ideal of A is the intersection with A of a minimal prime ideal of B (Proposition 10.2.43).

If $f : X \to Y$ is quasi-compact and dominant, then $f' = f_{(Y')}$ is quasi-compact by Proposition 22.6.3. On the other hand, a maximal point y' of Y' is hypothesis lying over a maximal point y of Y (**??**); as $f^{-1}(y)$ is nonempty by (i), the same holds for $f'^{-1}(y')$ (Proposition 22.3.35), whence the conclusion. □

Proposition 22.6.6. *For a quasi-compact morphism $f : X \to Y$, the following conditions are equivalent:*

(i) *The morphism f is closed.*

(ii) *For any $x \in X$ and any specialization y' of $y = f(x)$ distinct from y, there exists a specialization x' of x such that $f(x') = y'$.*

In particular, if $f : X \to Y$ is a quasi-compact immersion, for f to be a closed immersion, it is necessary and sufficient that X (considered as a subspace of Y) contains any specializations (in Y) of its points.

Proof. The condition (ii) expresses as $f(\overline{\{x\}}) = \overline{\{y\}}$, and is therefore a concequence of (i). To show that (ii) implies (i), consider a closed subset of X' of X; let $Y' = \overline{f(X')}$ and we prove that $Y' = f(X')$. Endow X' and Y' the reduced subscheme structure, there then exists a morphism $f' : X' \to Y'$ such that the diagram

$$\begin{tikzcd} X' \arrow[r, "f'"] \arrow[d] & Y' \arrow[d] \\ X \arrow[r, "f"] & Y \end{tikzcd}$$

commutes. As f is quasi-compact, so is f' (Proposition 22.6.3(i) and (v)). We are then reduced to proving that if f is a quasi-compact dominant morphism, then $f(X) = Y$. Now let y' be a point of y and let y be the generic point of a irreducible component of Y containing y'; by (ii), it suffices to note that $f^{-1}(y)$ is nonempty, which follows from Proposition 22.6.5. □

Proposition 22.6.7 (Properties of Quasi-Separated Morphisms).

(i) *Any radical morphism $f : X \to Y$ (in particular, any monomorphism and any immersion) is quasi-separated.*

(ii) If $f : X \to Y$ and $g : Y \to Z$ are two quasi-separated morphisms, $g \circ f$ is quasi-separated.

(iii) Let X, Y be two S-schemes and $f : X \to Y$ be a quasi-separated S-morphism. Then, for any base change $g : S' \to S$, the morphism $f_{(S')} : X_{(S')} \to Y_{(S')}$ is quasi-separated.

(iv) If $f : X \to X'$, $g : Y \to Y'$ are two quasi-separated S-morphisms, $f \times_S g$ is quasi-separated.

(v) If the composition $g \circ f$ of two morphisms $f : X \to Y$, $g : Y \to Z$ is quasi-separated, then f is quasi-separated; if moreover f is quasi-compact and surjective, g is also quasi-separated.

(vi) For a morphism $f : X \to Y$ to be quasi-separated, it is necessary and sufficient that f_{red} is quasi-separated.

Proof. The assertion (i) follows from Proposition 22.5.25(i). To prove (iii), we may reduce to the case $Y = S$, and the assertion then follows from $\Delta_{f_{(S')}} = (\Delta_f)_{(S')}$ (Corollary 22.5.2) and Proposition 22.6.3.

For assertion (ii), consider the projections p, q of $X \times_Y X$; if $\pi : X \times_Y X \to Y$ is the structural morphism and $j = (p, q)_Z$, we have the following cartesian square (Eq. (5.1.1))

$$\begin{tikzcd} X \times_Y X \arrow[r, "j"] \arrow[d, "\pi"'] & X \times_Z X \arrow[d, "f \times_Z f"] \\ Y \arrow[r, "\Delta_g"] & Y \times_Z Y \end{tikzcd}$$

If g is quasi-separated then Δ_g is quasi-compact, so j is also quasi-compact by Proposition 22.6.3(iii). If f is quasi-separated, Δ_f is quasi-compact and so is $j \circ \Delta_f$, which equals to $\Delta_{g \circ f}$. With these, assertion (iv) then follows from (ii) and (iii).

Suppose now that $g \circ f$ is quasi-separated. Then with the preceding notations, $\Delta_{g \circ f} = j \circ \Delta_f$ is quasi-compact, so Δ_f is quasi-compact by Proposition 22.6.3(v) and f is then quasi-separated. If moreover f is quasi-compact and surjective, $f \times_{\mathbb{Z}} f$ is also quasi-compact by Proposition 22.6.3(iv), and we conclude that $\Delta_g \circ \pi \circ \Delta_f$ is quasi-compact. Since $\pi \circ \Delta_f = f$ is surjective, it follows from Proposition 22.6.3(v) that Δ_g is quasi-compact, so g is quasi-separated.

Finally, for a morphism $f : X \to Y$, consider the following diagram

$$\begin{tikzcd} X_{\mathrm{red}} \arrow[r, "f_{\mathrm{red}}"] \arrow[d, "j_X"'] & Y_{\mathrm{red}} \arrow[d, "j_Y"] \\ X \arrow[r, "f"] & Y \end{tikzcd}$$

where j_X and j_Y are surjective closed immersions, and so quasi-separated and quasi-compact. From the equality $f \circ j_X = j_Y \circ f_{\mathrm{red}}$ and (v), we see f is quasi-separated if and only if f_{red} is quasi-separated. □

Corollary 22.6.8. *Let X and Y be schemes.*

(i) If f is quasi-separated, any morphism $f : X \to Y$ is quasi-separated.

(ii) If Y is quasi-separated, for a morphism $f : X \to Y$ to be quasi-separated, it is necessary and sufficient that the scheme X is quasi-separated.

(iii) Let X be a quasi-compact and Y be quasi-separated. Then any morphism $f : X \to Y$ is quasi-compact.

Proof. To show (i) we only need to note that any morphism $f : X \to Y$ is a $\mathbb{Z}$-morphism, and if X is quasi-separated, then for any morphism $f : X \to Y$ the composition $X \to Y \to \mathrm{Spec}(\mathbb{Z})$ is quasi-separated, so f is quasi-separated by Proposition 22.6.7(v). Similarly, assertion (ii) follows from Proposition 22.6.7(ii) and (v). Assertion (iii) follows from Proposition 22.6.3(v). □

Proposition 22.6.9. *Let $f : X \to Y$ be a morphism and (U_α) be a covering of Y by open subschemes that are quasi-separated. For f to be quasi-separated, it is necessary and sufficient that the open subschemes $f^{-1}(U_\alpha)$ is quasi-separated.*

Proof. The inverse image of U_α in $X \times_Y X$ is $X_\alpha \times_{U_\alpha} X_\alpha$, where $X_\alpha = f^{-1}(U_\alpha)$, and the restriction $X_\alpha \to X_\alpha \times_{U_\alpha} X_\alpha$ of Δ_f is just Δ_{f_α}, where f_α is the restriction $X_\alpha \to U_\alpha$ of f. Since quasi-compactness is local on target, we see f is quasi-separated if and only if each f_α is. But by hypothesis U_α is separated, so the conclusion follows from Corollary 22.6.8(ii). □

By Proposition 22.6.9, to verify a morphism is quasi-separated, it suffices to verify the quasi-separateness of some subschemes. This can be done by the following simple criteria:

Proposition 22.6.10. *Let X be a scheme and (U_α) be a covering of X formed by quasi-compact open subsets. Then the following conditions are equivalent:*

(i) X is a quasi-separated scheme.

(ii) For any quasi-compact open subset U of X, the canonical injection $U \to X$ is quasi-compact (that is, U is retrocompact in X).

(iii) The intersection of two quasi-compact open subsets of X is quasi-compact.

(iv) For any couple of indices (α, β), the intersection $U_\alpha \cap U_\beta$ is quasi-compact.

Proof. Properties (ii) and (iii) are equivalent by the definition of quasi-compactness. As a quasi-compact open is a finie union of affine open sets, for two quasi-compact open subsets U, V of X, $U \times_{\mathbb{Z}} V$ is a quasi-compact open subset of $X \times_{\mathbb{Z}} X$ (Corollary 22.3.2), with inverse image $U \cap V$ under Δ_X, hence (i) implies (iii). It is clear that (iii) implies (iv); finally, if (iv) holds, the $U_\alpha \times_{\mathbb{Z}} U_\beta$ form a covering of $X \times_{\mathbb{Z}} X$ by quasi-compact open sets and the inverse image of $U_\alpha \times_{\mathbb{Z}} U_\beta$ under Δ_X is $U_\alpha \cap U_\beta$, hence quasi-compact. It then follows that Δ_X is quasi-compact, so (iv) implies (i). □

Corollary 22.6.11. *Any locally Noetherian scheme X is quasi-separated, and any morphism $f : X \to Y$ is then quasi-separated.*

Proof. It suffices to note that any quasi-compact open subset of X is Noetherian, so X is quasi-separated by Proposition 22.6.10 and any morphism $f : X \to Y$ is quasi-separated by Proposition 22.6.9, since any open subscheme of X is again locally Noetherian. □

Proposition 22.6.12. *Let $f : X \to Y$ be a morphism and $g : Y' \to Y$ be a base change that is surjective and quasi-compact. Put $f' = f_{(Y')}$ and consider the following properties:*

(i) quasi-compact;

(ii) quasi-separated.

Then if $\mathcal{P}$ denotes one of these properties and f' possesses the property $\mathcal{P}$, then f possesses the property $\mathcal{P}$.

Proof. Let $g' : X' \to X$ be the cannical projection, which is surjective and quasi-compact (Proposition 22.3.26 and Proposition 22.6.3(iii)). If f' is quasi-compact, so is $g \circ f'$ and since $f \circ g' = g \circ f'$ we conclude that f is quasi-compact by Proposition 22.6.3(v).

Now assume that f' is quasi-separated. We have $X' \times_{Y'} X' = (X \times_Y X)_{(Y')}$ and $\Delta_{f'} = (\Delta_f)_{(Y')}$. The projection $X' \times_{Y'} X' \to X \times_Y X$ is quasi-compact and surjective by the same reasoning, and we can apply (i) to the morphism Δ_f. Since by hypothesis $\Delta_{f'}$ is quasi-compact, we conclude that Δ_f is quasi-compact, so f is quasi-separated. □

Proposition 22.6.13. *Let $f_i : X_i \to Y$ be a finite family of morphisms and $f : X \to Y$ be their coproduct. Then for f to be quasi-compact (resp. quasi-separated), it is necessary and sufficient that each f_i is quasi-compact (resp. quasi-separated).*

Proof. The assertion about quasi-compactness follows from definition. We also note that $X \times_Y X$ is the coproduct of that $X_i \times_Y X_j$, and Δ_f is the morphism that coincides with Δ_{f_i} on each X_i, so the assertion for quasi-separatedness also follows. □

Theorem 22.6.14. *Let X be a quasi-compact and quasi-separated scheme, $\mathscr{L}$ be an invertible $\mathscr{O}_X$-module, s be a section over X, X_s the open subset of $x \in X$ such that $s(x) \neq 0$, and $\mathscr{F}$ be a quasi-coherent $\mathscr{O}_X$-module.*

(a) If $t \in \Gamma(X, \mathscr{F})$ is such that $t|_{X_s} = 0$, there exists $n > 0$ such that $t \otimes s^{\otimes n} = 0$.

(b) For any section $t \in \Gamma(X_s, \mathscr{F})$, there exists an integer $n > 0$ such that $t \otimes s^{\otimes n}$ can be extended to a section $t' \in \Gamma(X, \mathscr{F} \otimes \mathscr{L}^{\otimes n})$.

Proof. As the space X is a finite union of affine opens U_i such that $\mathscr{L}|_{U_i}$ is isomorphic to $\mathscr{O}_X|_{U_i}$, we can assume that X is affine and $\mathscr{L} = \mathscr{O}_X$. The assertion (a) then follows from Theorem 22.1.20(iv).

Now let t be a sectin of $\mathscr{F}$ over X_s. Since $\mathscr{L}|_{U_i}$ is isomorphic to $\mathscr{O}_X|_{U_i}$, the restriction $(t \otimes s^{\otimes n})|_{U_i \cap X_s}$ is identified with $(t|_{U_i \cap X_s})(s|_{U_i \cap X_s})^n$ under the isomorphism $(\mathscr{F} \otimes \mathscr{L}^{\otimes n})|_{U_i} \cong \mathscr{F}|_{U_i}$. We then conclude from Theorem 22.1.20(iv) that there exists an integer $n \geq 0$ such that for each i, $(t \otimes s^{\otimes n})|_{U_i \cap X_s}$ extends to a section t_i of $\mathscr{F} \otimes \mathscr{L}^{\otimes n})$ over U_i. Let t_{ij} be the restriction of t_i to $U_i \cap U_j$; by definition we have $(t_{ij} - t_{ji})|_{X_s \cap U_i \cap X_j} = 0$. Since X is quasi-separated, $U_i \cap U_j$ is quasi-compact, so by Theorem 22.1.20(iv) there exists an integer $m \geq 0$ such that $(t_{ij} - t_{ji}) \otimes s^{\otimes m} = 0$. The sections $t_i \otimes s^{\otimes m}$ then glue together to give a section $t' \in \Gamma(X, \mathscr{F} \otimes \mathscr{L}^{\otimes(n+m)})$, which induces $t_i \otimes s^{\otimes m}$ over each U_i, and hence induces $t \otimes s^{\otimes(n+m)}$ over X_s. □

Corollary 22.6.15. *With the hypotheses of Theorem 22.6.14, consider the ring $A = \Gamma_*(\mathscr{L})$ and the graded A-module $M = \Gamma_*(\mathscr{L}, \mathscr{F})$ of type $\mathbb{Z}$. Then for each $s \in A_n$, there exists a canonical isomorphism $\Gamma(X_s, \mathscr{F}) \cong M_{(s)}$, where $M_{(s)} = (M_s)_0$ is the degree zero part of the localization M_s.*

Proof. With the notations of Theorem 22.6.14(b), we see that any element $t \in \Gamma(X_s, \mathscr{F})$ corresponds to an element t'/s^n in $M_{(s)}$, which is independent of the integer n and the chosen extension t', in view of Theorem 22.6.14(a). It is immediate that this defines a homomorphism, and is bijective. □

Corollary 22.6.16. *Let X be a quasi-compact and quasi-separated scheme and $\mathscr{F}$ a quasi-coherent $\mathscr{O}_X$-module. Then if $A = \Gamma(X, \mathscr{O}_X)$ and $M = \Gamma(X, \mathscr{F})$, the A_s-module $\Gamma(X_s, \mathscr{F})$ is canonically isomorphic to M_s.*

Proof. This is a special case of Corollary 22.6.15, by taking $\mathscr{L} = \mathscr{O}_X$. □

Proposition 22.6.17. *Let X be a quasi-compact scheme, $\mathscr{F}$ be a quasi-coherent $\mathscr{O}_X$-module of finite type, and $\mathscr{I}$ be a quasi-coherent ideal of $\mathscr{O}_X$ of finite type such that* $\operatorname{supp}(\mathscr{F})$ *is contained in* $\operatorname{supp}(\mathscr{O}_X/\mathscr{I})$. *Then there exists an integer $n \geq 0$ such that $\mathscr{I}^n\mathscr{F} = 0$.*

Proof. As X is a finite union of affine open subsets, we may assume that $X = \operatorname{Spec}(A)$ is affine. Then $\mathscr{F} = \widetilde{M}$ and $\mathscr{I} = \tilde{\mathfrak{a}}$, where M is a finitely generated A-module and $\mathfrak{a}$ is a finitely generated ideal of A, and

$$\operatorname{supp}(\mathscr{F}) = \operatorname{supp}(M) = V(\operatorname{Ann}(M)), \quad \operatorname{supp}(\mathscr{O}_X/\mathscr{I}) = \operatorname{supp}(A/\mathfrak{a}) = V(\mathfrak{a}).$$

By hypothesis we have $V(\operatorname{Ann}(M)) \subseteq V(\mathfrak{a})$, so $\mathfrak{a} \subseteq \sqrt{\operatorname{Ann}(M)}$. Since $\mathfrak{a}$ is finitely generated, there exists an integer $n \geq 0$ such that $\mathfrak{a}^n \subseteq \operatorname{Ann}(M)$, and therefore $\mathscr{I}^n\mathscr{F} = \widetilde{\mathfrak{a}^n M} = 0$. □

Corollary 22.6.18. *Under the hypothesis of Proposition 22.6.17, there exists a closed subscheme Y of X with underlying space* $\operatorname{supp}(\mathscr{O}_X/\mathscr{I})$ *such that, if $j : Y \to X$ is the canonical injection, we have $\mathscr{F} = j_*(j^*(\mathscr{F}))$.*

Proof. Note that the support of $\mathscr{O}_X/\mathscr{I}$ and $\mathscr{O}_X/\mathscr{I}^n$ are the same because if $\mathscr{I}_x = \mathscr{O}_{X,x}$, we also have $\mathscr{I}_x^n = \mathscr{O}_{X,x}$, and on the other hand we have $\mathscr{I}_n^x \subseteq \mathscr{I}_x$ for each $x \in X$. In view of Proposition 22.6.17, we may then suppose that $\mathscr{I}\mathscr{F} = 0$, so $\mathscr{F}$ is also an $(\mathscr{O}_X/\mathscr{I})$-module. If Y is the subscheme defined by $\mathscr{I}$, the conclusion is immediate. □

22.6.2 Morphisms of finite type and of finite presentation

Let $f : X \to Y$ be a morphism of schemes, x be a point of X, and $y = f(x)$. We say f is **of finite type** (resp. **of finite presentation**) **at the point x** if there exist an affine neighborhood V of y and an affine neighborhood U of x such that $f(U) \subseteq V$ and $\Gamma(U, \mathscr{O}_X)$ is a $\Gamma(V, \mathscr{O}_Y)$-algebra of finite type (resp. of finite presentation). We say f is **locally of finite type** (resp. **locally of finite presentation**) if it is of finite type (resp. of finite presentation) at every point of X. In this case, we say the Y-scheme X is locally of finite type (resp. locally of finite presentation) over Y.

Lemma 22.6.19. *Let $f : X \to Y$ be a morphism of schemes, x be a point of X, and $y = f(x)$. If there exist an affine neighborhood V of y and an affine neighborhood U of x such that $f(U) \subseteq V$ and $\Gamma(U, \mathscr{O}_X)$ is a $\Gamma(V, \mathscr{O}_Y)$-algebra of finite type (resp. of finite presentation), then for any affine open neighborhoods U' of x and V' of y, there exist affine open neighborhoods $U_1 \subseteq U \cap U'$ of x and $V_1 \subseteq V \cap V'$ of y, respectively of the form* $\operatorname{Spec}(\Gamma(U', \mathscr{O}_X)_{s'})$ *and* $\operatorname{Spec}(\Gamma(V', \mathscr{O}_Y)_{t'})$, *such that $f(U_1) \subseteq V_1$ and $\Gamma(U_1, \mathscr{O}_X)$ is a $\Gamma(V_1, \mathscr{O}_Y)$-algebra of finite type (resp. of finite presentation).*

Proof. Let $t' \in \Gamma(V', \mathcal{O}_Y)$ such that $V_1 = \mathrm{Spec}(\Gamma(V', \mathcal{O}_Y)_t)$ is an affine neighborhood of y contained in $V \cap V'$ and choose $s'_0 \in \Gamma(U', \mathcal{O}_X)$ such that $U'' = \mathrm{Spec}(\Gamma(U', \mathcal{O}_X)_{s'_0})$ is a neighborhood of x contained in $U \cap U' \cap f^{-1}(V_1)$. There then exists $s \in \Gamma(U, \mathcal{O}_X)$ such that $U_1 = \mathrm{Spec}(\Gamma(U, \mathcal{O}_X)_s)$ is a neighborhood of x contained in U''. If s'' is the image of s in $\Gamma(U'', \mathcal{O}_X)$, we then have $U_1 = \mathrm{Spec}(\Gamma(U'', \mathcal{O}_X)_{s''})$, so there exists $s' \in \Gamma(U', \mathcal{O}_X)$ such that $U_1 = \mathrm{Spec}(\Gamma(U', \mathcal{O}_X)_{s'})$. Now $\Gamma(U_1, \mathcal{O}_X) = \Gamma(U, \mathcal{O}_X)[1/s]$, so it is a $\Gamma(U, \mathcal{O}_X)$-algebra of finite presentation, and a fortiori a $\Gamma(V, \mathcal{O}_Y)$-algebra of finite type (resp. of finite presentation). The homomorphism $\Gamma(V, \mathcal{O}_Y) \to \Gamma(U_1, \mathcal{O}_X)$ factors into

$$\Gamma(V, \mathcal{O}_X) \longrightarrow \Gamma(V_1, \mathcal{O}_Y) \longrightarrow \Gamma(U_1, \mathcal{O}_X)$$

If $\Gamma(U_1, \mathcal{O}_X)$ is identified with a quotient algebra $\Gamma(V, \mathcal{O}_Y)[T_1, \dots, T_n]/\mathfrak{a}$, then it is also identified with the quotient algebra $\Gamma(V_1, \mathcal{O}_Y)[T_1, \dots, T_n]/\mathfrak{b}$, where $\mathfrak{b}$ is the ideal generated by $\mathfrak{a}$. It then follows that $\Gamma(U_1, \mathcal{O}_X)$ is a $\Gamma(V_1, \mathcal{O}_Y)$-algebra of finite type (resp. finite presentation). □

Proposition 22.6.20. *If Y is locally Noetherian, then $f : X \to Y$ is locally of finite type if and only if it is locally of finite presentation. Moreover, if this holds, then X is also locally Noetherian.*

Proof. The first assertion is clear since we can take $\Gamma(V, \mathcal{O}_Y)$ to be Noetherian. The second one follows because $\Gamma(U, \mathcal{O}_X)$ is then also Noetherian. □

Proposition 22.6.21 (Properties of Morphisms Locally of Finite Type).

(i) Any local immersion is locally of finite type.

(ii) If $f : X \to Y$ and $g : Y \to Z$ are two morphisms locally of finite type, then $g \circ f$ is locally of finite type.

(iii) If $f : X \to Y$ is an S-morphism locally of finite type, $f_{(S')} : X_{(S')} \to Y_{(S')}$ is locally of finite type for any base change $g : S' \to S$.

(iv) If $f : X \to X'$ and $g : Y \to Y'$ are two S-morphisms locally of finite type, $f \times_S g$ is locally of finite type.

(v) If the composition $g \circ f$ of two morphisms is locally of finite type, then f is locally of finite type.

(vi) If a morphism f is locally of finite type, so is f_{red}.

Proof. Assertion (vi) follows from the fact that if a ring homomorphism $A \to B$ is of finite type, then so is $A/\mathfrak{n}(A) \to B/\mathfrak{n}(B)$. Now in view of Proposition 22.5.14, it suffices to prove (i), (ii) and (iii). If $j : X \to Y$ is a local immersion, for any $x \in X$ there exists an affine open neighborhood V of $j(x)$ in Y and an affine open neighborhood U of x such that the restriction $U \to V$ of j is a closed immersion. Then $\Gamma(U, \mathcal{O}_X)$ is a quotient ring of $\Gamma(V, \mathcal{O}_Y)$, and is therefore of finite type.

To establish (iii), we may assume that $Y = S$; let $p : X_{(S')} \to X$ and $q : X_{(S')} \to S$ be the canonical projections, x' be a point of $X_{(S')}$, and $x = p(x')$, $s' = q(x')$, $s = f(p(x')) = g(q(x'))$. Let V be an affine neighborhood of s in S and U be an affine neighborhood of x in X such that $f(U) \subseteq V$ and $\Gamma(U, \mathcal{O}_X)$ is a $\Gamma(V, \mathcal{O}_S)$-algebra of finite type. Let V' be an affine open neighborhood of s' in S' contained in $g^{-1}(V)$; then $p^{-1}(U) \cap q^{-1}(V)$ is an affine neighborhood of x' and is identified with $U \times_V V'$ (Corollary 22.3.2). This is an affine scheme with ring $\Gamma(U, \mathcal{O}_X) \otimes_{\Gamma(V, \mathcal{O}_S)} \Gamma(V', \mathcal{O}_{S'})$; as this is a $\Gamma(V', \mathcal{O}_{S'})$-algebra of finite type, we see (iii) follows.

Finally, to prove (ii), consider a point $x \in X$; there exists by hypothesis an affine open neighborhood W of $g(f(x))$ in Z and an affine open neighborhood V of $f(x)$ in Y such that $g(V) \subseteq W$ and $\Gamma(V, \mathcal{O}_Y)$ is a $\Gamma(W, \mathcal{O}_Z)$-algebra of finite type. By Lemma 22.6.19 there exists an affine open neighborhood $V' \subseteq V$ of $f(x)$ and an affine open neighborhood $U \subseteq f^{-1}(V')$ of x such that $\Gamma(V', \mathcal{O}_Y)$ is a $\Gamma(V, \mathcal{O}_Y)$-algebra of finite type and $\Gamma(U, \mathcal{O}_X)$ is a $\Gamma(V', \mathcal{O}_Y)$-algebra of finite type. We then conclude that $\Gamma(U, \mathcal{O}_X)$ is a $\Gamma(W, \mathcal{O}_Z)$-algebra of finite type, so (ii) follows. □

Corollary 22.6.22. *Let $f : X \to Y$ be a morphism locally of finite type. For any morphism $Y' \to Y$ such that Y' is locally Noetherian, $X \times_Y Y'$ is locally Noetherian.*

Proof. This follows from Proposition 22.6.20, since $f_{(Y')} : X \times_Y Y' \to Y'$ is locally of finite type by Proposition 22.6.21. □

Proposition 22.6.23. *Let $\rho : A \to B$ be a homomorphism of rings. For the corresponding morphism $f : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ to be locally of finite type, it is necessary and sufficient that B is an A-algebra of finite type.*

Proof. This condition is clearly sufficient. Conversely, assume that f is locally of finite type. Then by Lemma 22.6.19 there exists a finite cover of $\mathrm{Spec}(B)$ by open sets $D(g_i)$ (where $g_i \in B$) such that B_{g_i} is an A-algebra of finite type. Since the $D(g_i)$'s cover $\mathrm{Spec}(B)$, we see g_i generate the ring B, and it follows from Corollary 10.4.54 that B is of finite type over A. □

Proposition 22.6.24 (Properties of Morphisms Locally of Finite Presentation).

(i) Any local isomorphism is locally of finite presentation.

(ii) If two morphisms $f : X \to Y$, $g : Y \to Z$ are locally of finite presentation, so is $g \circ f$.

(iii) If $f : X \to Y$ is an S-morphism locally of finite presentation, $f_{(S')} : X_{(S')} \to Y_{(S')}$ is locally of finite presentation for any base change $g : S' \to S$.

(iv) If $f : X \to X'$ and $g :\to Y'$ are two S-morphisms locally of finite presentation, $f \times_S g$ is locally of finite presentation.

(v) If the compositin $g \circ f$ of two morphisms $f : X \to Y$, $g : Y \to Z$ is locally of finite presentation and if g is locally of finite type, then f is locally of finite presentation.

Proof. The first assertion is trivial, and to prove (ii), (iii), it suffices to replace the "algebra of finite type" in the proof of Proposition 22.6.21 by "algebra of finite presentation", and use Lemma 22.6.19. Again, assertion (iv) then follows from these. For (v), consider the cartesian square

$$\begin{tikzcd} X \arrow[r, "\Gamma_f"] \arrow[d, "f"'] & X \times_Z Y \arrow[d, "f \times_Z 1_Y"] \\ Y \arrow[r, "\Delta_g"] & Y \times_Z Y \end{tikzcd}$$

If we can show that Δ_g is locally of finite presentation, then it follows from (iii) that Γ_f is also locally of finite presentation. But f factors into

$$X \xrightarrow{\Gamma_f} X \times_Z Y \xrightarrow{p_2} Y$$

and we have $p_2 = (g \circ f) \times_Z 1_Y$, which is locally of finite presentation by (iv) since $g \circ f$ is. We then deduce that f is locally of finite presentation.

It then suffices to prove that is $g : Y \to Z$ is a morphism locally of finite type, then the diagonal morphism $\Delta_g : Y \to Y \times_Z Y$ is locally of finite presentation. To do this we may assume that $Z = \mathrm{Spec}(A)$, $Y = \mathrm{Spec}(B)$, and B is an A-algebra of finite type. The diagonal Δ_g corresponds to the homomorphism $\pi : B \otimes_A B \to B$ such that $\pi(x \otimes y) = xy$. Let $\mathfrak{I}$ be the kernel of π. We claim that $\mathfrak{I}$ is generated by the elements $1 \otimes s - s \otimes 1$, where s runs through a system of generators for the A-algebra B (this then proves the claim since B is of finite type over A). Now, it is clear that for any $x \in B$, we have $x \otimes 1 - 1 \otimes x \in \mathfrak{I}$; on the other hand, for $x, y \in B$, we have

$$x \otimes y = xy \otimes 1 + (x \otimes 1)(1 \otimes y - y \otimes 1)$$

If $\sum_i (x_i \otimes y_i) \in \mathfrak{I}$, we have by definition that $\sum_i x_i y_i = 0$, so

$$\sum_i (x_i \otimes y_i) = \sum_i (x_i \otimes 1)(1 \otimes y_i - y_i \otimes 1).$$

Moreover, if $x = st$, then

$$x \otimes 1 - 1 \otimes x = (s \otimes 1)(t \otimes 1 - 1 \otimes t) + (s \otimes 1 - 1 \otimes t)(1 \otimes t).$$

The claim then follows by indcution on the number of factors of a product in B. □

Corollary 22.6.25. *Let $g : Y \to Z$ be a morphism locally of finite type. Then the diagonal morphism $\Delta_g : Y \to Y \times_Z Y$ is locally of finite presentation.*

Proof. This is contained in the proof of Proposition 22.6.24. □

Proposition 22.6.26. *Let A be a ring, B be an A-algebra, $B' = A[T_1, \ldots, T_n]$, and $\rho : B' \to B$ be a surjective homomorphism of A-algebras. Then for B to be an A-algebra of finite presentation, it is necessary and sufficient that the kernel $\mathfrak{a}$ of ρ is finitely generated in B'.*

Proof. The condition is sufficient by definition. Conversely, we note that the morphism $g : \mathrm{Spec}(B') \to \mathrm{Spec}(A)$ is locally of finite type; if B is an A-algebra of finite presentation, the morphism $f : \mathrm{Spec}(B) \to \mathrm{Spec}(B')$ corresponding to ρ and $g \circ f : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ are locally of finite presentation, so it follows from Proposition 22.6.24(v) that f is locally of finite presentation. Now to show that $\mathfrak{a}$ is finitely generated, it suffices to apply Proposition 10.4.55. □

Corollary 22.6.27. *Let X, Y be two schemes, $j : X \to Y$ be an immersion, U an open subset of Y such that $j(X)$ is closed in U, and $\mathcal{I}$ the quasi-coherent ideal of $\mathcal{O}_U$ defining the closed subscheme of Y associated with j. For j to be locally of finite presentation, it is necessary and sufficient that $\mathcal{I}$ is a $\mathcal{O}_U$-module of finite type.*

Proof. Since the question is local, we can assume that X and Y are affine. The assertion then reduces to Proposition 22.6.26. □

Proposition 22.6.28. *Let $\rho : A \to B$ be a ring homomorphism. For the corresponding morphism $f : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ to be locally of finite presentation, it is necessary and sufficient that B is an A-algebra of finite presentation.*

Proof. The condition is clearly sufficient, so we only need to prove the necessity. If f is locally of finite presentation, then it follows from Proposition 22.6.23 that B is an A-algebra of finite type, so there exists a surjective homomorphism $\rho : C' = A[T_1, \dots, T_n] \to B$ of A-algebras. It then follows from Proposition 22.6.24(v) that the closed immersion $j : \mathrm{Spec}(B) \to \mathrm{Spec}(B')$ is locally of finite presentation, so, if $\mathfrak{b}$ is the kernel of ρ, the $\widetilde{B'}$-module $\tilde{\mathfrak{b}}$ is of finite type, and $\mathfrak{b}$ is therefore finitely generated in B' by Corollary 22.1.23. □

Proposition 22.6.29. *Let $\rho : A \to B$ be a homomorphism of rings such that B is a finite A-algebra. For B to be an A-algebra of finite presentation, it is necessary and sufficient that B is an A-module of finite presentation.*

Proof. There exists a finite A-algebra B' of finite presentation B' that is a free A-module, and a surjective A-homomorphism of A-algebras $u : B' \to B$ (Proposition 7.2.33); we have a surjective A-homomorphism $v : B'' = A[T_1, \dots, T_m] \to B'$ with kernel finitely generated. If $w = v \circ u : B'' \to B$ and $\mathfrak{b}$ (resp. $\mathfrak{a}$) is the kernel of w (resp. u), we have $\mathfrak{a} = v(\mathfrak{b})$ since v is surjective. If B is an A-algebra of finite presentation, $\mathfrak{b}$ is a finitely generated ideal of B'' by Proposition 22.6.26, so $\mathfrak{a}$ is a finitely generated ideal in B', hence a finitely generated A-module since B' is a finite A-algebra. As B' is a free A-module, B is then an A-module of finite presentation. The converse is proved in Corollary 7.2.34. □

Proposition 22.6.30. *Let $f : X \to Y$ be a local immersion of finite type at a point of $y \in Y$. The following conditions are equivalent:*

(i) f is an open map at y.

(ii) There exists an open neighborhood U of y in Y such that $f|_U$ is a nilimmersion over the open subscheme U.

(iii) There exists an open neighborhood U of y in Y such that $f|_U$ is a nilpotent immersion over the open subscheme U.

Proof. It is clear that (iii) implies (ii) and (ii) implies (i). To show that (i) implies (iii), we can, by restricting f, suppose that f is a closed immersion from an affine open U of Y to an affine open V of X. Moreover, by choosing an irreducible component containing $f(y)$, we can further assume that V is irreducible. As f is a homeomorphism from U to $f(U)$, the hypothesis of (i) then implies that $f(U) = V$ since V is connected. If $V = \mathrm{Spec}(A)$, $U = \mathrm{Spec}(B)$, we have $B = A/\mathfrak{a}$, where $\mathfrak{a}$ is a nilideal of A. On the other hand, in view of Lemma 22.6.19, we can, by replacing A with a fraction field A_s, suppose that B is an A-algebra of finite presentation. But then $\mathfrak{a}$ is a finitely generated ideal of A by Proposition 22.6.26, so it is nilpotent. □

Proposition 22.6.31. *Let $f : X \to Y$ be a morphism locally of finite type. Suppose that f admits a Y-section g, and for every $y \in Y$, the fiber $X_y = f^{-1}(y)$ is a $\kappa(y)$-scheme $\kappa(y)$-isomorphic to* $\mathrm{Spec}(\kappa(y))$ *(and necessarily has underlying space $\{g(y)\}$). Then f is an isomorphism.*

Proof. In fact, g is a nilimmersion of Y to X (Corollary 22.5.8), so the image $g(Y)$ has underlying space X and is defined by a nilideal $\mathscr{I}$ of $\mathscr{O}_X$. As $f \circ g = 1_Y$ and f is locally of finite type, g is locally of finite presentation by Proposition 22.6.24(v), so $\mathscr{I}$ is an ideal of finite type of $\mathscr{O}_X$

(Corollary 22.6.27). For any $y \in Y$, put $x = g(y)$, and consider the following exact sequence:

$$\begin{tikzcd} 0 \arrow[r] & \mathscr{I}_x \arrow[r] & \mathscr{O}_{X,x} \arrow[r, shift left, "g_y^\#"] & \mathscr{O}_{Y,y} \arrow[l, shift left, bend left, "f_x^\#"] \arrow[r] & 0 \end{tikzcd}$$

The relation $f \circ g = 1_Y$ implies $f_x^\# \circ g_y^\# = 1$, so the above exact sequence splits. By tensoring with $\kappa(y) = \mathscr{O}_{Y,y}/\mathfrak{m}_y$, we then get an isomorphism $\mathscr{O}_{X,x}/\mathfrak{m}_y\mathscr{O}_{X,x} \cong \kappa(y) \oplus (\mathscr{I}_x/\mathfrak{m}_y\mathscr{I}_x)$. But the hypothesis on X_y implies that $\kappa(y)$-isomorphic to $\kappa(y)$, so we deduce that $\mathfrak{m}_y\mathscr{I}_x = \mathscr{I}_x$ and a fortiori $\mathfrak{m}_x\mathscr{I}_x = \mathscr{I}_x$. As $\mathscr{I}_x$ is a finitely generated ideal of $\mathscr{O}_{X,x}$, by Nakayama's lemma we conclude $\mathscr{I}_x = 0$, so $\mathscr{I} = 0$ and f is an isomorphism. □

Corollary 22.6.32. *Let X, Y be two S-schemes and $f : X \to Y$ be an S-morphism. Suppose that X is locally of finite type over S. For each $s \in S$, let X_s, Y_s be the fiber of X and Y at the point s, and $f_s : X_s \to Y_s$ be the morphism induced by f under the base change* $\mathrm{Spec}(\kappa(s)) \to S$. *Then if for each $s \in S$, f_s is a monomorphism, f is a monomorphism.*

Proof. If f_s is a monomorphism, so is $f_y : X_y \to \mathrm{Spec}(\kappa(y))$. By hypothesis f is locally of finite type (Proposition 22.6.21(v)), so we can limit ourselves to the case $Y = S$. To see that f is a monomorphism, it suffices to prove that the first projection $p : X \times_S X \to X$ is an isomorphism (Proposition 22.5.5). Now the hypothesis on f_s implies that the projections $p_s : X_s \otimes_{\kappa(s)} X_s \to X_s$ are isomorphisms for all $s \in S$. Since p admits an S-section, namely the diagonal Δ_f, it follows from Proposition 22.6.31 that p is an isomorphism. □

We now come to the definition of *morphisms of finite type*, which can be seen as a global version of morphisms locally of finite type. Briefly speaking, the notion of finite type concerns the "global finiteness" of a morphism: we have the following definition and proposition.

Proposition 22.6.33. *Let $f : X \to Y$ be a morphism and (U_α) be a covering of Y by affine opens. The following conditions are equivalent:*

(i) f is locally of finite type and quasi-compact.

(ii) For each α, $f^{-1}(U_\alpha)$ is a finite union of affine opens $V_{\alpha,i}$ such that the ring $\Gamma(V_{\alpha,i}, \mathscr{O}_X)$ is a $\Gamma(U_\alpha, \mathscr{O}_Y)$-algebra of finite type.

(iii) For any affine open U of Y, $f^{-1}(U)$ is a finite union of affine opens V_j such that $\Gamma(V_j, \mathscr{O}_X)$ is a $\Gamma(U, \mathscr{O}_X)$-algebra of finite type.

We say the morphism f is ***of finite type*** *if it satisfies the above equivalent conditions. In this case, we say X is of finite type over Y.*

Proof. It is clear that (iii)⇒(ii)⇒(i). To prove that (i) implies (iii), we may assume that $Y = U$ is affine; then X is quasi-compact, hence is a finte union of affine opens V_j such that the restriction $V_j \to U$ of f is locally of finite type. By Proposition 22.6.23, we see $\Gamma(V_j, \mathscr{O}_X)$ is a $\Gamma(U, \mathscr{O}_X)$-algebra of finite type. □

Proposition 22.6.34. *Let $f : X \to Y$ be a morphism of finite type. If Y is Noetherian (resp. locally Noetherian), so is X.*

Proof. This follows from Proposition 22.6.20 and Proposition 4.1.15. □

Proposition 22.6.35 (Properties of Morphisms of Finite Type).

(i) Any quasi-compact immersion is of finite type.

(ii) The composition of two morphisms of finite type is of finite type.

(iii) If $f : X \to Y$ is an S-morphism of finite type, $f_{(S')} : X_{(S')} \to Y_{(S')}$ is of finite type for any base change $S' \to S$.

(iv) If $f : X \to X'$ and $g : Y \to Y'$ are two S-morphisms of finite type, $f \times_S g$ is of finite type.

(v) If the composition $g \circ f$ of two morphisms $f : X \to Y$, $g : Y \to Z$ is of finite type and if g is quasi-separated or X is Noetherian, then f is of finite type.

(vi) If a morphism f is of finite type, so is f_{red}.

Proof. This follows directly from Proposition 22.6.21 and Proposition 22.6.3. □

Corollary 22.6.36. *Let $f : X \to Y$ be a morphism of finite type. For any morphism $Y' \to Y$ such that Y' is Noetherian, $X \times_Y Y'$ is Noetherian.*

Proof. This follows from Proposition 22.6.35(iii) and Proposition 22.6.34. □

Corollary 22.6.37. *Let X be a scheme of finite type over a locally Noetherian scheme S. Then any S-morphism $f : X \to Y$ is of finite type.*

Proof. The morphism f is locally of finite type by Proposition 22.6.21(v). To see it is quasi-compact, we can suppose that S is Noetherian. If $\varphi : X \to S$ and $\psi : Y \to S$ are the structural morphism, we have $\varphi = \psi \circ f$ and X is Noetherian by Proposition 22.6.34, so f is of finite type, by Proposition 22.6.35(v). □

Let X and Y be two schemes. We say a morphism $f : X \to Y$ is **of finite presentation** if it satisfies the following conditions:

(i) f is locally of presentation;

(ii) f is quasi-compact;

(iii) f is quasi-separated.

In this case, we say X is **of finite presentation over Y**, or is an **Y-scheme of finite presentation**. It is clear that condition (iii) is automatic if f is separated, or if X is locally Noetherian. If Y is locally Noetherian, then again, f is of finite type if and only if it is of finite presentation, and in this case X is also locally Noetherian.

Proposition 22.6.38 (Properties of Morphisms of Finite Presentation).

(i) Any quasi-compact immersion that is locally of finite presentation (in particular any quasi-compact open immersion) is of finite presentation.

(ii) The composition of two morphisms of finite presentation is of finite presentation.

(iii) If $f : X \to Y$ be an S-morphism of finite presentation, $f_{(S')} : X_{(S')} \to Y_{(S')}$ is of finite presentation for any base change $S' \to S$.

(iv) *If $f : X \to X'$ and $g : Y \to Y'$ are two S-morphisms of finite presentation, $f \times_S g$ is of finite presentation.*

(v) *If the composition $g \circ f$ of two morphisms $f : X \to Y$, $g : Y \to Z$ is of finite presentation and if g is quasi-separated and locally of finite type, then f is of finite presentation.*

Proof. This follows immediately from Proposition 22.6.3, Proposition 22.6.7, and Proposition 22.6.24. □

It follows from Proposition 22.6.38(iii) that if f is a morphism of finite presentation and U is an open subset of Y, the restriction $f^{-1}(U) \to U$ of f is also of finite presentation. conversely, let (U_α) be a covering of Y by affine opens and suppose that the restriction $f^{-1}(U_\alpha) \to U_\alpha$ of f is a morphism of finite presentation. Then it follows that f is of finite presentation, since f is clearly of finite presentation and quasi-compact and it is quasi-separated by Proposition 22.6.9.

If X is a quasi-separated scheme, any morphism $f : X \to Y$ is quasi-separated by Corollary 22.6.8. Therefore, if f is quasi-compact and locally of finite presentation, it is of finite presentation.

Corollary 22.6.39. *Let $\rho : A \to B$ be a ring homomorphism. For the corresponding morphism $f :$ $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ to be of finite type (resp. of finite presentation), it is necessary and sufficient that B is an A-algebra of finite type (resp. of finite presentation).*

Proof. Since any morphism of affine schemes is quasi-compact and separated, this follows from Proposition 22.6.23 and Proposition 22.6.28. □

Remark 22.6.1. In the definition of morphisms of finite presentation, the condition (iii) is not a concequence of the other two conditions. For example, let Y be a non-Noetherian affine scheme and let Y be a non-quasi-compact open subset of Y (an example for this is $Y = \mathrm{Spec}(k[x_1, x_2, \dots])$ and $U = Y - \{0\}$, cf. Example 22.6.2). Let X be the scheme obtained by glueing two schemes Y_1, Y_2 isomorphic to Y along the open sets U_1, U_2 corresponding to U, so that X is the union of two affine opens isomorphic to Y_1, Y_2, respectively, and $Y_1 \cap Y_2 = U$. Let $f : X \to Y$ be the morphism which coincides with the canonical isomorphism $Y_i \to Y$ on each Y_i. Then it is clearly locally of finite presentation, and is quasi-compact since the inverse image of a quasi-compact open of Y is the union of its images in Y_1 and Y_2; but as $Y_1 \cap Y_2 = U$ is not quasi-compact, it is not quasi-separated by Proposition 22.6.10 and Corollary 22.6.8(ii).

Proposition 22.6.40. *Let $f_i : X_i \to Y$ be a finite family of morphisms and $f : X \to Y$ be their coproduct, where $X = \coprod_i X_i$. Then for f to be of finite type (resp. finite presentation), it s necessary and sufficient that each f_i is.*

Proof. In view of Proposition 22.6.13, it suffices to note that the same assertion holds for morphisms of locally finite type and of finite presentation. □

22.6.3 Algebraic schemes

We say a K-scheme is **algebraic** (resp. **locally algebraic**) if it is of finite type over K (resp. locally of finite type over K). The field K is called the **base field** of X.

Proposition 22.6.41. *Let K be a field. A locally algebraic (resp. algebraic) K-scheme is locally Noetherian (Noetherian). Moreover X is a Jacobson scheme and a point $x \in X$ is closed if and only if $\kappa(x)$ is a finite extension of K.*

Proof. The first assertion is clear, and X is Jacobson by **??**. To characterize close points in X, we note that for a point $x \in X$ to be closed, it is necessary and sufficient that for an open covering (U_α) of X, s is closed in the U_α containing it. As there is a covering of X by affine opens U_α such that $\Gamma(U_\alpha, \mathcal{O}_X)$ is a K-algebra of finite type, we can then assume that $X = \operatorname{Spec}(A)$ where A is a K-algebra of finite type. The closed points of X are then maximal ideals of A; but then $A/\mathfrak{p}_x = \kappa(x)$ is a finite extension by Proposition 13.3.13. Conversely, if $\kappa(x)$ is a finite K-algebra, so is the ring $A/\mathfrak{p}_x \subseteq \kappa(x)$, and as an integral K-algebra is also a field (Proposition 13.1.62), we have $A/\mathfrak{p}_x = \kappa(x)$, so x is closed. □

Corollary 22.6.42. *Let K be an algebraically closed field and X be a locally algebraic K-scheme. Then the closed points of X are exactly the rational points of X over K, which are identified with the K-points of X with values in K.*

Proposition 22.6.43. *Let K be a field and X be a locally algebraic scheme over K. Then the following conditions are equivalent:*

(i) X is Artinian.

(ii) The underlying space of X has only finitely many closed points.

(iii) The underlying space of X is finite.

(iv) X is isomorphic to $\operatorname{Spec}(A)$ where A is K-algebra of finite dimension.

If X is algebraic over K, then these conditions are equivalent to the following:

(v) The underlying space of X is discrete.

(vi) The points of X are all closed.

Proof. We see (i) implies any other conditions, and (v) or (vi) implies (i) if X is Noetherian. Moreover, it is clear that (iv) implies (i), since a finite dimensional K-algebra is Artianian. In the condition of (ii), the set X_0 of closed points of X is then finite, closed and very dense in X, whence equal to X and X is therefore Artinian, since it is then Noetherian. □

Corollary 22.6.44. *Let K be a field, X be a locally algebraic K-scheme, and x be a point of X. The following conditions are equivalent:*

(i) x is isolated in X;

(ii) x is closed in X and $\mathcal{O}_{X,x}$ is Artinian;

(iii) $\mathcal{O}_{X,x}$ is a finite dimensional K-algebra.

Proof. If $\mathcal{O}_{X,x}$ is a finite dimensional K-algebra, so is the residue field $\kappa(x) = \mathcal{O}_{X,x}/\mathfrak{m}_x$, so (iii) implies (ii) in view of Proposition 22.6.41. The local ring $\mathcal{O}_{X,x}$ is Artinian signifies that x is a maximal point of X, since a Noetherian local ring is Artinian if and only if it has a unique primei deal. If x is moreover closed, the set $\{x\}$ is closed and stable under generalization, hence

open (**??**), and this proves x is isolated in X. Finally, if x is isolated in X, there exists an affine open neighborhood U of x such that $U = \{x\}$ and $\Gamma(U, \mathcal{O}_X)$ is a finite type K-algebra. But then $\Gamma(U, \mathcal{O}_X) = \mathcal{O}_{X,x}$, so (i) implies (iii). □

If the conditions in Proposition 22.6.43, we say X is a finite scheme over K, or a finite K-scheme. For such a scheme, we denote by $\dim_K(X)$ the dimension of the ring $\Gamma(X, \mathcal{O}_X)$ over K. If X and Y are two finite schemes over K, we have

$$\dim_K(X \amalg Y) = \dim_K(X) + \dim_K(Y), \quad \dim_K(X \times_K Y) = \dim_K(X)\dim_K(Y).$$

Corollary 22.6.45. *Let X be a finite scheme over a field K. For any extension K' of K, $X \otimes_K K'$ is a finite scheme over K', with* $\dim_{K'}(X') = \dim_K(X)$.

Proof. In fact, if $X = \operatorname{Spec}(A)$, we have $[A \otimes_K K' : K'] = [A : K]$, whence the claim. □

Corollary 22.6.46. *Let X be a finite scheme over a field K. We put*

$$n = \sum_{x \in X} [\kappa(x) : K]_s$$

Then, for any algebraically closed extension Ω of K, the underlying space of $X \otimes_K \Omega$ has exactly n points, which are identified with the Ω-valued points of X.

Proof. By Proposition 22.2.30, we can assume that $A = \Gamma(X, \mathcal{O}_X)$ is local; let $\mathfrak{m}$ be the maximal ideal of A, $L = A/\mathfrak{m}$ the residue field, which is a finite algebraic extension of K by Proposition 22.6.43. The Ω-points of X correspond bijectively to Ω-sections of $X \otimes_K \Omega$, and to the closed points of $X \otimes_K \Omega$ by Corollary 22.6.42, and finally to the points of this Artinian scheme (Proposition 22.2.30). They also correspond to K-homomorphisms of L into Ω, and the assertion then follows from the definition of separable degree. □

The number n defined in Corollary 22.6.46 is called the **separable rank** of A (or X) over K, or the **geometric number of points** of X. This is also the number of elements in $X(\Omega)_K$. It follows from this definition that for any extension K' of K, $X \otimes_K K'$ has the same geometric number of points as X. If we denote this number by $n(X)$, it is clear that, if X and Y are two finite schemes over K, we have

$$n(X \amalg Y) = n(X) + n(Y), \quad n(X \times_K Y) = n(X)n(Y).$$

Proposition 22.6.47. *Let $f : X \to Y$ be a morphism locally of finite type (resp. of finite type). Then, for any $y \in Y$, the fiber $X_y = f^{-1}(y)$ is a locally algebraic (resp. algebraic) scheme over $\kappa(y)$, and for each $x \in X_y$, $\kappa(x)$ is a extension of $\kappa(y)$ of finite type.*

Proof. As $X_y = X \otimes_Y \kappa(y)$, this is a concequence of Proposition 22.6.21(iii) and Proposition 22.6.35(iii). □

Proposition 22.6.48. *Let $f : X \to Y$, $g : Y' \to Y$ be two morphisms, and put $X' = X \times_Y Y'$, $f' = f_{(Y')} : X' \to Y'$. Let $y' \in Y'$ and $y = g(y')$. If the fiber $X_y = f^{-1}(y)$ is a finite scheme over $\kappa(y)$, then the fiber $X'_{y'} = f'^{-1}(y')$ is a finite scheme over $\kappa(y')$, and we have*

$$\dim_{\kappa(y')}(X'_{y'}) = \dim_{\kappa(y)}(X_y), \quad n(X'_{y'}) = n(X_y).$$

Proof. This follows from the observation $X'_{y'} = X_y \otimes_{\kappa(y)} \kappa(y')$. □

Proposition 22.6.47 shows that the morphisms of finite type (resp. locally of finite type) correspond intuitively to "algebraic families of algebraic varieties (resp. locally algebraic)", where Y plays the role of "parameters". Because of this, these morphisms are of significant geometric interests. The morphisms which are not locally of finite type will intervene them by the process of "base change", for example by localization and completion.

22.6.4 Local determination of morphisms

Proposition 22.6.49. *Let X and Y be S-schemes, $x \in X$, $y \in Y$ be points lying over the same point $s \in S$.*

(a) Suppose that Y is locally of finite type over S at the point y. Then if two S-morphisms f, g from X to Y are such that $f(x) = g(x) = y$ and the $\mathcal{O}_{S,s}$-homomorphisms $f_x^\#$ and $g_x^\#$ from $\mathcal{O}_{Y,y}$ to $\mathcal{O}_{X,x}$ coincide, then f and g coincide in an open neighborhood of x.

(b) Suppose that Y is locally of finite presentation over S at the point y. Then, for any $\mathcal{O}_{X,x}$-homomorphism $\varphi : \mathcal{O}_{Y,y} \to \mathcal{O}_{X,x}$ there exists an open neighborhood U of x in X and an S-morphism f from U to Y such that $f(x) = y$ and $f_x^\# = \varphi$.

Proof. We first consider case (a). The question is local over S, X and Y, so we can suppose that S, X, Y are affine with rings A, B, C, respectively. The morphisms f and g then correspond to A-homomorphisms ρ, σ from C to B such that $\rho^{-1}(\mathfrak{p}_x) = \sigma^{-1}(\mathfrak{p}_x) = \mathfrak{p}_y$, and the homomorphisms ρ_x and σ_x from C_y to B_x, deduced by ρ and σ, coincide. We can morphism suppose that C is an A-algebra of finite type. Let $(c_i)_{1\leq i\leq n}$ be generators of the A-algebra C, and put $b_i = \rho(c_i)$, $b'_i = \sigma(c_i)$. By hypothesis, we have $b_i/1 = b'_i/1$ in the ring B_x. This means there exist elements $s_i \in B - \mathfrak{p}_x$ such that $s_i(b_i - b'_i) = 0$ for each i, and we can evidently choose one $s \in B - \mathfrak{p}_x$ for all i. We then conclude that $b_i/1 = b'_i/1$ for each i in the ring B_s; if $i_s : B \to B_s$ is the canonical homomorphism, we then have $i_s \circ \rho = i_s \circ \sigma$, so the restriction of f and g on $D(s)$ are identical.

We now come to case (b). Again we can suppose that S, X, Y are affine with rings A, B, C. Put $\mathfrak{p} = \mathfrak{p}_x$, $\mathfrak{q} = \mathfrak{p}_y$, and let $\varphi : C_\mathfrak{q} \to B_\mathfrak{p}$ be an A-homomorphism. We then get an A-homomorphism $\rho : C \to C_\mathfrak{q} \xrightarrow{\varphi} B_\mathfrak{p}$. Since we can consider $B_\mathfrak{p}$ as an inductive limit of the filtered system of A-algebras B_s, where s runs through elements of $B - \mathfrak{p}$, and C is by hypothesis an A-algebra of finite presentation, we deduce from Proposition 7.2.37 that there exists $s \notin \mathfrak{p}$ and an A-homomorphism $\sigma : C \to B_s$ whose canonical image is ρ, that is, the following diagram is commutative

$$\begin{tikzcd} C \arrow[r, "\sigma"] \arrow[d] & B \arrow[d] \\ C_\mathfrak{q} \arrow[r, "\varphi"] & B_\mathfrak{p} \end{tikzcd} \tag{6.4.1}$$

It then suffices to take $U = D(s)$ and let f be the morphism induced by σ. □

Corollary 22.6.50. *Under the hypotheses of Proposition 22.6.49(ii), if moreover X is locally of finite type over S at the point of x, we can choose f to be of finite type.*

Proof. To see this, we can assume that S, X, Y are affine, so that the structural morphisms $X \to S$ and $Y \to S$ are respectively of finite type and of finite presentation; then the results follows from Lemma 22.6.19 and Proposition 22.6.21(iv). □

Corollary 22.6.51. *Retain the hypotheses of Proposition 22.6.49(ii) and suppose that Y is integral and $\varphi : \mathcal{O}_{Y,y} \to \mathcal{O}_{X,x}$ is injective. Then we can suppose that U is affine and f factors into*

$$U \xrightarrow{g} V \longrightarrow Y$$

where V is an affine open containing y and $g : U \to V$ is a morphism corresponding to a injective homomorphism $\Gamma(V, \mathcal{O}_Y) \to \Gamma(U, \mathcal{O}_X)$.

Proof. In fact, with the notations of Proposition 22.6.49(ii), C is integral and the canonical homomorphism $C \to C_g$ is then injective; the result then follows from the diagram (6.4.1), since σ is injective. □

Proposition 22.6.52. *Let $f : X \to Y$ be a morphism, x be a point of X and $y = f(x)$.*

(a) Suppose that f is locally of finite type at the point x. For f to be a local immersion at the point x, it is necessary and sufficient that $f_x^\# : \mathcal{O}_{Y,y} \to \mathcal{O}_{X,x}$ is surjective.

(b) Suppose that f is locally of finite presentation at the point x. For f to be a local isomorphism at the point x, it is necessary and sufficient that $f_x^\# : \mathcal{O}_{Y,y} \to \mathcal{O}_{X,x}$ is an isomorphism.

Proof. We only need to prove the sufficiency, and we first consider case (b). Then X is locally of finite presentation over y at the point x, so by Proposition 22.6.49(i) and (ii), there exists an open neighborhood V of y and a morphism $g : V \to X$ such that $g \circ f$ (resp. $f \circ g$) is defined and coincide with the identity on an open neighborhood W of x (resp. an open neighborhood T of y). Put $T' = T \cap g^{-1}(w)$ and $W' = f^{-1}(T')$, we then verify that $g(T') \subseteq W'$, $f(W') \subseteq T'$ and $(g \circ f)|_{W'} = 1_{W'}$, whence f is a local isomorphism.

For (a), we can assume that X and Y are affine, with ring A and B. Then f corresponds to a homomorphism $\varphi : B \to A$ of finite type; we have $\varphi^{-1}(\mathfrak{p}_x) = \mathfrak{p}_y$, and the homomorphism $\varphi_x : B_y \to A_x$ induced by φ is surjective. Let $(t_i)_{1 \le i \le n}$ be a system of generators of the B-algebra A. The hypothesis on φ_x then implies $t_i/1 = \varphi(b_i)/\varphi(c)$ in the ring A_x, where $b_i \in B$ and $c \in B - \mathfrak{p}_y$, so we can find $a \in A - \mathfrak{p}_x$ such that

$$a(t_i\varphi(c) - \varphi(b_i)) = 0.$$

If we put $g = a\varphi(c)$, then $t_i/1 = a\varphi(b_i)/g$ in the ring A_g. Now there exists by hypothesis a polynomial $Q(X_1, \dots, X_n)$ with coefficients in $\varphi(B)$ such that $a = Q(t_1, \dots, t_n)$; write $Q(X_1/T, \dots, X_n/T) = P(X_1, \dots, X_n, T)/T^m$, where P is a polynomial of degree m. In the ring A_g, we then have

$$\begin{aligned} a/1 &= Q(t_1/1, \dots, t_n/1) = Q(a\varphi(b_1)/g, \dots, a\varphi(b_n)/g) \\ &= a^m P(\varphi(b_1), \dots, \varphi(b_n), \varphi(c))/g^m = a^m \varphi(d)/g^m \end{aligned}$$

where $d \in B$. Since $g/1 = (a/1)(\varphi(c)/1)$ is invertible in A_g by definition, so is $a/1$ and $\varphi(c)/1$, and we can then write $a/1 = (\varphi(d)/1)(\varphi(c)/1)^{-m}$. We conclude that $\varphi(d)/1$ is also invertible in A_g. Put $h = cd$, as $\varphi(h)/1$ is invertible in A_g, the composed homomorphism $B \to A \to A_g$

factors into

$$\begin{tikzcd} B \arrow[r, "\varphi"] \arrow[dr] & A \arrow[r] & A_g \\ & B_h \arrow[ur, "\gamma"'] & \end{tikzcd}$$

We claim that γ is surjective. For this, it suffices to verify that the image of B_h in A_g contains $t_i/1$ and $1/g$. Now we have

$$1/g = (\varphi(c)/1)^{m-1}(\varphi(d)/1)^{-1} = \gamma(c^m/h)$$

and $a/1 = \gamma(d^{m+1}/h^m)$, so $(a\varphi(b_i))/1 = \gamma(b_i d^{m+1}/h^m)$, and as $t_i/1 = (a\varphi(b_i)/1)(g/1)^{-1}$, we conclude our assertion. The choice of h implies $f(D(g)) \subseteq D(h)$, and the restriction of f to $D(g)$ is induced by γ. Since γ is surjective, this restriction is a closed immersion from $D(g)$ to $D(h)$, so f is a local immersion at x. □

Corollary 22.6.53. *With the notations of Proposition 22.6.52, suppose that f is a local immersion at the point x and is locally of finite presentation at x. For f to be open at x, it is necessary and sufficient that the kernel of $f_x^\#$ is nilpotent.*

Proof. In view of Proposition 22.6.30, it suffices to prove the sufficiency of the condition. We can suppose that $Y = \operatorname{Spec}(A)$ and $X = \operatorname{Spec}(A/\mathfrak{n})$, where $\mathfrak{n}$ is a finitely generated ideal of A (Corollary 22.6.27), and by hypothesis $\mathfrak{n}_x$ is nilpotent. If $(s_i)_{1\leq i\leq n}$ is a system of generators of $\mathfrak{n}$, we then have $s_i^m/1 = 0$ in A_x for an integer m and all i. Then there exists $t \in A - \mathfrak{p}_x$ such that $ts_i^m = 0$ for all i, so $(s_i/1)^m = 0$ in the ring A_t. This shows $\mathfrak{n}_t$ is nilpotent, whence the conclusion. □

22.6.5 Direct image of quasi-coherent sheaves

Proposition 22.6.54. *Let X, Y be two schemes and $f : X \to Y$ be a quasi-compact and quasi-separated morphism. Then for any quasi-coherent $\mathscr{O}_X$-module, $f_*(\mathscr{F})$ is quasi-coherent.*

Proof. Since the question is local over Y, we can assume that Y is affine. If f is quasi-compact, X is then a union of finitely many open affines X_i, and in view of Proposition 22.6.7(ii), X is a quasi-separated scheme, hence the intersections $X_i \cap X_j$ are qausi-compact (Proposition 22.6.10).

We first assume that each intersection $X_i \cap X_j$ is affine. Put $\mathscr{F}_i = \mathscr{F}|_{X_i}$, $\mathscr{F}_{ij} = \mathscr{F}|_{X_i\cap X_j}$ and let $\mathscr{F}_i'$ and $\mathscr{F}_{ij}'$ be the inverse image of $\mathscr{F}_i$ and $\mathscr{F}_j$ under the restriction of f to X_i and to $X_{i\cap X_j}$. We see that $\mathscr{F}_i'$ and $\mathscr{F}_{ij}'$ are quasi-coherent (Proposition 19.4.1). We define a homomorphism

$$u : \bigoplus_i \mathscr{F}_i' \to \bigoplus_{i,j} \mathscr{F}_{ij}'$$

such that $f_*(\mathscr{F})$ is the kernel of u, and this then implies $f_*(\mathscr{F})$ is quasi-coherent by Corollary 22.1.6. For this, it suffices to define u as a homomorphism of presheaves, so for each open subset $W \subseteq Y$, we need a homomorphism

$$u_W : \bigoplus_i \Gamma(f^{-1}(W) \cap X_i, \mathscr{F}) \to \bigoplus_{ij} \Gamma(f^{-1}(W) \cap X_i \cap X_j, \mathscr{F})$$

so as to satisfy the compatibility for the restrictions to a smaller open subset. If for any section s_i of $\mathscr{F}$ over $f^{-1}(W) \cap X_i$, we denote by s_{ij} its restriction to $f^{-1}(W) \cap X_i \cap X_j$, we set

$$u_W((s_i)) = (s_{ij} - s_{ji})$$

and the compatibility is evident. To identity the kernel $\mathscr{R}$ of u, we define a homomorphism $v : f_*(\mathscr{F}) \to \mathscr{R}$ which sends a section s of $\mathscr{F}$ over $f^{-1}(W)$ to the family (s_i), where s_i is the restriction of s to $f^{-1}(W) \cap X_i$. By the sheaf axoims of $\mathscr{F}$, it is clear that v is bijective, which proves the assertion in this case.

In the general case, the same reasoning can be applied if we can show that each $\mathscr{F}'_{ij}$ is quasi-coherent. But by hypotheses, $X_i \cap X_j$ is a union of finitely many affine opens X_{ijk}, and since each X_{ijk} are affine open subschemes of the affine scheme X_i, their intersections are again affine (affine schemes are separated), so we can apply the previous arguments to conclude that $\mathscr{F}'_{ij}$ is quasi-coherent, and the proof is then complete. □

Remark 22.6.2. We should note that even if X and Y are Noetherian schemes and $f : X \to Y$ is a morphism of finite type, the direct image $f_*(\mathscr{F})$ of a coherent $\mathscr{O}_X$-module $\mathscr{F}$ is in general not coherent. For example, let Y be the spectrum of a field K, $X = \mathrm{Spec}(K[T])$, and choose $\mathscr{F} = \mathscr{O}_X$.

Proposition 22.6.55. *Let $f : X \to Y$ be a quasi-compact and quasi-separated morphism. Let $(\mathscr{F}_\lambda)$ be a inductive system of quasi-coherent $\mathscr{O}_X$-modules and $\mathscr{F} = \varinjlim \mathscr{F}_\lambda$ be the inductive limit. Then $\varinjlim f_*(\mathscr{F}_\lambda) \cong f_*(\mathscr{F})$.*

Proof. For each affine open subset W of Y and any λ, we have a canonical homomorphism

$$u_{W,\lambda} : (f_*(\mathscr{F}_\lambda))|_W \to f_*(\mathscr{F})|_W$$

whence a canonical homomorphism

$$u_W : (\varinjlim f_*(\mathscr{F}_\lambda))|_W \to f_*(\mathscr{F})|_W$$

and this hommorphism is compatible with restrictions. Since f is quasi-compact and quasi-separated, by Proposition 22.6.54 $\varinjlim f_*(\mathscr{F}_\lambda)$ and $f_*(\mathscr{F})$ are quasi-coherent. Moreover, the homomorphism u_W corresponds by taking global section over W to the canonical homomorphism

$$\varphi_W : \Gamma(W, \varinjlim f_*(\mathscr{F}_\lambda)) \to \Gamma(f^{-1}(W), \mathscr{F}).$$

Since f is quasi-compact and quasi-separated, by **??** (Stack Project. Lemma 6.29.1) we have

$$\Gamma(W, \varinjlim f_*(\mathscr{F}_\lambda)) = \varinjlim \Gamma(W, f_*(\mathscr{F}_\lambda)) = \varinjlim \Gamma(f^{-1}(W), \mathscr{F}_\lambda) = \Gamma(f^{-1}(W), \mathscr{F})$$

and φ_W is therefore the identity homomorphism. By Corollary 22.1.21, it then follows that u_W is an isomorphism for each W, and the assertion then follows. □

22.6.6 Extension of quasi-coherent sheaves

Let X be a topological space and $\mathscr{F}$ be a sheaf of sets (resp. of groups, of rings) over X. Let U be an open subset of X with $j : U \to X$ the canonical injection, and let $\mathscr{G}$ be a subsheaf of $\mathscr{F}|_U = j^{-1}(\mathscr{F})$. As the functor j_* is left exact, $j_*(\mathscr{G})$ is then a subsheaf of $j_*(j^{-1}(\mathscr{F}))$. Let

$\rho_{\mathscr{F}} : \mathscr{F} \to j_*(j^{-1}(\mathscr{F}))$ be the canonical homomorphism associated with $\mathscr{F}$ and consider the subsheaf $\overline{\mathscr{G}} = \rho_{\mathscr{F}}^{-1}(j_*(\mathscr{G}))$ of $\mathscr{F}$. It follows immediately from definition that, for any open subset V of X, $\Gamma(V, \overline{\mathscr{G}})$ is formed by sections $s \in \Gamma(V, \mathscr{F})$ whose restriction on $V \cap U$ is a section of $\mathscr{G}$ over $V \cap U$. In particular, we have $\overline{\mathscr{G}}|_U = j^{-1}(\overline{\mathscr{G}}) = \mathscr{G}$, and $\overline{\mathscr{G}}$ is the largest subsheaf of $\mathscr{F}$ inducing $\mathscr{G}$ on U. We say the subsheaf $\overline{\mathscr{G}}$ is the **canonical extension** of the subsheaf $\mathscr{G}$ of $\mathscr{F}|_U$ to a subsheaf of $\mathscr{F}$.

Proposition 22.6.56. *Let X be a scheme and U be an open subset of X such that the canonical injection $j : U \to X$ is quasi-compact (in other words, U is retrocompact in X).*

(a) For any quasi-coherent $(\mathscr{O}_X|_U)$-module $\mathscr{G}$, $j_*(\mathscr{G})$ is a quasi-coherent $\mathscr{O}_X$-module and we have $j_*(\mathscr{G})|_U = j^*(j_*(\mathscr{G})) = \mathscr{G}$.

(b) For any quasi-coherent $\mathscr{O}_X$-module $\mathscr{F}$ and any quasi-coherent sub-$(\mathscr{O}_X|_U)$-module $\mathscr{G}$ of $\mathscr{F}|_U$, the canonical extension $\overline{\mathscr{G}}$ of $\mathscr{G}$ is a quasi-coherent sub-$\mathscr{O}_X$-module of $\mathscr{F}$.

Proof. Assertion (a) is a special case of Proposition 22.6.54 since j is quasi-separated by Proposition 22.6.7(i), and the relation $j_*(\mathscr{G})|_U = j^*(j_*(\mathscr{G})) = \mathscr{G}$ can be checked directly. By the same reasoning, $j_*(j^*(\mathscr{F}))$ is quasi-coherent, and as $\overline{G}$ is the inverse image of $j_*(\mathscr{G})$ under the homomorphism $\rho_{\mathscr{F}} : \mathscr{F} \to j_*(j^*(\mathscr{F}))$, assertion (b) follows from Corollary 22.2.20. □

Corollary 22.6.57. *Let X be a scheme and U be a quasi-compact open subset of X such that the canonical injection $j : U \to X$ is quasi-compact. Suppose that any quasi-coherent $\mathscr{O}_X$-module is the inductive limit of its quasi-coherent sub-$\mathscr{O}_X$-modules of finite type (this is ture if X is an affine scheme). Let $\mathscr{F}$ be a quasi-coherent $\mathscr{O}_X$-module and $\mathscr{G}$ be a quasi-coherent sub-$(\mathscr{O}_X|_U)$-module of finite type of $\mathscr{F}|_U$. Then there exists a quasi-coherent sub-$\mathscr{O}_X$-module $\mathscr{G}'$ of finite type such that $\mathscr{G}'|_U = \mathscr{G}$.*

Proof. We have $\mathscr{G} = \overline{\mathscr{G}}|_U$, and $\overline{\mathscr{G}}$ is quasi-coherent by Proposition 22.6.56, hence is the inductive limit of its quasi-coherent sub-$\mathscr{O}_X$-modules $\mathscr{H}_\lambda$ of finite type. Then $\mathscr{G}$ is the inductive limit of the $\mathscr{H}_\lambda|_U$, hence equals to one of $\mathscr{H}_\lambda|_U$ since they are of finite type (Proposition 19.4.10). □

Remark 22.6.3. Suppose that for any affine open $U \subseteq X$ the injection $U \to X$ is quasi-compact. Then if the conclusion of Corollary 22.6.57 holds for any affine open U and any quasi-coherent sub-$(\mathscr{O}_X|_U)$-module of finite type $\mathscr{G}$ of $\mathscr{F}|_U$, it follows that $\mathscr{F}$ is the inductive limit of its quasi-coherent sub-$\mathscr{O}_X$-modules of finite type. In fact, for any affine open $U \subseteq X$, we have $\mathscr{F}|_U = \widetilde{M}$, where M is a $\Gamma(U, \mathscr{O}_X)$-module, and as the latter is the inductive limit of its finitely generated sub-modules, $\mathscr{F}|_U$ is the inductive limit of its quasi-coherent sub-$(\mathscr{O}_X|_U)$-modules of finite type. Now, by hypotheses, such a submodule is induced over U by a quasi-coherent sub-$\mathscr{O}_X$-module of finite type $\mathscr{G}_{\lambda,U}$ of $\mathscr{F}$. The finite sums of $\mathscr{G}_{\lambda,U}$ are then quasi-coherent of finite type, since the question is local and we can assume that X is affine, where the conclusion is trivial. It then follows that $\mathscr{F}$ is the inductive limit of these finite sums, whence our assertion.

Corollary 22.6.58. *Under the hypotheses of Corollary 22.6.57, if $\mathscr{G}$ is a quasi-coherent $(\mathscr{O}_X|_U)$-module of finite type, there exists a quasi-coherent $\mathscr{O}_X$-module $\mathscr{G}'$ such that $\mathscr{G}'|_U = \mathscr{G}$.*

Proof. As $\mathscr{F} = j_*(\mathscr{G})$ is quasi-coherent (Proposition 22.6.56) and $\mathscr{F}|_U = \mathscr{G}$, it suffices to apply Corollary 22.6.57 to $\mathscr{F}$. □

Lemma 22.6.59. *Let X be a scheme, $(V_\lambda)_{\lambda \in L}$ be a covering of X by affine opens where L is well-ordered, and U be an open subset of X. For each $\lambda \in L$, let $W_\lambda = \bigcup_{\mu<\lambda} V_\mu$. Suppose that*

(i) for any $\lambda \in L$, $V_\lambda \cap W_\lambda$ is quasi-compact;

(ii) the canonical injection $j : U \to X$ is quasi-compact.

Then for any quasi-coherent $\mathcal{O}_X$-module $\mathcal{F}$ and any quasi-coherent sub-$(\mathcal{O}_X|_U)$-module of finite type $\mathcal{G}$ of $\mathcal{F}|_U$, there exists a quasi-coherent sub-$\mathcal{O}_X$-module $\mathcal{G}'$ of $\mathcal{F}$ such that $\mathcal{G}'|_U = \mathcal{G}$.

Theorem 22.6.60. *Let X be a scheme and U be an open subset of X. Suppose that one of the following conditions is satisfied:*

(a) X is locally Noetherian;

(b) X is quasi-compact and quasi-separated and U is quasi-compact.

Then for any quasi-coherent $\mathcal{O}_X$-module $\mathcal{F}$ and any quasi-coherent sub-$(\mathcal{O}_X|_U)$-module of finite type $\mathcal{G}$ of $\mathcal{F}|_U$, there exists a quasi-coherent sub-$\mathcal{O}_X$-module $\mathcal{G}'$ of $\mathcal{F}$ such that $\mathcal{G}'|_U = \mathcal{G}$.

Corollary 22.6.61. *With the conditions of Theorem 22.6.60, for any quasi-coherent $(\mathcal{O}_X|_U)$-module $\mathcal{G}$ of finite type, there exists a quasi-coherent $\mathcal{O}_X$-module $\mathcal{G}'$ of finite type such that $\mathcal{G}'|_U = \mathcal{G}$.*

Corollary 22.6.62. *Let X be a locally Noetherian scheme or a quasi-compact and quasi-separated scheme. Then any quasi-coherent $\mathcal{O}_X$-module is the inductive limit of its quasi-coherent sub-$\mathcal{O}_X$-modules of finite type.*

Proof. This follows from Theorem 22.6.60 and Remark 22.6.3. □

Corollary 22.6.63. *Under the hypotheses of Corollary 22.6.62, if a quasi-coherent $\mathcal{O}_X$-module $\mathcal{F}$ is such that any quasi-coherent sub-$\mathcal{O}_X$-module of finite type of $\mathcal{F}$ is generated by its global sections, then $\mathcal{F}$ is generated by its global sections.*

Proof. Let U be an affine neighborhood of a point $x \in X$, and let s be a section of $\mathcal{F}$ over U. The sub-$\mathcal{O}_X$-module $\mathcal{G}$ of $\mathcal{F}|_U$ generated by s is quasi-coherent and of finite type, hence there exists a quasi-coherent sub-$\mathcal{O}_X$-module of finite type $\mathcal{G}'$ of $\mathcal{F}$ such that $\mathcal{G}'|_U = \mathcal{G}$ (Theorem 22.6.60). By hypotheses, there is then a finite number of sections t_i of $\mathcal{G}'$ over X and sections a_i of $\mathcal{O}_X$ over a neighborhood $V \subseteq U$ of x such that $s|_V = \sum_i a_i \cdot (t_i|_V)$, which proves the corollary. □

22.6.7 Scheme-theoretic image

Let $f : X \to Y$ be a morphism of schemes. If there exists a smallest closed subscheme Y' of Y such that the canonical injection $j : Y' \to Y$ dominates f (or equivalently, the inverse image $f^{-1}(Y')$ is equal to X), we then say that Y' is the **scheme-theoretic image** of X under f, or the **scheme-theoretic image of f**. If X is a subscheme of Y, the scheme-theoretic image of the canonical injection $j : X \to Y$ is called the **scheme-theoretic closure** of X.

Proposition 22.6.64 (Transitivity). *Let $f : X \to Y$ and $g : Y \to Z$ be morphisms. Suppose that Y' is the scheme-theoretic image of X under f, and if g' is the restriction of g to Y', the scheme-theoretic image of Z' under g' exists. Then the scheme-theoretic image of X under $g \circ f$ is equal to Z'.*

Proof. To say that a closed subscheme Z_1 of Z is such that $(g \circ f)^{-1}(Z_1) = X$ signifies that $f^{-1}(g^{-1}(Z_1)) = X$, or that f is dominated by the canonical injection $g^{-1}(Z_1) \to Y$. Now, in view of the existence of the scheme-theoretic image Y', for any closed subscheme Z_1 of Z having

this property, $g^{-1}(Z_1)$ dominates Y', which, if $j : Y' \to Y$ is the canonical injection, amounts to saying that $j^{-1}(g^{-1}(Z_1)) = g'^{-1}(Z_1) = Y'$. We then conclude that Z' is the smallest closed subscheme Z_1 having this property, whence our claim. □

Corollary 22.6.65. *Let $f : X \to Y$ be an S-morphism such that Y is the scheme-theoretic image of Y under f. Let Z be a separated S-scheme; if two S-morphisms $g_1, g_2 : Y \to Z$ are such that $g_1 \circ f = g_2 \circ f$, then $g_1 = g_2$.*

Proof. Let $h = (g_1, g_2)_S : Y \to Z \times_S Z$. As the diagonal $T = \Delta_Z(Z)$ is a closed subscheme of $Z \times_S Z$, $Y' = h^{-1}(T)$ is a closed subscheme of Y. Put $u = g_1 \circ f = g_2 \circ f$; we then have $h \circ f = (u, u)_S = \Delta_Z \circ u$. As $\Delta_Z^{-1}(T) = Z$, we have $(h \circ f)^{-1}(T) = u^{-1}(Z) = X$, so $f^{-1}(Y') = X$. We then conclude that the canonical injection $Y' \to Y$ dominates f, so $Y' = Y$ by hypothesis. Then by Proposition 22.4.14, h factors into $\Delta_Z \circ v$ where v is a morphism $Y \to Z$, which implies $g_1 = g_2 = v$. □

Let $f : X \to Y$ be a morphism and suppose that the scheme-theoretic image Y' of f exists. Then Y' is defined by a quasi-coherent ideal $\mathscr{I}'$ of $\mathscr{O}_Y$, and by definition, $\mathscr{J}'$ is the largest quasi-coherent ideal such that the homomorphism $f^\# : \mathscr{O}_Y \to f_*(\mathscr{O}_X)$ factors into $\mathscr{O}_Y \to \mathscr{O}_Y/\mathscr{J}' \to f_*(\mathscr{O}_X)$. This implies that $\mathscr{J}' \subseteq \ker f^\# = \mathscr{J}$; we therefore obtain a case where Y' exists, the one where $\mathscr{J}$ is quasi-coherent, and where $\mathscr{J}' = \mathscr{J}$.

Proposition 22.6.66. *Let $f : X \to Y$ be a morphism. Then the scheme-theoretic image of X under f exists if one of the following conditions is satisfied:*

(a) $f_*(\mathscr{O}_X)$ is quasi-coherent (which is the case if f is quasi-compact and quasi-separated).

(b) X is reduced.

In this case, the underlying space of Y' is equal to $\overline{f(X)}$, and if f factors into

$$X \xrightarrow{f'} Y' \xrightarrow{Y} Y$$

where j is the canonical injection, f' is scheme-theoretic dominant. Moreover, if X is reduced (resp. integral), so is Y'.

Proof. The case (a) is immediate by our previous argument; moreover, as $\mathscr{O}_Y/\mathscr{J} \to f_*(\mathscr{O}_X)$ is then injective, this shows that f' is scheme-theoretic dominant. We still need to verify that the closed subscheme of Y defined by $\mathscr{J} = \ker f^\#$ has underlying space $\overline{f(X)}$. Since the support of $f_*(\mathscr{O}_X)$ is contained in $\overline{f(X)}$, we have $\mathscr{J}_y = \mathscr{O}_y$ for $y \notin \overline{f(X)}$, so the support pf $\mathscr{O}_Y/\mathscr{J}$ is contained in $\overline{f(X)}$. Moreover, this support is closed and contains $f(X)$: if $y \in f(X)$, the identity element of the ring $(f_*(\mathscr{O}_X))_y$ is nonzero, being the germ at y of the section $1 \in \Gamma(X, \mathscr{O}_X) = \Gamma(Y, f_*(\mathscr{O}_X))$; as this is the image of the identity element under $f^\#$, it is not contained in $\mathscr{J}_y$, so $\mathscr{O}_y/\mathscr{J}_y \neq 0$; this proves our first claim. The case (b) follows from Proposition 22.4.44, because there is a smallest closed subscheme Z with underlying space $\overline{f(X)}$ such that $f(X) \subseteq Z$. □

Proposition 22.6.67. *Suppose the notations of Proposition 22.6.66 is satisfied, and let Y' be the scheme-theoretic image of X under f. For any open subset V of Y, let $f_V : f^{-1}(V) \to V$ be the restriction of f. Then the scheme-theoretic image of $f^{-1}(V)$ under f_V exists and is equal to the oepn subscheme $V \cap Y'$ of Y'.*

Proof. Put $X' = f^{-1}(V)$; as the direct image of $\mathscr{O}_{X'}$ is the restriction of $f_*(\mathscr{O}_X)$ to V, it is clear that the kernel of the homomorphism $\mathscr{O}_V \to (f_V)_*(\mathscr{O}_{X'})$ is the restriction of $\mathscr{J}$ to V, whence the assertion. □

Proposition 22.6.68. *Let Y be a subscheme of a scheme X, such that the canonical injection $j : Y \to X$ is quasi-compact. Then the scheme-theoretic closure of Y exists and has $\overline{Y}$ as underlying space.*

Proof. It suffices to apply Proposition 22.6.66 to the injection j, which is separated (Proposition 22.5.25) and quasi-compact by hypothesis. □

With these notations, let $\overline{Y}$ be the scheme-theoretic closure of Y in X. If the injection $\overline{Y} \to X$ is quasi-compact, and if $\mathscr{I}$ is the quasi-coherent ideal of $\mathscr{O}_X|_{\overline{Y}}$ defining the closed subscheme Y of $\overline{Y}$, then the quasi-coherent ideal of $\mathscr{O}_X$ defining $\overline{Y}$ is the canonical extension (Proposition 22.6.56) $\overline{\mathscr{I}}$ of $\mathscr{I}$, because it is evidently the largest quasi-coherent ideal of $\mathscr{O}_X$ inducing $\mathscr{I}$ over Y.

Corollary 22.6.69. *Under the hypothesis of Proposition 22.6.68, any section of $\mathscr{O}_{\overline{Y}}$ over an open subset V of $\overline{Y}$ that is zero on $V \cap Y$ is zero.*

Proof. In view of Proposition 22.6.67, we can assume that $V = \overline{Y}$. If we consider sections of $\mathscr{O}_{\overline{Y}}$ over $\overline{Y}$ as $\overline{Y}$-sections of $\overline{Y} \otimes_{\mathbb{Z}} \mathbb{Z}[T]$, which is separated over $\overline{Y}$, the assertion is then a particular case of Corollary 22.6.65. □

22.7 Rational maps over schemes

22.7.1 Rational maps and rational functions

Let X and Y be two schemes, U and V be open dense sets of X, and f (resp. g) be a morphism from U (resp. V) to Y. We say the morphisms f and g are equivalent if they coincide over an open subset dense in $U \cap V$. As the intersection of finitely many open dense subsets of X is an open dense subset of X, it is clear that this relation is an equivalence relation.

Given two schemes X and Y, a **rational map** from X to Y is defined to be an equivalent class of morphisms from an open dense subset of X to Y. If X and Y are S-schemes, this class is called an **rational S-map** is there exists an S-morphism in it. An rational S-map from S to X is called an **rational S-section** of X. The rational X-sections of the X-scheme $X \otimes_{\mathbb{Z}} \mathbb{Z}[T]$ (where T is an indeterminate) are called the **rational functions over** X (cf. Example 22.3.11). A rational map f from X to Y is usually denoted by $f : X \dashrightarrow Y$.

Let $f : X \dashrightarrow Y$ be a rational map and U be an open subset of X. If f_1, f_2 are morphisms belonging to the class f, defined respectively over the open dense sets V_1, V_2 of X, the restrictions $f_1|_{U\cap V_1}$ and $f_2|_{U\cap V_2}$ coincide on $U \cap V_1 \cap V_2$, which is dense in U; the class of morphisms f therefore defines a rational map $U \dashrightarrow Y$, called the **restriction** of f to U and denoted by $f|_U$.

It is clear that we have a canonical map from $\mathrm{Hom}_S(X, Y)$ to the set of rational S-maps from X to Y, which associates any S-morphism $f : X \to Y$ to the rational S-map it belongs to. If we denote by $\Gamma_{\mathrm{rat}}(X/Y)$ the set of rational Y-sections of X, we then have a canonical map $\Gamma(X/Y) \to \Gamma_{\mathrm{rat}}(X/Y)$. It is also clear that if X and Y are two S-schemes, the set of rational S-maps from X to Y is canonically identified with $\Gamma_{\mathrm{rat}}((X \times_S Y)/X)$.

In view of Example 22.3.11, we see the rational functions over X are canonically identified with the equivalent classes of sections of the structural sheaf $\mathscr{O}_X$ over open dense sets of X,

where two sections are equivalent if they coincide over an open dense subset of the intersection of their defining domain. In partiuclar, we see the rational functions over X form a ring $K(X)$.

If X is an irreducible scheme, any nonempty open subset of X is dense; we can also say that the non-empty open sets of X are the open neighborhoods of the generic point x of X. To say that two morphisms from nonempty open subsets of X to Y are equivalent therefore means in this case that they have the same germ at the point x. In other words, rational maps (resp. rational S-maps) $X \dashrightarrow Y$ are identified with the germs of morphisms (resp. of S-morphisms) of non-empty open subsets of X to Y at the generic point x of X. In particular:

Proposition 22.7.1. *If X is an irreducible scheme, the ring $K(X)$ of rational functions over X is canonically identified with the local ring $\mathcal{O}_{X,x}$ at the generic point x of X. This is a local ring of zero dimension, and therefore an Artinian local ring if X is Noetherian. It is a field if X is integral, and is identified with the fraction field of $\Gamma(X, \mathcal{O}_X)$ if X is moreover affine.*

Proof. Since we can identify rational functions with sections over X, the first assertion follows from the definiton of stalks. For the second one, we can assume that X is affine with ring A; then $\mathfrak{p}_x$ is the nilradical of A, and in particular $\mathcal{O}_{X,x}$ has zero dimension. If A is integral, $\mathfrak{p}_x = (0)$ and $\mathcal{O}_{X,x}$ is the fraction field of A. Finally, if A is Noetherian, then $\mathfrak{p}_x$ is nilpotent and $\mathcal{O}_{X,x} = A_x$ is Artinian. □

If X is integral, the ring $\mathcal{O}_{X,z}$ is integral for any $z \in X$. Any affine open U containing x must contain x as its generic point, and $\mathcal{O}_{X,z}$, equal to a fraction field of $\Gamma(U, \mathcal{O}_X)$, is identified with $K(X)$. We then conclude that $K(X)$ is identified with the fraction field of $\mathcal{O}_{X,z}$, and in this way, $\mathcal{O}_{X,z}$ is canonically identified with a subring of $K(X)$, so that a germ $s \in \mathcal{O}_{X,z}$ is canonically identified with a rational function over X.

Proposition 22.7.2. *Let X and Y be two S-schemes such that the family (X_λ) of irreducible components of X is locally finite. For each λ, let x_λ be the generic point of X_λ. If R_λ is the set of germs at x_λ of S-morphisms from open subsets of X to Y, the set of rational S-maps from X to Y is identified with the product of R_λ. In particular, the ring of rational functions over X is identified with the product of the local rings $\mathcal{O}_{X,x_\lambda}$.*

Proof. The set of the intersections $X_\lambda \cap X_\mu$ for $\lambda \neq \mu$ is then locally finite, so their union is closed and contains the maximal points of X. If we set $X'_\lambda = X_\lambda - \bigcup_{\mu \neq \lambda} X_\lambda \cap X_\mu$, then X'_λ is irreducible, with generic point equal to that of X_λ, and pairwise disjoint with union dense in X. For any open dense subset U of X, $U'_\lambda = U \cap X'_\lambda$ is a nonempty open dense subset of X'_λ, and U'_λ are pairwise disjoint with $U' = \bigcup_\lambda U'_\lambda$ closed in X. To give a morphism from U' to Y is then equivalent to giving (arbitrarily) a morphism from each of the U'_λ in Y, so the assertion follows. □

Corollary 22.7.3. *Let A be a Noetherian ring and $X = \mathrm{Spec}(A)$. The ring of rational function functions over X is identified with the total fraction ring $Q(A)$.*

Proof. Let S be the complement of the union of minimal prime ideals of A. Then by Proposition 10.4.16, the ring of sections $\Gamma(D(f), \mathcal{O}_X)$ is identified with A_f, so $D(f)$ with $f \in S$ form a cofinal subset of the open dense sets of X, and the ring of rational functions over X is then identified with the inductive limit of A_f, $f \in S$, which is exactly $Q(A)$. □

Suppose that X is irreducible with generic point x. As any nonempty open set U of X contains x, and therefore contains any generalization $z \in X$, any morphism $U \to Y$ can be composed with the canonical morphism $\mathrm{Spec}(\mathcal{O}_{X,x}) \to X$ (Corollary 22.2.10). Two morphisms from nonempty open subsets of X to Y which coincide on a smaller open subset then give the same morphism $\mathrm{Spec}(\mathcal{O}_{X,x}) \to Y$. In other words, to any rational map X to Y, there corresponds a well-defined morphism $\mathrm{Spec}(\mathcal{O}_{X,x}) \to Y$.

Proposition 22.7.4. *Let X and Y be S-schemes. Suppose that X is irreducible with generic point x, and Y is of finite type over S. Then two rational S-maps X to Y corresponding to the same S-morphism $\mathrm{Spec}(\mathcal{O}_{X,x}) \to Y$ are identical. If moreover S is locally of finite presentation over S, then any S-morphism $\mathrm{Spec}(\mathcal{O}_{X,x}) \to Y$ corresponds to a rational S-map from X to Y.*

Proof. Given that every non-empty open subset of X is dense, this result follows immediately from Proposition 22.6.49. □

Corollary 22.7.5. *Suppose that X is irreducible with generic point x and Y is localy of finite presentation. Then the rational S-maps from X to Y are identified with the points of Y with values in the S-scheme $\mathrm{Spec}(\mathcal{O}_{X,x})$.*

Proof. This is just a reformulation of Proposition 22.7.4. □

Corollary 22.7.6. *Suppose that X is irreducible with generic point x and Y is localy of finite presentation. Let s be the image of x in S. Then giving a rational S-map from X to Y is equivalent to giving a point y of Y lying over s and a $\mathcal{O}_{S,s}$-homomorphism $\mathcal{O}_{Y,y} \to \mathcal{O}_{X,x} = K(X)$.*

Proof. This follows from Proposition 22.7.4 and Proposition 22.2.12. □

Corollary 22.7.7. *Suppose that X is irreducible with generic point x and Y is localy of finite presentation, then the rational S-maps from X to Y (with Y given) only depends on the S-scheme $\mathrm{Spec}(\mathcal{O}_{X,x})$ and in particular remain the same if we replace X by $\mathrm{Spec}(\mathcal{O}_{X,z})$, $z \in X$.*

Proof. In fact, if $z \in \overline{\{x\}}$ then x is the generic point of $Z = \mathrm{Spec}(\mathcal{O}_{X,z})$ and $\mathcal{O}_{X,x} = \mathcal{O}_{Z,x}$. □

Corollary 22.7.8. *Suppose that X is integral with generic point x and Y is localy of finite presentation. Let s be the image of x in S. Then following dates are equivalent:*

(i) a rational S-map from X to Y;

(ii) a point of $Y \otimes_S \kappa(s)$ with values in the extension $K(X)$ of $\kappa(s)$;

(iii) a point $y \in Y$ over s and an $\kappa(s)$-homomorphism $\kappa(y) \to \kappa(x) = K(X)$.

Proof. The points of Y over s belong to $Y \otimes_S \kappa(s)$ and the $\mathcal{O}_{S,s}$-homomorphisms $\mathcal{O}_{Y,y} \to K(X)$ are $\kappa(s)$-homomorphisms $\kappa(y) \to K(X)$, since $K(X)$ is a field. □

Corollary 22.7.9. *Let k be a field and X, Y be two schemes locally algebraic over k. Suppose that X is integral, then the rational k-maps from X to Y are identified with the points of Y with values in the extension $K(X)$ of k.*

22.7.2 Defining domain of a rational map

Let X and Y be schemes, f a rational map from X to Y. We say f is **defined at a point** $x \in X$ if there exists an open dense subset U containing x and a morphism $U \to Y$ representing f. The set of points $x \in X$ where f is defined is called the **defining domain** of the rational map f. It is clearly an open dense subset of X.

Proposition 22.7.10. *Let X and Y be two S-schemes such that X is reduced and Y is separated over S. Let f be a rational S-map from X to Y, and U_0 be its domain. There then exists a unique S-morphism $U_0 \to Y$ belonging to the class f.*

Proof. For any morphism $U \to Y$ belonging to the class f, we necessarily have $U \subseteq U_0$, so we only need to prove that if U_1, U_2 are two dense subsets of X and $f_i : U_i \to Y$ $(i = 1, 2)$ are two S-morphisms that coincide on an open subset $V \subseteq U_1 \cap U_2$, then f_1 and f_2 coincide on $U_1 \cap U_2$. For this, we can clearly assume that $X = U_1 = U_2$. As X (hence V) is reduced, X is smallest closed subscheme of X dominating V (Proposition 22.4.44). Let $g = (f_1, f_2)_S : X \to Y \times_S Y$; as by hypothesis the diagonal $T = \Delta_Y(Y)$ is a closed subscheme of $Y \times_S Y$, $Z = g^{-1}(T)$ is a closed subscheme of X. If $h : V \to Y$ is the restriction of f_1 and f_2 to V, the restriction of g to V is $\tilde{g} = (h, h)_S$, which factors into $\tilde{g} = \Delta_Y \circ h$. As $\Delta_Y^{-1}(T) = Y$, we have $\tilde{g}^{-1}(T) = V$, and Z is therefore a closed subscheme of X inducing the subscheme structure on V, hence dominates V, and this implies $Z = X$. From the relation $g^{-1}(T) = X$, we deduce that g factors into $\Delta_Y \circ f$, where f is a morphism $X \to Y$ (Proposition 22.4.14), and we have $f_1 = f_2 = f$ from the definition of the diagonal morphism. □

It is clear that the morphism $U_0 \to Y$ defined in Proposition 22.7.10 is the unique morphism in the class f that admits no further extension to open dense subsets of X containing U_0. Under the conditions of Proposition 22.7.10, we can then identify the rational maps from X to Y with the morphisms unextendable to open dense subsets of X to Y.

Corollary 22.7.11. *Let X and Y be two S-schemes such that X is reduced and Y is separated over S. Let U be an open dense subset of X, then there is a canonical bijective correspondence between the S-morphisms from U to Y and the rational S-maps from X to Y defined at each point of U.*

Proof. In view of Proposition 22.7.10, for any S-morphism $f : U \to Y$, there exists a rational S-map $\bar{f}$ from X to Y which extends f. □

Corollary 22.7.12. *Let S be a separated scheme, X be a reduced S-scheme, Y be an S-scheme, and $f : U \to Y$ be an S-morphism from an open dense subset U of X to Y. If $\bar{f}$ is the rational $\mathbb{Z}$-map from X to Y extending f, $\bar{f}$ is an S-morphism (and therefore the rational S-map from X to Y extending f).*

Proof. In fact, if $\varphi : X \to S$ and $\psi : Y \to S$ are the structural morphisms, U_0 is the defining domain of $\bar{f}$, and $j : U_0 \to X$ is the injection, it suffices to prove that $\psi \circ \bar{f} = \varphi \circ j$, which follows from the proof of Proposition 22.7.10, since f is an S-morphism. □

Corollary 22.7.13. *Let X and Y be S-schemes. Suppose that X is reduced and X, Y are spearated over S. Let $p : Y \to X$ be an S-morphism, U be an open dense subset of X, and f be a U-section of Y. Then the rational map $\bar{f}$ from X to Y extending f is a rational X-section of Y.*

Proof. We only need to prove that $p \circ \bar{f}$ is the identity on the defining domain of $\bar{f}$; since X is separated over S, this follows from the proof of Proposition 22.7.10. □

Corollary 22.7.14. *Let X be a reduced scheme and U be an open dense subset of X. There exists a canonical bijective correspondence between sections of $\mathcal{O}_X$ over U and rational functions f over X defined on each point of U.*

Proof. It suffices to remark that the X-scheme $X \otimes_{\mathbb{Z}} \mathbb{Z}[T]$ is separated over X by Proposition 22.5.25. □

Corollary 22.7.15. *Let Y be a reduced scheme, $f : X \to Y$ be a separated morphism, U be an open dense subset of Y, $g : U \to f^{-1}(U)$ be a U-section of $f^{-1}(U)$, and Z the reduced subscheme of X induced on $\overline{g(U)}$. For g to be the restriction of a Y-section of X, it is necessary and sufficient that the restriction of f to Z is an isomorphism from Z to Y.*

Proof. The restriction of f to $f^{-1}(U)$ is a separated morphism (Proposition 22.5.25(i)), so g is a closed immersion by Corollary 22.5.19, and therefore $g(U) = Z \cap f^{-1}(U)$ coincides with the subscheme induced by Z over the open subset $g(U)$ of Z. It is then clear that the given condition is sufficient, since if $f_Z : Z \to Y$ is an isomorphism and $\bar{g} : Y \to Z$ is the inverse morphism, then $\bar{g}$ extends g. Conversely, if g is the restriction to U of a Y-section h of X, h is then a closed immersion by Corollary 22.5.19, so $h(Y)$ is clossed, and as it contains $g(U)$ and we have (as h is continuous) $h(Y) = h(\overline{U}) \subseteq \overline{h(U)} = \overline{g(U)}$, we conclude that $h(Y) = Z$. It then follows from Proposition 22.4.40 that h is necessarily an isomorphism from Y to the closed subscheme Z of X, so $f|_Z$ is also an isomorphism. □

Let X and Y be two S-schemes, where X is reduced and Y is separated over S. Let f be a rational S-map from X to Y, and let x be a point of X. We can compose f with the canonical morphism $\mathrm{Spec}(\mathcal{O}_{X,x}) \to X$ provided that the trace on $\mathrm{Spec}(\mathcal{O}_{X,x})$ of the defining domain of f is dense in $\mathrm{Spec}(\mathcal{O}_{X,x})$ (identified with the set $z \in X$ such as $x \in \overline{\{z\}}$ (cf. Corollary 22.2.10). This happens if the family of irreducible components of X is *locally finite*:

Lemma 22.7.16. *Let X be a scheme such that the family of irreducible components of X is locally finite, and x be a point of X. The irreducible components of $\mathrm{Spec}(\mathcal{O}_{X,x})$ are then the traces over $\mathrm{Spec}(\mathcal{O}_{X,x})$ of the irreducible components of X containing x. For an open subset U of X to be such that $U \cap \mathrm{Spec}(\mathcal{O}_{X,x})$ is dense in $\mathrm{Spec}(\mathcal{O}_{X,x})$, it is necessary and sufficient that it meets the irreducible components of X containing x (and this is ture in particular if U is dense in X).*

Proof. The second assertion clearly follows from the first one. As $\mathrm{Spec}(\mathcal{O}_{X,x})$ is contained in any affine open U containing x and the irreducible components of U containing x are the traces of the irreducible components of X containing x on U (Proposition 4.1.13), we can suppose that X is affine with ring A. Then the prime ideals of A_x correspond to prime ideals of A contained in $\mathfrak{p}_x$, so the minimal prime ideals of A_x correspond to minimal prime ideals of A contained in $\mathfrak{p}_x$, and the lemma follows from Proposition 10.4.16. □

Suppose that we are under the assumption of Lemma 22.7.16. If U is the defining domain of definition of the rational S-map f, denote by f' the rational map from $\mathrm{Spec}(\mathcal{O}_{X,x})$ to Y which coincides with f over $U \cap \mathrm{Spec}(\mathcal{O}_{X,x})$; we will say that this rational map is **induced** by f.

Proposition 22.7.17. *Let S be a scheme, X be a reduced S-scheme, and Y be a separted S-scheme that is locally of finite presentation over S. Suppose that the family of irreducible components of X is locally finite. Let f be a rational S-map from X to Y and x be a point of X. For f to be defined at the point x, it is necessary and sufficient that the rational map f' from $\mathrm{Spec}(\mathcal{O}_{X,x})$ to Y induced by f is a morphism.*

Proof. The conditions is clearly necessary since $\mathrm{Spec}(\mathscr{O}_{X,x})$ is contained in any open subset containing x. We now prove the sufficiency, so suppose that f' is a morphism. In view of Proposition 22.6.49, there exists an open neighborhood U of x in X and an S-morphism $g : U \to Y$ inducing f' on $\mathrm{Spec}(\mathscr{O}_{X,x})$. The point is that U is not necessarily dense in X, so we want to extend g to a morphism defined on an open dense subset of X. Now by Lemma 22.7.16, there are finitely many irreducible components X_i of X containing x, and we can assume that these are the only ones meeting U, by replacing U with a smaller open subset. As the generic points of X_i belong to the defining domain of f and to U, we see that f and g coincide over a non-empty open dense subset of each of the X_i (Proposition 22.6.49). Consider the morphism f_1 defined on an open dense subset of $U \cup (X - \overline{U})$ which equals to g over U and to f over the intersection of $X - \overline{U}$ and the defining domain of f (we also note that each X_i is contained in $\overline{U}$). As $U \cup (X - \overline{U})$ is dense in X, f_1 and f coincide on an open dense subset of X, and f is an extension of f_1. Since f_1 is defined at x, this shows f is defined at x. □

22.7.3 Sheaf of rational functions

Let X be a scheme. For each open subset U of X, we denote by $K(U)$ the ring of rational functions over U, which is an $\Gamma(U, \mathscr{O}_X)$-algebra. Moreover, if $V \subseteq U$ is a second open subset of X, any section of $\mathscr{O}_X$ over a dense subset of U restricts to a section over a dense subset of V, and if two sections coincide over an open dense subset of U, their restriction also coincide over a smaller open dense subset of V. We then define a homomorphism of algebras $\mathrm{Res}_V^U : K(U) \to K(V)$, and it is clear that for $U \supseteq V \supseteq W$ open in X we have $\mathrm{Res}_W^U = \mathrm{Res}_W^V \circ \mathrm{Res}_V^U$. Therefore, we get a presheaf of algebras over X. The associated sheaf of $\mathscr{O}_X$-algebras over X is then called the **sheaf of rational functions** over the scheme X, and denoted by $\mathscr{K}_X$. For any open subset U of X, it is clear that the restriction $\mathscr{K}_X|_U$ is equal to $\mathscr{K}_U$.

Proposition 22.7.18. *Let X be a scheme such that the family (X_λ) of irreducible components of X is locally finite. Then the $\mathscr{O}_X$-module $\mathscr{K}_X$ is quasi-coherent and for any open subset U of X, $K(U)$ is equal to $\Gamma(U, \mathscr{K}_X)$ and is identified with the product of the local rings of the generic points x_λ of the irreducible components X_λ such that $X_\lambda \cap U \neq \varnothing$.*

Proof. The fact that $K(U)$ is identified with the product follows from Proposition 22.7.2. We now show that the presheaf $U \mapsto K(U)$ is a sheaf. Consider an open subset U of X and an open covering (V_α) of U. If $s_\alpha \in K(V_\alpha)$ are such that s_α and s_β coincide over $V_\alpha \cap V_\beta$ for each pair of indices, we then conclude that for any index λ such that $U \cap X_\lambda \neq \varnothing$, the component in $K(X_\lambda)$ of all s_α such that $V_\alpha \cap X_\lambda \neq \varnothing$ are the same. Denoting by t_λ this component, it is clear that the element of $K(U)$ with component t_λ in $K(X_\lambda)$ has restriction s_α on each V_α. Finally, to see the sheaf $\mathscr{K}_X$ is quasi-coherent, we can limit ourselves to the case $X = \mathrm{Spec}(A)$ is affine with finitely many irreducible components; by taking for U the affine open sets of the form $D(f)$, where $f \in A$, it follows from the above argument that we have $\mathscr{K}_X = \widetilde{M}$, where M is the direct sum of the A-modules A_{x_λ}. □

Corollary 22.7.19. *Let X be a reduced scheme with irreducible components $(X_i)_{1 \leq i \leq n}$, endowed with the reduced subscheme structures. If $\iota_i : X_i \to X$ is the canonical injection, $\mathscr{K}_X$ is the direct product of the $\mathscr{O}_X$-algebras $(\iota_i)_*(\mathscr{K}_{X_i})$.*

Proof. This is a particular case of Proposition 22.7.18, in view of the conditions in that proposition. □

Corollary 22.7.20. *If X is irreducible, any quasi-coherent $\mathscr{K}_X$-module $\mathscr{F}$ is a simple sheaf.*

Proof. It suffices to show that any $x \in X$ admits a neighborhood U such that $\mathscr{F}|_U$ is a simple sheaf, which means we can assume that X is affine. We can then suppose that $\mathscr{F}$ is the cokernel of a homomorphism $\mathscr{K}_X^{\oplus I} \to \mathscr{K}_X^{\oplus J}$, and it all boils down to seeing that $\mathscr{K}_X$ is a simple sheaf. But this is evident since $\Gamma(U, \mathscr{K}_X) = K(X)$ for any nonempty open subset U, since U contains the generic point of X. □

Corollary 22.7.21. *If X is irreducible, for any quasi-coherent $\mathscr{O}_X$-module $\mathscr{F}$, $\mathscr{F} \otimes_{\mathscr{O}_X} \mathscr{K}_X$ is a simple sheaf. If moreover X is reduced (hence integral), $\mathscr{F} \otimes_{\mathscr{O}_X} \mathscr{K}_X$ is isomorphic to a sheaf of the form $\mathscr{K}_X^{\oplus I}$.*

Proof. The first claim follows from Corollary 22.7.20, and the second one follows from the fact that if X is integral then $K(X)$ is a field. □

Proposition 22.7.22. *Let X be a scheme such that the family (X_λ) of irreducible components of X is locally finite. Then $\mathscr{K}_X$ is a quasi-coherent $\mathscr{O}_X$-algebra. If X is reduced, the canonical homomorphism $\mathscr{O}_X \to \mathscr{K}_X$ is injective.*

Proof. Since the question is local, the first claim follows from Proposition 22.7.18. The second one follows from Corollary 22.7.14. □

Let X and Y be integral schemes, so that $\mathscr{K}_X$ (resp. $\mathscr{K}_Y$) is a quasi-coherent $\mathscr{O}_X$-module (resp. $\mathscr{O}_Y$-module). Let $f : X \to Y$ be a dominant morphism; then there exists a canonical homomorphism of $\mathscr{O}_X$-modules:

$$\tau : f^*(\mathscr{K}_Y) \to \mathscr{K}_X.$$

Suppose that $X = \operatorname{Spec}(A)$ and $Y = \operatorname{Spec}(B)$ are affine with integral domains A and B, then f corresponds to the injective homomorphism $B \to A$ (Corollary 10.4.19), which extens to a monomorphism $L \to K$ of fraction fields. The homomorphism τ then corresponds to the canonical homomorphism $L \otimes_B A \to K$.

In the general case, for any couple of affine opens $U \subseteq X$, $V \subseteq Y$ such that $f(U) \subseteq V$, we define similarly a homomorphism $\tau_{U,V}$ and note that if $U' \subseteq U$, $V' \subseteq V$ and $f(U') \subseteq V'$, then $\tau_{U,V}$ extends $\tau_{U',V'}$. If x and y are the generic points of X and Y, respectively, then $f(x) = y$ and

$$(f^*(\mathscr{K}_Y))_x = \mathscr{O}_{Y,y} \otimes_{\mathscr{O}_{Y,y}} \mathscr{O}_{X,x} = \mathscr{O}_{X,x}$$

and τ_x is therefore an isomorphism. However, the homomorphism τ is usually not an isomorphism: for example, if $B = L$ is a field containing the integral domain A and A is not a field, the canonical homomorphism $L \otimes_B A \to K$ is then the canonical homomorphism $A \to K$, which is not bijective.

22.7.4 Torsion sheaves and torsion-free sheaves

Let X be a reduced scheme whose family of irreducible components is locally finite. For any $\mathscr{O}_X$-module $\mathscr{F}$, the canonical homomorphism $\mathscr{O}_X \to \mathscr{K}_X$ is injective by Proposition 22.7.22, and defines a homomorphism $\mathscr{F} \to \mathscr{F} \otimes_{\mathscr{O}_X} \mathscr{K}_X$ which on each stalk, is none other than the homomorphism $z \mapsto z \otimes 1$ from $\mathscr{F}_x$ to $\mathscr{F}_x \otimes_{\mathscr{O}_{X,x}} \mathscr{K}_{X,x}$. The kernel $\mathscr{T}$ (also denoted by $\mathscr{T}(\mathscr{F})$) of this homomorphism is a sub-$\mathscr{O}_X$-module $\mathscr{F}$ is called the **torsion sheaf** of $\mathscr{F}$, which is quasi-coherent if $\mathscr{F}$ is quasi-coherent (Proposition 22.7.18). The sheaf $\mathscr{F}$ is called **torsion-free** if $\mathscr{T} = 0$, and a **torsion sheaf** if $\mathscr{T} = \mathscr{F}$. For any $\mathscr{O}_X$-module $\mathscr{F}$, $\mathscr{F}/\mathscr{T}$ is torsion-free.

Proposition 22.7.23. *If X is an integral scheme, for a quasi-coherent $\mathscr{O}_X$-module $\mathscr{F}$ to be torsion-free, it is necessary and sufficient that it is isomorphic to a sub-$\mathscr{O}_X$-module $\mathscr{G}$ of a simple sheaf of the form $\mathscr{K}_X^{\oplus I}$, generated (as a $\mathscr{K}_X$-module) by $\mathscr{G}$.*

Proof. This follows from Corollary 22.7.21, since $\mathscr{F}$ is torsion-free if and only if the canonical homomorphism $\mathscr{F} \to \mathscr{F} \otimes_{\mathscr{O}_X} \mathscr{K}_X$ is injective. □

The cardinality of the set I is called the **rank** of $\mathscr{F}$. For any affine open U of X, since the generic point of x is contained in U, the rank of $\mathscr{F}$ is also equal to the rank of $\Gamma(U, \mathscr{F})$ as a $\Gamma(U, \mathscr{O}_X)$-module.

Corollary 22.7.24. *Over an integral scheme X, any torsion-free quasi-coherent $\mathscr{O}_X$-module of rank* 1 *(and in particular any invertible $\mathscr{O}_X$-module) is isomorphic to a sub-$\mathscr{O}_X$-module of $\mathscr{K}_X$, and the converse is also true.*

Corollary 22.7.25. *Let X be an integral scheme, $\mathscr{L}$, $\mathscr{L}'$ be two torsion-free $\mathscr{O}_X$-module, s (resp. s') be two sections of $\mathscr{L}$ (resp. $\mathscr{L}'$) over X. For $s \otimes s' = 0$, it is necessary and sufficient that one of the sections s, s' is zero.*

Proof. Let x be the generic point of X. We have by hypothesis $(s \otimes s')_x = s_x \otimes s'_x = 0$. As $\mathscr{L}_x$ and $\mathscr{L}'_x$ are identified with sub-$\mathscr{O}_{X,x}$-modules of the field $\mathscr{O}_{X,x}$, the preceding relation implies $s_x = 0$ or $s'_x = 0$, and therefore $s = 0$ or $s' = 0$ since $\mathscr{L}$ and $\mathscr{L}'$ are torsion-free (Corollary 22.7.20). □

Proposition 22.7.26. *Let X and Y be two integral schemes and $f : X \to Y$ be a dominant morphism. For any torsion-free quasi-coherent $\mathscr{O}_X$-module $\mathscr{F}$, $f_*(\mathscr{F})$ is a torsion-free $\mathscr{O}_Y$-module.*

Proof. As f_* is left exact, it suffices, in view of Proposition 22.7.23, to prove the proposition for $\mathscr{F} = \mathscr{K}_X^{\oplus I}$. Now any open subset U of Y contains the generic point of Y, hence $f^{-1}(U)$ contains the generic point of X, so we have $\Gamma(U, f_*(\mathscr{F})) = \Gamma(f^{-1}(U), \mathscr{F}) = K(X)^{\oplus I}$. Therefore $f_*(\mathscr{F})$ is the simple sheaf with stalk $K(X)^{\oplus I}$, considered as a $\mathscr{K}_Y$-module, and it is evidently torsion-free. □

Proposition 22.7.27. *Let X be reduced scheme whose family of irreducible components is locally finite. For any quasi-coherent $\mathscr{O}_X$-module $\mathscr{F}$ of finite type, the following conditions are equivalent:*

(i) *$\mathscr{F}$ is a torsion sheaf.*

(ii) *$\mathscr{F}_x = 0$ for every maximal point of x.*

(iii) $\operatorname{supp}(\mathscr{F})$ *contains no irreducible component of X.*

Proof. Since the question is local, we may assume that X has finitely many irreducible components $(X_i)_{1 \leq i \leq n}$, with generic points x_i. Endow each X_i the reduced subscheme structure of X, and let $\iota_i : X_i \to X$ be the canonical injection. If we put $\mathscr{F} = \iota_i^*(\mathscr{F})$, we see immediately that (Corollary 22.7.19) $\mathscr{F}$ is torsion-free if and only if each $\mathscr{F}_i$ is torsion-free. As $\mathscr{F}_{x_i} = (\mathscr{F}_i)_{x_i}$, to establish the equivalence of (i) and (ii), we can assume that X is integral. But then if x is the generic point of X, the relation $\mathscr{F}_x = 0$ and $\mathscr{F} \otimes_{\mathscr{O}_X} \mathscr{K}_X = 0$ are equivalent by Proposition 22.7.23 and Corollary 22.7.20. The equivalenct of (ii) and (iii) results from the fact that $\operatorname{supp}(\mathscr{F})$ is closed in X (since $\mathscr{F}$ is quasi-coherent) and that the conditions $\operatorname{supp}(\mathscr{F}) \cap X_i = \varnothing$ and $x_i \notin \operatorname{supp}(\mathscr{F})$ are then equivalent. □

22.7.5 Separation criterion for integral schemes

Let X be an integral scheme, K its function field, identified with the local ring at the generic point ξ of X. For any $x \in X$, we can identify $\mathscr{O}_{X,x}$ as a subring of K, formed by the rational functions defined at the point x. For any rational function $f \in K$, the defining domain $\delta(f)$ of f is then the open subset of $x \in X$ such that $f \in \mathscr{O}_{X,x}$, and in view of Corollary 22.7.14 we have, for each open subset $U \subseteq X$, that

$$\Gamma(U, \mathscr{O}_X) = \bigcap_{x \in U} \mathscr{O}_{X,x}. \tag{7.5.1}$$

Given a field K, for any subring A of K, we denote by $L(A)$ the set of localizations $A_{\mathfrak{p}}$, where $\mathfrak{p}$ runs through prime ideals of A; they are identified with local subrings of K containing A. As $\mathfrak{p} = (\mathfrak{p}A_{\mathfrak{p}}) \cap A$, the map $\mathfrak{p} \mapsto A_{\mathfrak{p}}$ from $\operatorname{Spec}(A)$ to $L(A)$ is bijective.

Lemma 22.7.28. *Let K be a field and A be a subring of K. For a local subring R to dominate a ring in $L(A)$, it is necessary and sufficient that $A \subseteq R$. In this case, the local ring $A_{\mathfrak{p}}$ dominated by R is then unique and corresponds to the prime ideal $\mathfrak{p} = \mathfrak{m}_R \cap A$, where $\mathfrak{m}_R$ is the maximal ideal of R.*

Proof. In fact, if R dominates $A_{\mathfrak{p}}$, then $\mathfrak{m}_R \cap A_{\mathfrak{p}} = \mathfrak{p}A_{\mathfrak{p}}$ by Proposition 14.1.6, hence the uniqueness of $\mathfrak{p}$. On the other hand, if $A \subseteq R$, $\mathfrak{m}_R \cap A = \mathfrak{p}$ is a prime ideal of A, and as the elements of $A - \mathfrak{p}$ are then invertible in R, we have $A_{\mathfrak{p}} \subseteq R$, so $\mathfrak{p}A_{\mathfrak{p}} \subseteq \mathfrak{m}_R$ and R dominates $A_{\mathfrak{p}}$. □

Lemma 22.7.29. *Let K be a field, A, B be two local subrings of K, and C be the subring of K generated by $A \cup B$. The following conditions are equivalent:*

(i) There exists a prime ideal $\mathfrak{r}$ of C such that $\mathfrak{m}_A = \mathfrak{r} \cap A$ and $\mathfrak{m}_B = \mathfrak{r} \cap B$.

(ii) The ideal $\mathfrak{c}$ generated in C by $\mathfrak{m}_A \cup \mathfrak{m}_B$ is proper.

(iii) There exists a local subring R of K dominating both A and B.

Proof. It is clear that (i) implies (ii). Conversely, if $\mathfrak{c}$ is proper, it is contained in a maximal ideal $\mathfrak{n}$ of C, and $\mathfrak{n} \cap A$ contains $\mathfrak{m}_A$ and is proper, so $\mathfrak{n} \cap A = \mathfrak{m}_A$ and similarly $\mathfrak{n} \cap B = \mathfrak{m}_B$. Finally, it is clear that if R dominates A and B then $C \subseteq R$ and $\mathfrak{m}_A = \mathfrak{m}_R \cap A = (\mathfrak{m}_R \cap C) \cap A$, $\mathfrak{m}_B = \mathfrak{m}_R \cap B = (\mathfrak{m}_R \cap C) \cap B$, so (iii) implies (i). the converse is clear since we can take $R = C_{\mathfrak{r}}$. □

If the equivalent conditions in Lemma 22.7.29 hold, we say the two local subrings A and B are **related**.

Proposition 22.7.30. *Let A and B be subrings of a field K and C be the subring of K generated by $A \cup B$. The following conditions are equivalent:*

(i) For any local ring R containing A and B, we have $A_{\mathfrak{p}} = B_{\mathfrak{q}}$, where $\mathfrak{p} = \mathfrak{m}_R \cap A$ and $\mathfrak{q} = \mathfrak{m}_R \cap B$.

(ii) For any prime ideal $\mathfrak{r}$ of C, we have $A_{\mathfrak{p}} = B_{\mathfrak{q}}$, where $\mathfrak{p} = \mathfrak{r} \cap A$ and $\mathfrak{q} = \mathfrak{r} \cap B$.

(iii) If $P \in L(A)$ and $Q \in L(B)$ are related, they are identical.

(iv) We have $L(A) \cap L(B) = L(C)$.

Proof. It follows from Lemma 22.7.28 and Lemma 22.7.29 that (i) and (iii) are equivalent, and (i) implies (ii) by applying (i) to the ring $R = C_{\mathfrak{r}}$. Conversely, (ii) implies (i) because if R contains $A \cup B$, it contains C, and if $\mathfrak{r} = \mathfrak{m}_R \cap C$, we have $\mathfrak{p} = \mathfrak{r} \cap A$ and $\mathfrak{q} = \mathfrak{r} \cap B$, so $A_{\mathfrak{p}} = B_{\mathfrak{q}}$. We also see that (iv) implies (i), because if R contains $A \cup B$, it then dominates a local ring $C_{\mathfrak{r}} \in L(C)$ by Lemma 22.7.28; we have by hypothesis that $L(C) = L(A) \cap L(B)$, and as R dominates a unique ring in $L(A)$ (resp. $L(B)$), we conclude that $C_{\mathfrak{r}} = A_{\mathfrak{p}} = B_{\mathfrak{q}}$.

Finally, we show that (iii) implies (iv). Let $R \in L(C)$; R then dominates a ring $P \in L(A)$ and a ring $Q \in L(B)$ by Lemma 22.7.28, so P and Q are related, hence identical by hypothesis. As we then have $C \subseteq P$, P dominates a ring $R' \in L(C)$ (Lemma 22.7.28), so R dominates the ring R', and by Lemma 22.7.28 we necessarily have $R = R' = P$, so $R \in L(A) \cap L(B)$. Conversely, if $R \in L(A) \cap L(B)$, we have $C \subseteq R$, so R dominates a ring $R'' \in L(C)$ by Lemma 22.7.28. The two subrings R and R'' are clearly related, and as $L(C) \subseteq L(A) \cap L(B)$, we conclude from condition (iii) that $R = R''$, so $R \in L(C)$ and the proof is complete. □

Proposition 22.7.31. *Let X be an integral scheme and K be its field of rational functions. Then for X to be separated, it is necessary and sufficient that the relation "$\mathscr{O}_{X,x}$ and $\mathscr{O}_{X,y}$ are related" for two points $x, y \in X$ implies $x = y$.*

Proof. Suppose the given condition on X, we prove that X is separated. Let $U = \operatorname{Spec}(A)$ and $V = \operatorname{Spec}(B)$ be two distinct affine opens of X, with A, B identified as subrings of K. Then U (resp. V) is identified with the set $L(A)$ (resp. $L(B)$), and by Proposition 22.7.30 the hypothesis on X implies that, if C is the subring of K generated by $A \cup B$, $W = U \cap V$ is identified with $L(A) \cap L(B) = L(C)$. Moreover, we have seen from Proposition 10.3.25 that any subring R of K is equal to the intersection of the local rings belong to $L(R)$, so

$$C = \bigcap_{z \in W} \mathscr{O}_{X,z} = \Gamma(W, \mathscr{O}_X) \tag{7.5.2}$$

where we use formula (7.5.1). Consider then the subscheme induced by X over W. The identity homomorphism $\varphi : C \to \Gamma(W, \mathscr{O}_X)$ corresponds to a morphism $\psi : W \to \operatorname{Spec}(C)$. In view of (7.5.2) and the relation $L(C) = L(A) \cap L(B)$, any prime ideal $\mathfrak{r}$ of C is of the form $\mathfrak{r} = \mathfrak{m}_x \cap C$, where $x \in W$ is the point in $\operatorname{Spec}(C)$ corresponding to $\mathfrak{r}$, and the map ψ just sends x to $\mathfrak{r}$, so it is bijective. On the other hand, for any $x \in W$, $\psi_x^\#$ is the canonical injection $C_{\mathfrak{r}} \to \mathscr{O}_{X,x}$, where $\mathfrak{r} = \mathfrak{m}_x \cap C$. Now the local ring $\mathscr{O}_{X,x}$ dominates $A_{\mathfrak{p}}$, $B_{\mathfrak{q}}$ and $C_{\mathfrak{r}}$, where $\mathfrak{p} = \mathfrak{m}_x \cap A$ and $\mathfrak{q} = \mathfrak{m}_x \cap B$, and as $C_{\mathfrak{r}} \in L(C) = L(A) \cap L(B)$, by Lemma 22.7.28 we then conclude that $C_{\mathfrak{r}} = A_{\mathfrak{p}} = B_{\mathfrak{q}}$ (we already have seen this in the proof of Proposition 22.7.30). But the local rings $A_{\mathfrak{p}}$ and $B_{\mathfrak{q}}$ are both identified with the stalk $\mathscr{O}_{X,x}$, so we see that $C_{\mathfrak{r}} = \mathscr{O}_{X,x}$ and $\psi_x^\#$ is bijective. It then remains to show that ψ is a homeomorphism, which amounts to show that, for any closed subset $F \subseteq W$, the image $\psi(F)$ is closed in $\operatorname{Spec}(C)$. Now F is the intersection with W of a closed subset E of the form $V(\mathfrak{a})$, where $\mathfrak{a}$ is an ideal of A. We claim that $\psi(F) = V(\mathfrak{a}C)$: in fact, the prime ideal of C containing $\mathfrak{a}C$ are the prime ideals of C containing $\mathfrak{a}$, hence the ideals of the form $\psi(x) = \mathfrak{m}_x \cap C$, where $\mathfrak{a} \subseteq \mathfrak{m}_x$ and $x \in W$. As $\mathfrak{a} \subseteq \mathfrak{m}_x$ is equivalent to $x \in V(\mathfrak{a}) = W \cap E$ for $x \in U$, we then get $\psi(F) = V(\mathfrak{a}C)$. In view of Proposition 22.5.30, we then conclude that X is separated, because $U \cap V$ is affine and the ring C is generated by $A \cup B$.

Conversely, suppse that X is separated, and let x, y be two points of X such that $\mathscr{O}_{X,x}$ and $\mathscr{O}_{X,y}$ are related. Let U (resp. V) be an open affine containing x (resp. y), with ring A (resp. B). We then see $U \cap V$ is affine and its ring C is generated by $A \cup B$ (Proposition 22.5.30). If

$\mathfrak{p} = \mathfrak{m}_x \cap A$ and $\mathfrak{q} = \mathfrak{m}_x \cap B$, we have $A_\mathfrak{p} = \mathcal{O}_{X,x}$ and $B_\mathfrak{q} = \mathcal{O}_{X,y}$, so $A_\mathfrak{p}$ and $B_\mathfrak{q}$ are related. Then by Lemma 22.7.29 there exists a prime ideal $\mathfrak{r}$ of C such that $\mathfrak{p} = \mathfrak{r} \cap A$, $\mathfrak{q} = \mathfrak{r} \cap B$. But the prime ideal $\mathfrak{r}$ then corresponds to a point $z \in U \cap V$ since $U \cap V$ is affine, and we have $x = z$ and $y = z$, so $x = y$. □

Corollary 22.7.32. *Let X be a separated integral scheme and x, y be two points of X. For $x \in \overline{\{y\}}$, it is necessary and sufficient that $\mathcal{O}_{X,x} \subseteq \mathcal{O}_{Y,y}$, which means the rational functions defined at x are also defined at y.*

Proof. This condition is clearly necessary since the defining domain $\delta(f)$ of a rational function is open, hence stable under generalization. To see it is also sufficient, assume that $\mathcal{O}_{X,x} \subseteq \mathcal{O}_{X,y}$, so there exists a prime ideal $\mathfrak{p}$ of $\mathcal{O}_{X,x}$ such that $\mathcal{O}_{Y,y}$ dominates $(\mathcal{O}_{X,x})_\mathfrak{p}$ (Lemma 22.7.28). By Corollary 22.2.10, there exists $z \in X$ such that $x \in \overline{\{z\}}$ and $\mathcal{O}_{X,z} = (\mathcal{O}_{X,x})_\mathfrak{p}$; as $\mathcal{O}_{X,z}$ and $\mathcal{O}_{X,y}$ are then related, we have $z = y$ by Proposition 22.7.31, whence the corollary. □

Corollary 22.7.33. *If X is a separated integral scheme, the map $x \mapsto \mathcal{O}_{X,x}$ is injective. In other words, if x, y are two distinct points of X, there exists a rational function defined at only one of these points.*

Proof. This follows from Corollary 22.7.32 and the T_0-axiom. □

Corollary 22.7.34. *Let X be a Noetherian separated integral scheme. The sets $\delta(f)$ for $f \in K(X)$ form a subbasis the topology of X.*

Proof. In fact, any closed subset of X is then a finite union of irreducible closed subsets, which are of the form $\overline{\{y\}}$. Now if $x \notin \overline{\{y\}}$, there exists a rational function f defined at x but not at y (Corollary 22.7.33), which means $x \in \delta(f)$ and $\delta(f) \cap \overline{\{y\}} = \varnothing$. The complement of $\overline{\{y\}}$ is then a union of sets of the form $\delta(f)$, and in view of the previous remark, any open subset of X is a union of finite intersections of sets of the form $\delta(f)$. □

Proposition 22.7.35. *Let X, Y be two integral schemes with rational function fields K and L, respectively. Suppose that Y is separated and let $f : X \to Y$ be a dominant morphism. Then L is identified with a subfield of K, and for every point $x \in X$, $\mathcal{O}_{Y,f(x)}$ is the unique local ring of Y dominated by $\mathcal{O}_{X,x}$.*

Proof. Ths first assertion is already proved in Proposition 22.4.21. Now for every $x \in X$, the local homomorphism $f_x^\# : \mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x}$ is injective by Proposition 22.4.21, so, if we identify L as a subfield of K, $\mathcal{O}_{Y,f(x)}$ is dominated by $\mathcal{O}_{X,x}$. As Y is separated, two local rings of Y can not be dominated by the same local ring (Proposition 22.7.31), so our assertion follows. □

Proposition 22.7.36. *Let X be an irreducible scheme and $f : X \to Y$ be a local immersion (resp. a local isomorphism). Suppose that f is separated, then it is an immersion (resp. an open immersion).*

Proof. It suffices to prove that f is a homeomorphism from X to $f(X)$ (Proposition 22.4.9). By replacing f with f_{red}, we may assume that X and Y are reduced. If Y' is the reduced subscheme of Y with underlying space $\overline{f(X)}$, f then factors into

$$X \xrightarrow{f'} Y' \xrightarrow{j} Y$$

where j is the canonical injection. Then f' is separated by Proposition 22.5.25(v) and is a local immersion by Proposition 22.5.15(iii), so we may reduce to the case that f is dominant.

But then Y is irreducible by Proposition 4.1.6, and by Proposition 22.4.21, we see f is in fact a local isomorphism, so for each $x \in X$ the homomorphism $f_x^\#$ is an isomorphism. By Corollary 22.7.33, this implies that f is injective, so f is in fact a homeomorphism. □

22.8 Formal schemes

22.8.1 Formal affine schemes and morphisms

LEt A be a admissible topological ring, with a defining ideal $\mathfrak{I}$; $\mathrm{Spec}(A/\mathfrak{I})$ is then a closed subscheme of $\mathrm{Spec}(A)$, which is the set of open prime ideals of A. This topological space does not depend on the defining ideal of $\mathfrak{I}$, and we denote it by $\mathfrak{X}$. Let $(\mathfrak{I}_\lambda)$ be a system of fundamental neighborhood of 0 in A, formed by the defining ideals of A, and for any λ, let $\mathcal{O}_\lambda$ be the structural sheaf of $\mathrm{Spec}(A/\mathfrak{I}_\lambda)$. This sheaf is induced over $\mathfrak{X}$ by $\widetilde{A}/\widetilde{\mathcal{F}}_\lambda$ (which is zero outside $\mathfrak{X}$). For $\mathfrak{I}_\mu \subseteq \mathfrak{I}_\lambda$, the canonical homomorphism $A/\mathfrak{I}_\mu \to A/\mathfrak{I}_\lambda$ defines a homomorphism $u_{\lambda\mu} : \mathcal{O}_\mu \to \mathcal{O}_\lambda$ of sheaves of rings, and $(\mathcal{O}_\lambda)$ is a projective system of sheaves of rings for these homomorphisms. As the topology of $\mathfrak{X}$ admits a basis formed by quasi-compact open subsets, we can associate to any $\mathcal{O}_\lambda$ a sheaf of discrete topological rings with $\mathcal{O}_\lambda$ as underlying ring, still denoted by $\mathcal{O}_\lambda$; the $\mathcal{O}_\lambda$ then form a projective system of sheaves of topological rings. We denote by $\mathcal{O}_\mathfrak{X}$ the limit of this system $(\mathcal{O}_\lambda)$; by **??**, for any quasi-compact open subset U of $\mathfrak{X}$, $\Gamma(U, \mathcal{O}_\mathfrak{X})$ is then the limit topological ring of the discrete rings $\Gamma(U, \mathcal{O}_\lambda)$.

Given an admissible topological ring A, the closed subspace $\mathfrak{X}$ of $\mathrm{Spec}(A)$ formed by open prime ideals of A is called the **formal spectrum** of A and denoted by $\mathrm{Spf}(A)$. A topoloigcally ringed space is called a **formal affine scheme** if it is isomorphic to a formal spectrum $\mathrm{Spf}(A) = \mathfrak{X}$ endowed with the sheaf of topological rings $\mathcal{O}_\mathfrak{X}$, which is the limit of the sheaf of discrete rings $(\widetilde{A}/\widetilde{\mathfrak{I}_\lambda})|_\mathfrak{X}$, where $\mathfrak{I}_\lambda$ runs through the filtered set of defining ideals of A. When we speak of a formal spectrum $\mathfrak{X} = \mathrm{Spf}(A)$ as an formal affine scheme, it will always be understood that the topologically ringed space $(\mathfrak{X}, \mathcal{O}_\mathfrak{X})$ where $\mathcal{O}_\mathfrak{X}$ is defined as above. By an **adic** (resp. **Noetherian**) formal affine scheme, we mean a formal affine scheme which is isomorphic to a formal specturm $\mathrm{Spf}(A)$, where A is adic (resp. adic and Noetherian).

We note that any affine scheme $X = \mathrm{Spec}(A)$ can be considered as a formal affine scheme in a unique way: consider A as a discrete topological ring, the rings $\Gamma(U, \mathcal{O}_X)$ are then discrete if U is quasi-compact (but not true in general if U is any open set of X).

Proposition 22.8.1. *If $\mathfrak{X} = \mathrm{Spf}(A)$, where A is an admissible ring, then $\Gamma(X, \mathcal{O}_\mathfrak{X})$ is homeomorphic to A.*

Proof. In fact, as $\mathfrak{X}$ is closed in $\mathrm{Spec}(A)$, it is quasi-compact, and therefore $\Gamma(\mathfrak{X}, \mathcal{O}_\mathfrak{X})$ is homeomorphic to the limit of the discrete rings $\Gamma(\mathfrak{X}, \mathcal{O}_\lambda)$. But $\Gamma(\mathfrak{X}, \mathcal{O}_\lambda)$ is isomorphic to $A/\mathfrak{I}_\lambda$, and as A is separated and complete, this is homeomorphic to $\varinjlim A/\mathfrak{I}_\lambda$, whence the proposition. □

Proposition 22.8.2. *Let A be an admissible ring, $\mathfrak{X} = \mathrm{Spf}(A)$, and for $f \in A$, let $\mathfrak{D}(f) = D(f) \cap \mathfrak{X}$. Then the topologically ringed space $(\mathfrak{D}(f), \mathcal{O}_\mathfrak{X}|_{\mathfrak{D}(f)})$ is isomorphic to a formal affine spectrum $\mathrm{Spf}(A_{\{f\}})$.*

Proof. For any defining ideal $\mathfrak{I}$ of A, the discrete ring $A_f/\mathfrak{I}_f$ is canonically identified with $A_{\{f\}}/\mathfrak{I}_{\{f\}}$ (**??**), so the topological space $\mathrm{Spf}(A_{\{f\}})$ is canonically identified with $\mathfrak{D}(f)$. Moreover, for any quasi-compact open U of $\mathfrak{X}$ contained in $\mathfrak{D}(f)$, $\Gamma(U, \mathcal{O}_\lambda)$ is identified with the module

of sections of the structural sheaf of $\mathrm{Spec}(A_f/\mathfrak{I}_\lambda)$ over U, so, if we put $\mathfrak{Y} = \mathrm{Spf}(A_{\{f\}})$, $\Gamma(U, \mathcal{O}_{\mathfrak{X}})$ is identified with $\Gamma(U, \mathcal{O}_{\mathfrak{Y}})$, whence the proposition. □

As a sheaf of rings, the stalk of the structural sheaf $\mathcal{O}_{\mathfrak{X}}$ of $\mathrm{Spf}(A)$ for any $x \in X$ is, by Proposition 22.8.2, identified with the inductive limit $\varinjlim A_{\{f\}}$ for $f \notin \mathfrak{p}_x$. Therefore, by **??** and **??**, we have the following result:

Proposition 22.8.3. *For any $x \in \mathfrak{X} = \mathrm{Spf}(A)$, the stalk $\mathcal{O}_{\mathfrak{X},x}$ is a local ring whose residue field is isomorphic to $\kappa(x) = A_x/\mathfrak{p}_x A_x$. If A is adic and Noetherian, then $\mathcal{O}_{X,x}$ is a Noetherian ring.*

As the field $\kappa(x)$ is not reduced to 0, we conclude in particular that the support of $\mathcal{O}_{\mathfrak{X}}$ is equal to $\mathfrak{X}$, and $(\mathfrak{X}, \mathcal{O}_{\mathfrak{X}})$ is a locally topologically ringed space.

We now consider morphisms of formal affine schemes. Let A, B be admissible rings, and $\varphi : B \to A$ be a continuous homomorphism. The continuous map ${}^a\varphi : \mathrm{Spec}(A) \to \mathrm{Spec}(B)$ then maps $\mathfrak{X} = \mathrm{Spf}(A)$ into $\mathfrak{Y} = \mathrm{Spf}(B)$, because the inverse image of an open prime ideal of A is an open prime ideal of B. On the other hand, for any $g \in B$, φ defines a continuous homomorphism $\Gamma(\mathfrak{D}(g), \mathcal{O}_{\mathfrak{Y}}) \to \Gamma(\mathfrak{D}(\varphi(g), \mathcal{O}_{\mathfrak{X}}))$ in view of Proposition 22.8.1 and Proposition 22.8.2; as these homomorphisms are compatible with restrictions and $\mathfrak{D}(\varphi(g)) = ({}^a\varphi)^{-1}(\mathfrak{D}(g))$, we obtain a continuous homomorphism of sheaves of topological rings $\mathcal{O}_{\mathfrak{Y}} \to {}^a\varphi_*(\mathcal{O}_{\mathfrak{X}})$, which we denoted by $\tilde{\varphi}$. We then get a morphism $({}^a\varphi, \tilde{\varphi}) : (X, \mathcal{O}_{\mathfrak{X}}) \to (\mathfrak{Y}, \mathcal{O}_{\mathfrak{Y}})$ of topologically ringed spaces.

Proposition 22.8.4. *Let A, B be admissible topological rings, and $\mathfrak{X} = \mathrm{Spf}(A)$, $\mathfrak{Y} = \mathrm{Spf}(B)$. For a morphism $\psi : \mathfrak{X} \to \mathfrak{Y}$ of topologically ringed spaces to be of the form $({}^a\varphi, \tilde{\varphi}) : \mathfrak{X} \to \mathfrak{Y}$, it is necessary and sufficient that for each $x \in X$, $f_x^\# : \mathcal{O}_{\mathfrak{Y},\psi(x)} \to \mathcal{O}_{\mathfrak{X},x}$ is a local homomorphism.*

Proof. This conditions is necessary: in fact, let $\mathfrak{p} = \mathfrak{p}_x \in \mathrm{Spf}(A)$, and $\mathfrak{q} = \varphi^{-1}(\mathfrak{p}_x)$; if $g \notin \mathfrak{q}$, then $\varphi(g) \notin \mathfrak{p}$, and it is immediate that the homomorphism $B_{\{g\}} \to A_{\{\varphi(g)\}}$ induced from φ maps $\mathfrak{q}_{\{g\}}$ into $\mathfrak{p}_{\{\varphi(g)\}}$; by passing to inductive limit, we then see that $\tilde{\varphi}_x$ is a local homomorphism.

Conversely, let ψ be a morphism satisfying this condition. By Proposition 22.8.1, $\psi^\#$ defines a continuous homomorphism

$$\varphi = \Gamma(\psi^\#) : B = \Gamma(\mathfrak{Y}, \mathcal{O}_{\mathfrak{Y}}) \to \Gamma(\mathfrak{X}, \mathcal{O}_{\mathfrak{X}}) = A.$$

By the hypothesis on $\psi^\#$, for the section $\varphi(g)$ of $\mathcal{O}_{\mathfrak{X}}$ over $\mathfrak{X}$ has invertible germ at a point x, it is necessary and sufficient that g has invertible germ at $\psi(x)$. But by **??**, the sections of $\mathcal{O}_{\mathfrak{X}}$ (resp. $\mathcal{O}_{\mathfrak{Y}}$) over $\mathfrak{X}$ (resp. $\mathfrak{Y}$) which have non-invertible germs at x (resp. $\psi(x)$) are exactly the elements of $\mathfrak{p}_x$ (resp $\mathfrak{p}_{\psi(x)}$), so we conclude that $\psi = {}^a\varphi$. Finally, for any $g \in B$, the diagram

$$\begin{tikzcd}
B = \Gamma(\mathfrak{Y}, \mathcal{O}_{\mathfrak{Y}}) \arrow[r, "\varphi"] & \Gamma(\mathfrak{X}, \mathcal{O}_{\mathfrak{X}}) = A \arrow[d] \\
B_{\{g\}} = \Gamma(\mathfrak{D}(g), \mathcal{O}_{\mathfrak{Y}}) \arrow[r, "\Gamma(\psi^\#_{\mathfrak{D}(g)})"] & \Gamma(\mathfrak{D}(\varphi(g), \mathcal{O}_{\mathfrak{X}})) = A_{\{\varphi(g)\}}
\end{tikzcd}$$

is commutative. By the universal property of localization of complete rings (**??**), we conclude that $\psi^\#_{\mathfrak{D}(g)}$ is equal to $\tilde{\varphi}_{\mathfrak{D}(g)}$ for $g \in B$, so we have $\psi^\# = \tilde{\varphi}$. □

We say a morphism $\psi : \mathfrak{X} \to \mathfrak{Y}$ satisfying the condition in Proposition 22.8.4 is a **morphism of formal affine schemes**. Then by Proposition 22.8.4, the functor $A \mapsto \mathrm{Spf}(A)$ and $\mathfrak{X} \to$

$\Gamma(\mathfrak{X}, \mathcal{O}_{\mathfrak{X}})$ define an equivalence from the category of admissible topological rings to the opposite of the category of formal affine schemes.

As a particular case of Proposition 22.8.4, note that for $f \in A$, the canonical injection of the formal affine scheme over $\mathfrak{D}(f)$ induced by $\mathfrak{X}$ corresponds to the canonical homomorphism $A \to A_{\{f\}}$. Under the hypothesis of Proposition 22.8.4, let h be an element of B and g be an element of A, which is a multiple of $\varphi(h)$. We then have $\psi(\mathfrak{D}(g)) \subseteq \mathfrak{D}(h)$; the restriction of ψ to $\mathfrak{D}(g)$, considered as a morphism $\mathfrak{D}(g) \to \mathfrak{D}(h)$, is the unique morphism η such that the diagram

$$\begin{tikzcd} \mathfrak{D}(g) \arrow[r, "\eta"] \arrow[d] & \mathfrak{D}(h) \arrow[d] \\ \mathfrak{X} \arrow[r, "\psi"] & \mathfrak{Y} \end{tikzcd}$$

This morphism corresponds to the unique continuous homomorphism $\varphi' : B_{\{h\}} \to A_{\{g\}}$ (**??**) such that the diagram

$$\begin{tikzcd} B \arrow[r, "\varphi"] \arrow[d] & A \arrow[d] \\ B_{\{h\}} \arrow[r, "\varphi'"] & A_{\{g\}} \end{tikzcd}$$

is commutative.

Let A be an admissible ring, $\mathfrak{I}$ be an open ideal of A, $\mathfrak{X}$ the formal affine scheme $\mathrm{Spf}(A)$. Let $(\mathfrak{I}_\lambda)$ be the set of defining ideals of A contained in $\mathfrak{I}$; then $\widetilde{\mathfrak{I}}/\widetilde{\mathfrak{I}}_\lambda$ is a sheaf of ideals of $\widetilde{A}/\widetilde{\mathfrak{I}}_\lambda$. Denote by $\mathfrak{I}^\Delta$ the projective limit of the sheaves induced by $\widetilde{\mathcal{I}}/\widetilde{\mathfrak{I}}_\lambda$ over $\mathfrak{X}$, which is identified as an ideal of $\mathcal{O}_{\mathfrak{X}}$. For any $f \in A$, $\Gamma(\mathfrak{D}(f), \mathfrak{I}^\Delta)$ is the projective limit of $\mathfrak{I}_f/(\mathcal{I}_\lambda)_f$, which is identified with the open ideal $\mathfrak{I}_{\{f\}}$ of the ring $A_{\{f\}}$ (**??**), and in particular $\Gamma(\mathfrak{X}, \mathfrak{I}^\Delta) = \mathfrak{I}$. We then conclude that (the $\mathfrak{D}(f)$ form a base of $\mathfrak{X}$) that we have

$$\mathfrak{I}^\Delta|_{\mathfrak{D}(f)} = (\mathfrak{I}_{\{f\}})^\Delta \tag{8.1.1}$$

With these notations, for $f \in A$ the canonical map of $A_{\{f\}} = \Gamma(\mathfrak{D}, \mathcal{O}_{\mathfrak{X}})$ in $\Gamma(\mathfrak{D}(f), (\widetilde{A}/\widetilde{\mathfrak{I}})|_{\mathfrak{X}}) = A_f/\mathfrak{I}_f$ is surjective with kernel $\Gamma(\mathfrak{D}(f), \mathfrak{I}^\Delta) = \mathfrak{I}_{\{f\}}$ (**??**). These maps define a canonical continuous epimorphism from the sheaf $\mathcal{O}_{\mathfrak{X}}$ to the sheaf of discrete rings $(\widetilde{A}/\widetilde{\mathfrak{I}})|_{\mathfrak{X}}$, whose kernel is $\mathfrak{I}^\Delta$; this homomorphism is none other than the homomorphism $\tilde{\varphi}$, where φ is the canonical continuous homomorphism $A \to A/\mathfrak{I}$. The morphism $({}^a\varphi, \tilde{\varphi}) : \mathrm{Spec}(A/\mathfrak{I}) \to \mathfrak{X}$ of the formal affine schemes is then called the canonical morphism. We then have a canonical isomorphism

$$\mathcal{O}_{\mathfrak{X}}/\mathfrak{I}^\Delta \xrightarrow{\sim} (\widetilde{A}/\widetilde{\mathfrak{I}})|_{\mathfrak{X}}. \tag{8.1.2}$$

It is clear (in view of $\Gamma(X, \mathfrak{I}^\Delta) = \mathfrak{I}$) that the map $\mathfrak{I} \mapsto \mathfrak{I}^\Delta$ is strictly increasing: in fact, for $\mathfrak{I} \subseteq \mathfrak{I}'$, the sheaf $\mathfrak{I}'^\Delta/\mathfrak{I}^\Delta$ is canonically isomorphic to $\widetilde{\mathfrak{I}'}/\widetilde{\mathfrak{I}} = \widetilde{\mathfrak{I}'/\mathfrak{I}}$.

We now say that an ideal $\mathcal{I}$ of $\mathcal{O}_{\mathfrak{X}}$ is a defining ideal of $\mathfrak{X}$ if, for any $x \in \mathfrak{X}$, there exists an open neighborhood of x in $\mathfrak{X}$ of the form $\mathfrak{D}(f)$, where $f \in A$, such that $\mathcal{I}|_{\mathfrak{D}(f)}$ is of the form $\mathfrak{J}^\Delta$ for a defining ideal $\mathfrak{J}$ of $A_{\{f\}}$. It is clear from our definiton that for any $f \in A$, any defining ideal of $\mathfrak{X}$ induces an defining ideal of $\mathfrak{D}(f)$.

Proposition 22.8.5. *If A is an admissible ring, any defining ideal of $\mathfrak{X} = \mathrm{Spf}(A)$ is of the form $\mathfrak{I}^\Delta$, where $\mathfrak{I}$ is a defining ideal of A.*

Proof. Let $\mathscr{I}$ be a defining ideal of $\mathfrak{X}$; by hypothesis, and since $\mathfrak{X}$ is quasi-compact, there exist finitely many elements $f_i \in A$ such that $\mathfrak{D}(f)$ cover $\mathfrak{X}$ and such that $\mathscr{I}|_{\mathfrak{D}(f)} = \mathfrak{J}_i$, where $\mathfrak{J}_i$ is a defining ideal of $A_{\{f_i\}}$. For any i, there then exists an open ideal $\mathfrak{I}_i$ of A such that $(\mathfrak{I}_i)_{\{f_i\}} = \mathfrak{J}_i$ (**??**); let $\mathfrak{R}$ be a defining ideal of A contained in each the $\mathfrak{I}_i$. The canonical image of $\mathscr{I}/\mathfrak{R}^\Delta$ in the structural sheaf $\widetilde{(A/\mathfrak{R})}$ of $\operatorname{Spec}(A/\mathfrak{R})$ is then such that its restriction to each $\mathfrak{D}(f_i)$ is equal to $\widetilde{\mathfrak{I}_i/\mathfrak{R}}$; we then conclude that this canonical image is a quasi-coherent ideal over $\operatorname{Spec}(A/\mathfrak{R})$, hence is of the form $\widetilde{\mathfrak{I}/\mathfrak{R}}$, where $\mathfrak{I}$ is an ideal of A containing $\mathfrak{R}$, and whence $\mathscr{I} = \mathfrak{I}^\Delta$ by (8.1.2). Moreover, as for each i there exists an integer n_i such that $\mathfrak{I}_i^{n_i} \subseteq \mathfrak{R}_{\{f_i\}}$, we have $(\mathscr{I}/\mathfrak{R}^\Delta)^n = 0$ for n sufficiently large, and therefore $(\widetilde{\mathfrak{I}/\mathfrak{R}})^n = 0$, and finally $(\mathfrak{I}/\mathfrak{R})^n = 0$, which proves that $\mathfrak{I}$ is a defining ideal of A. □

Proposition 22.8.6. *Let A be an adic ring, $\mathfrak{I}$ be a defining ideal of A such that $\mathfrak{I}/\mathfrak{I}$ is an $A/\mathfrak{I}$ of finte type. For any integer $n > 0$, we then have $(\mathfrak{I}^\Delta)^n = (\mathfrak{I}^n)^\Delta$.*

Proof. In fact, for any $f \in A$ we have (since $\mathfrak{I}^n$ is an open ideal)

$$(\Gamma(\mathfrak{D}(f), \mathfrak{I}^\Delta))^n = (\mathfrak{I}_{\{f\}})^n = (\mathfrak{I}^n)_{\{f\}} = \Gamma(\mathfrak{D}(f^n), (\mathfrak{I}^n)^\Delta)$$

in view of (8.1.1) and **??**. As $(\mathfrak{I}^\Delta)^n$ is associated with the presheaf $U \mapsto (\Gamma(U, \mathfrak{I}^\Delta))^n$, the corollary then follows since $\mathfrak{D}(f)$ form a basis for $\mathfrak{X}$. □

We say that a family $(\mathscr{I}_\lambda)$ of defining ideals of $\mathfrak{X}$ is a **fundamental system of defining ideals** if any defining ideal of $\mathscr{I}$ contains at least one of these $\mathscr{I}_\lambda$. As $\mathscr{I}_\lambda = \mathfrak{I}_\lambda^\Delta$, this is equivalent to saying that the $\mathfrak{I}_\lambda$ form a fundamental neighborhood of 0 in A, where $\mathscr{I}_\lambda = \mathscr{I}_\lambda^\Delta$. Let (f_α) be a family of elements of A such that the $\mathfrak{D}(f_\alpha)$ cover $\mathfrak{X}$. If $(\mathscr{I}_\lambda)$ is a filtered decreasing family of ideals of $\mathscr{O}_\mathfrak{X}$ such that for any α, the family $(\mathscr{I}_\lambda|_{\mathfrak{D}(f_\alpha)})$ is a fundamental system of defining ideals of $\mathfrak{D}(f_\alpha)$, then $(\mathscr{I}_\lambda)$ is a fundamental system of defining ideals of $\mathfrak{X}$. In fact, for any defining ideal of $\mathfrak{X}$, there exists a finite covering of $\mathfrak{X}$ by the $\mathfrak{D}(f_i)$ such that, for any i, $\mathscr{I}_{\lambda_i}|_{\mathfrak{D}(f_i)}$ is a defining ideal of $\mathfrak{D}(f_i)$ contained in $\mathfrak{I}|_{\mathfrak{D}(f_i)}$. If μ is an index such that $\mathscr{I}_\mu \subseteq \mathscr{I}_{\lambda_i}$ for all i, then $\mathscr{I}_\mu$ is a defining ideal of $\mathfrak{X}$ which is evidently contained in $\mathscr{I}$, whence the assertion.

22.8.2 Morphisms of formal schemes

Given a topologically ringed space $\mathfrak{X}$, we say an open subset $U \subseteq \mathfrak{X}$ is a **formal affine open** (resp. **an adic formal affine open**, resp. **a Noetherian formal affine open**) if the topologically ringed space $(U, \mathscr{O}_\mathfrak{X}|_U)$ is a formal affine scheme (resp. an adic formal affine scheme, resp. a Noetherian formal affine scheme). We way $(\mathfrak{X}, \mathscr{O}_\mathfrak{X})$ is a **formal scheme** (resp. adic formal scheme, resp. locally Noetherian formal scheme) if each of its point admits a formal affine open neighborhood (resp. an adic formal affine open, resp. a locally Noetherian formal affine open). We say that $\mathfrak{X}$ is Noetherian if it is locally Noetherian and the underlying space is quasi-compact (hence Noetherian). As any affine scheme can be considered as a formal affine scheme, any scheme can be considered as a formal scheme.

Proposition 22.8.7. *If $\mathfrak{X}$ is a formal scheme (resp. locally Noetherian formal scheme), the set of formal affine opens (resp. Noetherian formal affine opens) form a base for $\mathfrak{X}$.*

Proof. This follows from Proposition 22.8.2, and the fact that if A is a Noetherian adic ring, so is $A_{\{f\}}$ for any $f \in A$ (**??**). □

Corollary 22.8.8. *If $\mathfrak{X}$ is a formal scheme (resp. locally Noetherian formal scheme, resp. Noetherian formal scheme), the topological ringed space over any open subset of $\mathfrak{X}$ is a formal scheme (resp. locally Noetherian formal scheme, resp. Noetherian formal scheme).*

Given two formal schemes $\mathfrak{X}, \mathfrak{Y}$, we say that $f : \mathfrak{X} \to \mathfrak{Y}$ is a morphism of formal schemes if it is a morphism of the underlying locally ringed spaces. That is, if $(f, f^{\#})$ is a morphism of ringed spaces and $f_x^{\#} : \mathcal{O}_{\mathfrak{Y},f(x)} \to \mathcal{O}_{\mathfrak{X},x}$ is a local homomorphism. The composition of two morphisms are defined as the same and clearly a morphism of formal schemes. The formal schemes then form a category, which we denoted by **Shf**, and we denote by $\mathrm{Hom}_{\mathsf{Shf}}(\mathfrak{X}, \mathfrak{Y})$ the set of morphisms of formal schemes $\mathfrak{X} \to \mathfrak{Y}$.

If U is an open subset of $\mathfrak{X}$, the canonical injection $U \to \mathfrak{X}$ is then a morphism of formal schemes, if we endow U the formal scheme structure induced by $\mathfrak{X}$. It is clear that this morphism is a monomorphism in the category **Shf**.

Proposition 22.8.9. *Let $\mathfrak{X}$ be a formal scheme, $\mathfrak{Y} = \mathrm{Spec}(A)$ be a formal affine scheme. Then there exists a canonical bijection*

$$\mathrm{Hom}_{\mathbf{Scf}}(\mathfrak{X}, \mathfrak{Y}) \xrightarrow{\sim} \mathrm{Hom}_{\mathbf{TopRing}}(A, \Gamma(\mathfrak{X}, \mathcal{O}_{\mathfrak{X}})).$$

Proof. We first note that, if $(\mathfrak{X}, \mathcal{O}_{\mathfrak{X}})$ and $(\mathfrak{Y}, \mathcal{O}_{\mathfrak{Y}})$ are two topologically ringed spaces, a morphism $f : (\mathfrak{X}, \mathcal{O}_{\mathfrak{X}}) \to (\mathfrak{Y}, \mathcal{O}_{\mathfrak{Y}})$ defines canonically a continuous homomorphism of rings $\varphi : \Gamma(\mathfrak{Y}, \mathcal{O}_{\mathfrak{Y}}) \to \Gamma(\mathfrak{X}, \mathcal{O}_{\mathfrak{X}})$. In our case, we need to show that a continuous hommorphism $\varphi : A \to \Gamma(\mathfrak{X}, \mathcal{O}_{\mathfrak{X}})$ is of the form $\Gamma(\psi^{\#})$ for a unique morphism $(\psi, \psi^{\#})$. Now there exists by hypothesis a covering (V_α) of $\mathfrak{X}$ by formal affine opens; by composing φ with the restriction homomorphisms $\Gamma(\mathfrak{X}, \mathcal{O}_{\mathfrak{X}}) \to \Gamma(V_\alpha, \mathcal{O}_{\mathfrak{X}}|_{V_\alpha})$, we obtain a continuous homomorphism $\varphi_\alpha : A \to \Gamma(V_\alpha, \mathcal{O}_{\mathfrak{X}}|_{V_\alpha})$, which corresponds to a unique morphism $\psi_\alpha : (V_\alpha, \mathcal{O}_{\mathfrak{X}}|_{V_\alpha}) \to (\mathfrak{Y}, \mathcal{O}_{\mathfrak{Y}})$, in view of Proposition 22.8.4. Moreover, for any couple (α, β) of indices, any point of $V_\alpha \cap V_\beta$ admits a formal affine open neighborhood W contained in $V_\alpha \cap V_\beta$ and it is clear that the compositions of φ_α and φ_β with the canonical restriction are the same continuous homomorphism $\Gamma(\mathfrak{Y}, \mathcal{O}_{\mathfrak{Y}}) \to \Gamma(W, \mathcal{O}_{\mathfrak{X}}|_W)$, so, in view of the relations $(\psi_\alpha^{\#})_x = (\tilde{\varphi}_\alpha)_x$ for any $x \in V_\alpha$, the restrictions of ψ_α and ψ_β coincides on $V_\alpha \cap V_\beta$. We then conclude that there exists a unique morphism $\psi : (\mathfrak{X}, \mathcal{O}_{\mathfrak{X}}) \to (\mathfrak{Y}, \mathcal{O}_{\mathfrak{Y}})$ whose restriction to V_α coincides with ψ_α, and it is clear that this is the unique morphism such that $\Gamma(\psi^{\#}) = \varphi$. □

Given a formal scheme $\mathfrak{S}$, a **formal $\mathfrak{S}$-scheme** is defined to be a formal scheme $\mathfrak{X}$ together with a morphism $\varphi : \mathfrak{X} \to \mathfrak{S}$, called the **structural morphism** of $\mathfrak{X}$. If $\mathfrak{S} = \mathrm{Spf}(A)$, where A is an admissible ring, we also say that the $\mathfrak{S}$-formal scheme $\mathfrak{X}$ is a formal A-scheme or a formal scheme over A. Any formal scheme can be clearly considered as a formal scheme over $\mathbb{Z}$ (endowed with the discrete topology).

If $\mathfrak{X}, \mathfrak{Y}$ are two formal $\mathfrak{S}$-schemes, we say a morphism $f : \mathfrak{X} \to \mathfrak{Y}$ is an **$\mathfrak{S}$-morphism** if the diagram

$$\begin{tikzcd} \mathfrak{X} \arrow[rr, "f"] \arrow[dr] & & \mathfrak{Y} \arrow[dl] \\ & \mathfrak{S} & \end{tikzcd}$$

where the vertical arrows are structural morphisms, is commutative. With this definition,

the $\mathfrak{S}$-schemes form (for $\mathfrak{S}$ fixed) a category $\mathbf{Scf}_{\mathfrak{S}}$. We denote by $\mathrm{Hom}_{\mathfrak{S}}(\mathfrak{X}, \mathfrak{Y})$ the set of $\mathfrak{S}$-morphisms $\mathfrak{X} \to \mathfrak{Y}$. If $\mathfrak{S} = \mathrm{Spf}(A)$, we also say A-morphism for $\mathfrak{S}$-morphisms.

Let $\mathfrak{X}$ be a formal scheme; we say an ideal $\mathscr{I}$ of $\mathscr{O}_{\mathfrak{X}}$ is a defining ideal of $\mathfrak{X}$ if any $x \in \mathfrak{X}$ admits a formal affine open neighborhood U such that $\mathscr{I}|_U$ is a defining ideal of the formal scheme U induced by $\mathfrak{X}$. In view of Proposition 22.8.7, for any open $V \subseteq \mathfrak{X}$, $\mathscr{I}|_V$ is then a defining ideal of the formal scheme induced over V.

We say that a family $(\mathscr{I}_\lambda)$ of defining ideals of $\mathfrak{X}$ is a **fundamental system of defining ideals** if there exists a covering (U_α) of $\mathfrak{X}$ by formal affine opens such that, for any α, the family $(\mathscr{I}_\lambda|_{U_\alpha})$ form a fundamental system of defining ideals of U_α. For any open subset V of $\mathfrak{X}$, the family $(\mathscr{I}_\lambda|_V)$ then forms a fundamental system of defining ideals for V, in view of (8.1.1). If $\mathfrak{X}$ is locally Noetherian, and $\mathscr{I}$ is a defining ideal of $\mathfrak{X}$, it then follows from Proposition 22.8.6 that the powers of $\mathscr{I}^n$ form a fundamental system of defining ideals of $\mathfrak{X}$.

Let $\mathfrak{X}$ be a formal scheme, $\mathscr{I}$ be a defining ideal of $\mathfrak{X}$. Then the ringed space $(\mathfrak{X}, \mathscr{O}_{\mathfrak{X}}/\mathscr{I})$ is a scheme, which is affine (resp. locally Noetherian, resp. Noetherian) if $\mathfrak{X}$ is a formal affine scheme (resp. a locally Noetherian formal scheme, resp. a Noetherian formal scheme). Moreover, if $\varphi : \mathscr{O}_{\mathfrak{X}} \to \mathscr{O}_{\mathfrak{X}}/\mathscr{I}$ is the cannical homomorphism, then $(1_{\mathfrak{X}}, \varphi)$ is a morphism (called canonical) of formal schemes $(\mathfrak{X}, \mathscr{O}_{\mathfrak{X}}/\mathscr{I}) \to (\mathfrak{X}, \mathscr{O}_{\mathfrak{X}})$.

Proposition 22.8.10. *Let $\mathfrak{X}$ be a formal scheme, $(\mathscr{I}_\lambda)$ be a fundamental system of defining ideals of $\mathfrak{X}$. Then the sheaf $\mathscr{O}_{\mathfrak{X}}$ is the projective limit of the sheaf of discrete rings $\mathscr{O}_{\mathfrak{X}}/\mathscr{I}_\lambda$.*

Proof. As $\mathfrak{X}$ admits a basis by quasi-compact open sets, we are reduced to the affine case, where the proposition follows from Proposition 22.8.5 and the definition of $\mathscr{O}_{\mathfrak{X}}$. □

Proposition 22.8.11. *Let $\mathfrak{X}$ be a locally Noetherian formal scheme. Then there exists a largest defining ideal $\mathscr{T}$ of $\mathfrak{X}$, which is the unique defining ideal $\mathscr{I}$ such that the scheme $(\mathfrak{X}, \mathscr{O}_{\mathfrak{X}}/\mathscr{I})$ is reduced. If $\mathscr{I}$ is a defining ideal of $\mathfrak{X}$, $\mathscr{T}$ is the inverse image of the nilradical of $\mathscr{O}_{\mathfrak{X}}/\mathscr{I}$ under the homomorphism $\mathscr{O}_{\mathfrak{X}} \to \mathscr{O}_{\mathfrak{X}}/\mathscr{I}$. The reduced (usual) scheme $(\mathfrak{X}, \mathscr{O}_{\mathfrak{X}}/\mathscr{T})$ is denoted by $\mathfrak{X}_{\mathrm{red}}$.*

Proof. Suppose first that $\mathfrak{X} = \mathrm{Spf}(A)$, where A is a Noetherian adic ring. The existence of $\mathscr{T}$ and its properties then follows from Proposition 22.8.5, in view of **??** and **??** about the largest defining ideal of A. To prove the existence of $\mathscr{T}$ in the general case, it suffices to prove that if $V \subseteq U$ are two Noetherian formal affine opens of X, the largest defining ideal $\mathscr{T}_U$ of U induces the largest defining ideal $\mathscr{T}_V$ of V; but as $(V, (\mathscr{O}_{\mathfrak{X}}|_V)/(\mathscr{T}_U|_V))$ is reduced, this is immediate. □

Corollary 22.8.12. *Let $\mathfrak{X}$ be a locally Noetherian formal scheme, $\mathscr{T}$ be the largest defining ideal of $\mathfrak{X}$. Then for any open subset V of $\mathfrak{X}$, $\mathscr{T}|_V$ is the largest defining ideal of V.*

Proof. This is already shown in the proof of Proposition 22.8.11. □

Proposition 22.8.13. *Let $\mathfrak{X}, \mathfrak{Y}$ be formal schemes, $\mathscr{I}$ (resp. $\mathscr{J}$) be the defining ideal of $\mathfrak{X}$ (resp. $\mathfrak{Y}$), $f : \mathfrak{X} \to \mathfrak{Y}$ be a morphism of formal schemes.*

(i) If $f^*(\mathscr{J})\mathscr{O}_{\mathfrak{X}} \subseteq \mathscr{I}$, there exists a unique morphism

$$f_{\mathrm{red}} : (\mathfrak{X}, \mathscr{O}_{\mathfrak{X}}/\mathscr{I}) \to (\mathfrak{Y}, \mathscr{O}_{\mathfrak{Y}}/\mathscr{K})$$

of schemes such that the following diagram

$$\begin{tikzcd} (\mathfrak{X}, \mathscr{O}_{\mathfrak{X}}/\mathscr{I}) \arrow[r, "f_{\mathrm{red}}"] \arrow[d] & (\mathfrak{Y}, \mathscr{O}_{\mathfrak{Y}}/\mathscr{J}) \arrow[d] \\ (\mathfrak{X}, \mathscr{O}_X) \arrow[r, "f"] & (\mathfrak{Y}, \mathscr{O}_{\mathfrak{Y}}) \end{tikzcd} \tag{8.2.1}$$

(ii) Suppose that $\mathfrak{X} = \mathrm{Spf}(A)$, $\mathfrak{Y} = \mathrm{Spf}(B)$ are formal affine schemes, $\mathscr{I} = \mathfrak{I}^{\Delta}$, $\mathscr{K} = \mathfrak{K}^{\Delta}$, where $\mathfrak{I}$ (resp. $\mathfrak{K}$) is a defining ideal of A (reps. B), and $f = ({}^a\varphi, \tilde{\varphi})$ where $\varphi : B \to A$ is a continuous homomorphism. For $f^*(\mathscr{K})\mathscr{O}_{\mathfrak{X}} \subseteq \mathscr{K}$, it is necessary and sufficient that $\varphi(\mathfrak{K}) \subseteq \mathfrak{I}$, and f_{red} is then the morphism $({}^a\varphi', \tilde{\varphi}')$, where $\varphi' : B/\mathfrak{K} \to A/\mathfrak{I}$ is the induced homomorphism by passing to quotients.

Proof. In case (a), the hypothesis implies that the image of the ideal $f^{-1}(\mathscr{K})$ of $f^{-1}(\mathscr{O}_{\mathfrak{Y}})$ under $f^{\#} : f^{-1}(\mathscr{O}_{\mathfrak{Y}}) \to \mathscr{O}_{\mathfrak{X}}$ is contained in $\mathscr{I}$. By passing to quotients, we then deduce that $f^{\#}$ is a homomorphism

$$\omega : f^{-1}(\mathscr{O}_{\mathfrak{Y}}/\mathscr{K}) = f^{-1}(\mathscr{O}_{\mathfrak{Y}})/f^{-1}(\mathscr{K}) \to \mathscr{O}_{\mathfrak{X}}/\mathscr{I};$$

moreover, as for any $x \in \mathfrak{X}$, $f_x^{\#}$ is a local homomorphism, so is ω_x. The morphism $(f, \omega^{\flat})$ is then the unique morphism of ringed spaces satisfying the requirements.

With the assumptions of (b), the canonical correspondence between morphisms of formal affine schemes and continuous homomorphisms of ringed spaces shows that the relation $f^*(\mathscr{K})\mathscr{O}_{\mathfrak{X}} \subseteq \mathscr{I}$ implies that $f' = ({}^a\varphi', \tilde{\varphi}')$, where $\varphi' : B/\mathfrak{K} \to A/\mathfrak{I}$ is the unique homomorphism such that the diagram

$$\begin{tikzcd} B \arrow[r, "\varphi"] \arrow[d] & A \arrow[d] \\ B/\mathfrak{K} \arrow[r, "\varphi'"] & A/\mathfrak{I} \end{tikzcd} \tag{8.2.2}$$

The existence of φ' implies then that $\varphi(\mathfrak{K}) \subseteq \mathfrak{I}$. Conversely, if this condition is verified, we have a canonical homomorphism $\varphi' : B/\mathfrak{K} \to A/\mathfrak{I}$, whence the induced morphism $f' = ({}^a\varphi', \tilde{\varphi}')$ satisfies the commutativity of (8.2.2). By considering the homomorphisms ${}^a\varphi^*(\mathscr{O}_{\mathfrak{Y}}) \to \mathscr{O}_{\mathfrak{X}}$ and ${}^a\varphi'^*(\mathscr{O}_{\mathfrak{Y}}/\mathscr{K}) \to \mathscr{O}_{\mathfrak{X}}/\mathscr{I}$, we then see that $f^*(\mathscr{K})\mathscr{O}_{\mathfrak{X}} \subseteq \mathscr{I}$. □

To conclude this paragraph, we consider product of formal schemes; let $\mathfrak{S}$ be a formal scheme.

Proposition 22.8.14. *Let $\mathfrak{X} = \mathrm{Spf}(B)$, $\mathfrak{Y} = \mathrm{Spf}(C)$ be two formal affine schemes over a formal affine scheme $\mathrm{Spf}(A)$. Let $\mathfrak{Z} = \mathrm{Spf}(B\widehat{\otimes}_A C)$ and p_1, p_2 be the $\mathfrak{S}$-morphisms corresponding to the A-homomorphisms $\rho_1 : B \to B\widehat{\otimes}_A C$ and $\rho_2 : C \to B\widehat{\otimes}_A C$. Then $(\mathfrak{Z}, p_1, p_2)$ forms a product in the category of the formal $\mathfrak{S}$-schemes $\mathfrak{X}$ and $\mathfrak{Y}$.*

Proof. In view of Proposition 22.8.4, we note that for any continuous A-homomorphism $\varphi : B\widehat{\otimes}_A C \to D$, where D is an admissible ring that is a topological A-algebra, we can associate the couple $(\varphi \circ \sigma_1, \varphi \circ \sigma_2)$, so that we define a bijection

$$\mathrm{Hom}_A(B\widehat{\otimes}_A C, D) \xrightarrow{\sim} \mathrm{Hom}_A(B, D) \times \mathrm{Hom}_A(C, D)$$

which follows from the universal property of the complete tensor product. □

Proposition 22.8.15. *For any formal $\mathfrak{S}$-schemes $\mathfrak{X}, \mathfrak{Y}$, the product $\mathfrak{X} \times_{\mathfrak{S}} \mathfrak{Y}$ exists.*

Proof. The demonstration is similar as the case for usual schemes, where we replace affine schemes by formal affine schemes and use Proposition 22.8.14. □

22.8.3 Inductive limits of schemes

Let $\mathfrak{X}$ be a formal scheme, $(\mathscr{I}_\lambda)$ be a fundamental system of defining ideals of $\mathfrak{X}$; for each λ, let $f_\lambda : (\mathfrak{X}, \mathscr{O}_\mathfrak{X}/\mathscr{I}_\lambda) \to \mathfrak{X}$. For $\mathscr{I}_\mu \subseteq \mathscr{I}_\lambda$, the canoincal homomorphism $\mathscr{O}_\mathfrak{X}/\mathscr{I}_\mu \to \mathscr{O}_\mathfrak{X}/\mathscr{I}_\lambda$ defines a canonical morphism

$$f_{\mu\lambda} : (\mathfrak{X}, \mathscr{O}_\mathfrak{X}/\mathscr{I}_\lambda) \to (\mathfrak{X}, \mathscr{O}_\mathfrak{X}/\mathscr{I}_\mu)$$

of (usual) schemes such that we have $f_\lambda = f_\mu \circ f_{\mu\lambda}$. The scheme $X_\lambda = (\mathfrak{X}, \mathscr{O}_\mathfrak{X}/\mathscr{I}_\lambda)$ is the morphisms $f_{\mu\lambda}$ then constitutes an inductive system in the category of formal schemes.

Proposition 22.8.16. *The formal scheme and the morphisms f_λ constitute an inductive limit of the system $(X_\lambda, f_{\mu\lambda})$ in the cateogry of formal schemes.*

Proof. Let $\mathfrak{Y}$ be a formal scheme, and for each index λ, let

$$g_\lambda : X_\lambda \to \mathfrak{Y}$$

be a morphism such that $g_\lambda = g_\mu \circ f_{\mu\lambda}$ for $\mathscr{I}_\mu \subseteq \mathscr{I}_\lambda$. This last condition and the definition of X_λ then imply that the g_λ are equal to the same continuous map $g : \mathfrak{X} \to \mathfrak{Y}$ on the underlying space; moreover, the homomorphisms $g_\lambda^\# : g^{-1}(\mathscr{O}_\mathfrak{Y}) \to \mathscr{O}_{X_\lambda} = \mathscr{O}_\mathfrak{X}/\mathscr{I}_\lambda$ form a projective system of homomorphisms of sheaves of rings. By passing to projective limit, we then deduce a homomorphism $\omega : g^{-1}(\mathscr{O}_\mathfrak{Y}) \to \lim \mathscr{O}_\mathfrak{X}/\mathscr{I}_\lambda = \mathscr{O}_\mathfrak{X}$, and it is clear that (g, ω) is a morphism of ringed spaces such that the diagram

$$\begin{tikzcd} X_\lambda \arrow[rr, "g_\lambda"] \arrow[dr, "f_\lambda"'] & & \mathfrak{Y} \\ & \mathfrak{X} \arrow[ur, "g"'] & \end{tikzcd} \tag{8.3.1}$$

It remains to prove that g is a morphism of formal schemes; the question is local on $\mathfrak{X}$ and $\mathfrak{Y}$, we can assume that $\mathfrak{X} = \mathrm{Spf}(A)$, $\mathfrak{Y} = \mathrm{Spf}(B)$, where A, B are admissible rings, and $\mathscr{I}_\lambda = \mathfrak{I}^\Delta$ where $(\mathfrak{I}_\lambda)$ is a fundamental system of defining ideals of A (Proposition 22.8.5). As $A = \varprojlim A/\mathfrak{I}_\lambda$, the existence of the morphism of formal affine schemes g fitting into the diagram (8.3.1) then follows from the one-to-one correspondence Proposition 22.8.4 between morphisms of formal affine schemes and continuous homomorphisms of rings, and of the definition of the projective limit. But the uniqueness of g as a morphism of ringed spaces shows that it coincides with the morphism at the beginning of the demonstration. □

Proposition 22.8.17. *Let $\mathfrak{X}$ be a topological space, $(\mathscr{O}_i, u_{ji})$ a projective system of sheaves of rings over $\mathfrak{X}$, with $\mathbb{N}$ the index set. Let $\mathscr{I}_i$ be the kernel of $u_{0,i} : \mathscr{O}_i \to \mathscr{O}_0$. Suppose that*

(a) For each i, the ringed space $X_i = (\mathfrak{X}, \mathscr{O}_i)$ is a scheme.

(b) For any $x \in \mathfrak{X}$ and any $i \in \mathbb{N}$, there exists an open neighborhood U_i of x in $\mathfrak{X}$ such that the restriction $\mathscr{I}_i|_{U_i}$ is nilpotent.

(c) The homomorphisms u_{ji} are surjective.

Let $\mathcal{O}_{\mathfrak{X}}$ be the sheaf of topological rings which is the projective limit of the sheaf of discrete rings $\mathcal{O}_i$, and $u_i : \mathcal{O}_{\mathfrak{X}} \to \mathcal{O}_i$ be the canonical homomorphism. Then the topologically ringed space $(\mathfrak{X}, \mathcal{O}_{\mathfrak{X}})$ is a formal scheme; the homomorphisms u_i are surjective whose kernel $\mathcal{I}^{(i)}$ form a fundamental system of defining ideals of $\mathfrak{X}$, and $\mathcal{I}^{(0)}$ is the projective limit of the sheaf of ideals $\mathcal{I}_i$.

Proof. We first note that at each stalk, u_{ji} is a surjective hommorphism and a fortiori a local homomorphism, so $v_{ij} = (1_{\mathfrak{X}}, u_{ji}) : X_j \to X_i$ is a morphism of schemes for $i \geq j$. Suppose that each X_i is an affine scheme with ring A_i. Then there exists a homomorphism $\varphi_{ji} : A_i \to A_j$ such that $u_{ji} = \tilde{\varphi}_{ji}$, so the sheaf $\mathcal{O}_j$ is a quasi-coherent $\mathcal{O}_i$-module over X_i, associated with A_j considered as an A_i-module via φ_{ji}. For each $f \in A_i$, let $f' = \varphi_{ji}(f)$; by hypothesis, the opens $D(f)$ and $D(f')$ are identical over $\mathfrak{X}$, and the homomorphism from $\Gamma(D(f), \mathcal{O}_i) = (A_i)_f$ to $\Gamma(D(f), \mathcal{O}_j) = (A_j)_{f'}$ corresponding to u_{ji} is none other than $(A_j)_{f'}$. But if we consider A_j as an A_i-module, $(A_j)_{f'}$ is the $(A_j)_f$-module $(A_j)_f$, so we have $u_{ji} = \tilde{\varphi}_{ji}$, if φ_{ji} is considered as a homomorphism of A_i-modules. Then, as u_{ji} is surjective, so is the φ_{ji} and if $\mathfrak{j}_i$ is the kernel of φ_{ji}, the kernel of u_{ji} is the quasi-coherent $\mathcal{O}_i$-module $\widetilde{\mathfrak{J}}_{ji}$. In particular, we have $\mathcal{I}_i = \widetilde{\mathfrak{J}}_i$, where $\mathfrak{J}_i$ is the kernel of $\varphi_{0,i} : A_i \to A_0$. The hypothesis (b) implies that $\mathcal{I}_i$ is nilpotent: in fact, as $\mathfrak{X}$ is quasi-compact, we can cover X by finitely many opens U_k such that $(\mathcal{I}_i|_{U_k})^{n_k} = 0$ and by choosing n to be the largest n_k, we have $\mathcal{I}_i^n = 0$. We then conclude that each $\mathfrak{J}_i$ is nilpotent. Then the ring $A = \varprojlim A_i$ is admissible by **??**, the canonical homomorphisms $\varphi_i : A \to A_i$ is surjective and its kernel $\mathfrak{J}^{(i)}$ is equal to the projective limit of the $\mathfrak{J}_{ik}$ for $k \geq i$; the $\mathfrak{J}^{(i)}$ form a fundamental system of neighborhoods of 0 in A. The assertion of the proposition then follows from the fact that $(\mathfrak{X}, \mathcal{O}_{\mathfrak{X}}) = \mathrm{Spf}(A)$. We also note that if $f = (f_i)$ is an element in the projective limit $A = \varprojlim A_i$, the open subsets $D(f_i)$ (affine open in X_i) is then identified with $\mathfrak{D}(f)$, and the scheme induced by X_i over $\mathfrak{D}(f)$ is then identified with the affine scheme $\mathrm{Spec}((A_i)_{f_i})$.

In the general case, we remark that for any quasi-compact open U of $\mathfrak{X}$, the $\mathcal{I}_i|_U$ is nilpotent as we have seen. We claim that for any $x \in \mathfrak{X}$, there is an open neighborhood U of x in $\mathfrak{X}$ which is an affine open for any X_i. In fact, let U be an affine open for X_0, and observe that $\mathcal{O}_{X_0} = \mathcal{O}_X/\mathcal{I}_i$. As $\mathcal{I}_i|_U$ is nilpotent in view of the preceding arguments, U is also an affine open for X_i in view of Example 22.4.6. Now for any U satisfying this property, it follows from the same arguments that $(U, \mathcal{O}_{\mathfrak{X}}|_U)$ is a formal scheme such that the $\mathcal{I}^{(i)}|_U$ form a fundamental system of defining ideals and $\mathcal{I}^{(0)}|_U$ is the projective limit of $\mathcal{I}_i|_U$, whence the conclusion. □

Corollary 22.8.18. *Suppose that for $i \geq j$, the kernel of u_{ji} is $\mathcal{I}_i^{j+1}$ and that $\mathcal{I}_1/\mathcal{I}_1^2$ is of finite type over $\mathcal{O}_0 = \mathcal{O}_1/\mathcal{I}_1$. Then $\mathfrak{X}$ is an adic formal scheme, and if $\mathcal{I}^n$ is the kernel of $\mathcal{O}_{\mathfrak{X}} \to \mathcal{O}_n$, we have, putting $\mathcal{I} = \mathcal{I}^{(0)}$, $\mathcal{I}^n = \mathcal{I}^{n+1}$ and $\mathcal{I}/\mathcal{I}^2$ is isomorphic to $\mathcal{I}_1$. If moreover X_0 is locally Noetherian (resp. Noetherian), then $\mathfrak{X}$ is locally Noetherian (resp. Noetherian).*

Proof. As the underlying space of $\mathfrak{X}$ and X_0 are the same, the question is local and we can assume that each X_i is affine. In view of the relations $\mathcal{I}_{ji} = \widetilde{\mathfrak{J}}_{ji}$ (With the notations of Proposition 22.8.17), we are then reduced to the case of Proposition 11.3.42, and note that $\mathfrak{J}_1/\mathfrak{J}_1^2$ is then an A_0-module of finite type (Corollary 22.1.23). □

In particular, any locally Noetherian formal scheme $\mathfrak{X}$ is the inductive limit of a sequence (X_n) of locally Noetherian (usual) schemes verifying the conditions of Proposition 22.8.17 and Corollary 22.8.18: it suffices to consider a defining ideal $\mathfrak{J}$ of $\mathfrak{X}$ (Proposition 22.8.11) and put $X_n = (\mathfrak{X}, \mathcal{O}_{\mathfrak{X}}/\mathcal{I}^{n+1})$ (Proposition 22.8.16). More generally, we the same properties if $\mathfrak{X}$ is an

adic formal scheme having a defining ideal $\mathscr{I}$ such that $\mathscr{I}/\mathscr{I}^2$ is a finitely generated $(\mathscr{O}_{\mathfrak{X}}/\mathscr{I})$-module.

Corollary 22.8.19. *Let A be an admissible ring. For the formal affine scheme $\mathfrak{X} = \mathrm{Spf}(A)$ to be Noetherian, it is necessary and sufficient that A is adic and Noetherian.*

Proof. This condition is clearly sufficient. Conversely, suppose that $\mathfrak{X}$ is Noetherian, and let $\mathfrak{I}$ be a defining ideal of A, $\mathscr{I} = \mathfrak{I}^{\Delta}$ the defining ideal of $\mathfrak{X}$. The (usual) schemes $X_n = (\mathfrak{X}, \mathscr{O}_{\mathfrak{X}}/\mathscr{I}^{n+1})$ is then affine and Noetherian, so the ring $A_n = A/\mathscr{I}^{n+1}$ is Noetherian (Proposition 22.2.26), and we conclude that $\mathfrak{I}/\mathfrak{I}^2$ is a finitely generated $(A/\mathfrak{I})$-module. As the $\mathfrak{I}^n$ form a fundamental system of defining ideals of $\mathfrak{X}$, we have $\mathscr{O}_{\mathfrak{X}} = \varprojlim(\mathscr{O}_{\mathfrak{X}}/\mathfrak{I}^n)$ (Proposition 22.8.10). □

Remark 22.8.1. With the notations of Proposition 22.8.17, let $\mathscr{F}_i$ be an $\mathscr{O}_i$-module, and suppose that we are given for $i \geq j$ a v_{ij}-morphism $\theta_{ji} : \mathscr{F}_i \to \mathscr{F}_j$, such that $\theta_{kj} \circ \theta_{ji} = \theta_{ki}$ for $k \leq j \leq i$. As the underlying continuous map of v_{ij} is the identity, θ_{ji} is a homomorphism of sheaves of abelian groups over $\mathfrak{X}$. Moreover, if $\mathscr{F}$ is the limit of the projective system $(\mathscr{F}_i)$ of sheaves of abelian groups, the fact that θ_{ji} are v_{ij}-morphisms permits us to define over $\mathscr{F}$ an $\mathscr{O}_{\mathfrak{X}}$-module structure by passing to projective limits. With this, we say that $\mathscr{F}$ is the projective limit (for the θ_{ji}) of the system of $\mathscr{O}_i$-modules $(\mathscr{F}_i)$. In the particular case where $v_{ij}^*(\mathscr{F}_i) = \mathscr{F}_j$ and there θ_{ji} is the identity, we then say that $\mathscr{F}$ is the limit of the system $(\mathscr{F}_i)$ such that $v_{ij}^*(\mathscr{F}_i) = \mathscr{F}_j$ for $j \leq i$ (without mension of θ_{ji}).

Let $\mathfrak{X}, \mathfrak{Y}$ be two formal schemes, $\mathscr{I}$ (resp. $\mathscr{K}$) be a defining ideal of $\mathfrak{X}$ (resp. $\mathfrak{Y}$), and $f : \mathfrak{X} \to \mathfrak{Y}$ be a morphism such that $f^*(\mathscr{K})\mathscr{O}_{\mathfrak{X}} \subseteq \mathscr{I}$. We then have for each integer $n > 0$ that $f^*(\mathscr{K}^n)\mathscr{O}_{\mathfrak{X}} = (f^*(\mathscr{K})\mathscr{O}_{\mathfrak{X}}) \subseteq \mathscr{I}^n$, so Proposition 22.8.13 deduce a morphism $f_n : X_n \to Y_n$ of (usual) schemes such that the diagram

$$\begin{tikzcd} X_m \arrow[r, "f_m"] \arrow[d] & Y_m \arrow[d] \\ X_n \arrow[r, "f_n"] & Y_n \end{tikzcd} \tag{8.3.2}$$

is commutative for $m \leq n$; in other words, (f_n) is a inductive system of morphisms.

Conversely, let (X_n) (resp. (Y_n)) be a inductive system of schemes satisfying the conditions (b), (c) of Proposition 22.8.17, and let $\mathfrak{X}$ (resp. $\mathfrak{Y}$) be the inductive limits (whose existence is proved by Proposition 22.8.17). By the definition of inductive limits, any sequence (f_n) of morphisms $f_n : X_n \to Y_n$ forming an inductive limit admits an inductive limit $f : \mathfrak{X} \to \mathfrak{Y}$, which is the unique morphism of formal schemes rendering the diagram

$$\begin{tikzcd} X_n \arrow[r, "f_n"] \arrow[d] & Y_n \arrow[d] \\ \mathfrak{X} \arrow[r, "f"] & \mathfrak{Y} \end{tikzcd}$$

Proposition 22.8.20. *Let $\mathfrak{X}, \mathfrak{Y}$ be adic formal schemes, $\mathscr{I}$ (resp. $\mathscr{K}$) be a defining ideal of $\mathfrak{X}$ (resp. $\mathfrak{Y}$). The map $f \mapsto (f_n)$ is a bijection from the set of morphisms $f : \mathfrak{X} \to \mathfrak{Y}$ such that $f^*(\mathscr{K})\mathscr{O}_{\mathfrak{X}} \subseteq \mathscr{I}$ to the set of sequences (f_n) of morphisms rendering the diagram (8.3.2).*

Proof. If f is the inductive limit of this sequence, it is necessary to prove that $f^*(\mathscr{K})\mathscr{O}_{\mathfrak{X}} \subseteq \mathscr{I}$. This question is local over $\mathfrak{X}$ and $\mathfrak{Y}$, so we can assume that $\mathfrak{X} = \mathrm{Spf}(A)$, $\mathfrak{Y} = \mathrm{Spf}(B)$ are affine,

where A, B are adic, $\mathscr{I} = \mathfrak{I}^\Delta$, $\mathscr{K} = \mathfrak{K}^\Delta$, where $\mathfrak{I}$ (resp. $\mathfrak{K}$) is a defining ideal of A (resp. B). We then have $X_n = \operatorname{Spec}(A_n)$, $Y_n = \operatorname{Spec}(B_n)$, where $A_n = A/\mathfrak{I}^{n+1}$ and $B_n = B/\mathfrak{K}^{n+1}$, in view of Proposition 22.8.6. Then $f_n = ({}^a\varphi_n, \tilde{\varphi}_n)$, where $\varphi_n : B_n \to A_n$ is the homomorphism forming a projective system, so $f = ({}^a\varphi, \tilde{\varphi})$, where $\varphi = \varprojlim \varphi_n$. The commutative diagram (8.3.2) shows that $\varphi_n(\mathfrak{K}/\mathfrak{K}^{n+1}) \subseteq \mathfrak{I}/\mathfrak{I}^{n+1}$ for each n (by take $m = 0$), so by passing to limit, $\varphi(\mathfrak{K}) \subseteq \mathfrak{I}$, and this implies $f^*(\mathscr{K})\mathscr{O}_{\mathfrak{X}} \subseteq \mathscr{I}$ (Proposition 22.8.13). □

Corollary 22.8.21. *Let $\mathfrak{X}, \mathfrak{Y}$ be locally Noetherian formal schemes, $\mathscr{T}$ be the largest defining ideal of $\mathfrak{X}$.*

(i) For any defining ideal $mathscrK$ of $\mathfrak{Y}$ and any morphism $f : \mathfrak{X} \to \mathfrak{Y}$, we have $f^*(\mathscr{K})\mathscr{O}_{\mathfrak{X}} \subseteq \mathscr{T}$.

(ii) There exists a bijective correspondence between $\operatorname{Hom}(\mathfrak{X}, \mathfrak{Y})$ and the set of sequences (f_n) of morphisms rendering the diagram (8.3.2), where $X_n = (\mathfrak{X}, \mathscr{O}_{\mathfrak{X}}/\mathscr{T}^{n+1})$, $Y_n = (\mathfrak{Y}, \mathscr{O}_{\mathfrak{Y}}/\mathscr{K}^{n+1})$.

Proof. It is clear that (ii) follows from (i) and Proposition 22.8.20. To prove (i), we can assume that $\mathfrak{X} = \operatorname{Spf}(A)$, $\mathfrak{Y} = \operatorname{Spf}(B)$, A, B being Noetherian and adic, $\mathscr{T} = \mathfrak{T}^\Delta$, $\mathscr{K} = \mathfrak{K}^\Delta$, where $\mathfrak{T}$ is the largest defining ideal of A and $\mathfrak{K}$ is a defining ideal of B. Let $f = ({}^a\varphi, \tilde{\varphi})$ where $\varphi : B \to A$ is a continuous homomorphism; as the elements of $\mathfrak{K}$ are topologically nilpotent, so are those of $\varphi(\mathfrak{K})$, so $\varphi(\mathfrak{K}) \subseteq \mathfrak{T}$ since $\mathfrak{T}$ is the set of topologically nilpotent elements of A (**??**). The conclusion then follows from Proposition 22.8.13(ii). □

Corollary 22.8.22. *Let $\mathfrak{X}, \mathfrak{Y}, \mathfrak{S}$ be adic formal schemes, $f : \mathfrak{X} \to \mathfrak{S}$, $g : \mathfrak{Y} \to \mathfrak{S}$ be morphisms. Let $\mathscr{I}$ (resp. $\mathscr{K}$, $\mathscr{L}$) be a defining ideal of $\mathfrak{S}$ (resp. $\mathfrak{X}$, $\mathfrak{Y}$), and suppose that $f^*(\mathscr{I})\mathscr{O}_{\mathfrak{X}} \subseteq \mathscr{K}$, $g^*(\mathscr{I})\mathscr{O}_{\mathfrak{Y}} = \mathscr{L}$. Let $S_n = (\mathfrak{S}, \mathscr{O}_{\mathfrak{S}}/\mathscr{I}^{n+1})$, $X_n = (\mathfrak{X}, \mathscr{O}_{\mathfrak{X}}/\mathscr{K}^{n+1})$, $Y_n = (\mathfrak{Y}, \mathscr{O}_{\mathfrak{Y}}/\mathscr{L}^{n+1})$. Then there exists a bijective correspondence between $\operatorname{Hom}_{\mathfrak{S}}(\mathfrak{X}, \mathfrak{Y})$ and the set of sequences (u_n) of S_n-morphisms $u_n : X_n \to Y_n$ rendering the diagram (8.3.2).*

Proof. For any $\mathfrak{S}$-morphism $u : \mathfrak{X} \to \mathfrak{Y}$, we have $f = g \circ u$ by definition, so

$$u^*(\mathscr{L})\mathscr{O}_{\mathfrak{X}} = u^*(g^*(\mathscr{I})\mathscr{O}_{\mathfrak{Y}})\mathscr{O}_{\mathfrak{X}} = f^*(\mathscr{I})\mathscr{O}_{\mathfrak{X}} \subseteq \mathscr{K},$$

so the corollary follows from Proposition 22.8.20. □

We note that, for $m \leq n$, the datum of a morphism $f_n : X_n \to Y_n$ determines uniquely a morphism $f_m : X_m \to Y_m$ rendering the diagram (8.3.2), as we immediately see by reducing to the affine case; we have thus defined a map

$$\varphi_{mn} : \operatorname{Hom}_{S_n}(X_n, Y_n) \to \operatorname{hom}_{S_m}(X_m, Y_m)$$

and the $\operatorname{Hom}_{S_n}(X_n, Y_n)$ form for the φ_{mn} a projective system of sets; Corollary 22.8.22 then shows that there exists a canonical bijection

$$\operatorname{Hom}_{\mathfrak{S}}(\mathfrak{X}, \mathfrak{Y}) \xrightarrow{\sim} \varprojlim_n \operatorname{Hom}_{S_n}(X_n, Y_n).$$

Remark 22.8.2. Let $\mathfrak{S}$, $\mathfrak{X}, \mathfrak{Y}$ be formal schemes and $f : \mathfrak{X} \to \mathfrak{S}$, $g : \mathfrak{Y} \to \mathfrak{S}$ be morphisms. Suppose that there are fundamental system of defining ideals $(\mathscr{I}_\lambda)$, $(\mathscr{K}_\lambda)$, $(\mathscr{L}_\lambda)$ in $\mathfrak{S}, \mathfrak{X}, \mathfrak{Y}$, respectively, with the same index set I, such that $f^*(\mathscr{I}_\lambda)\mathscr{O}_{\mathfrak{X}} \subseteq \mathscr{K}_\lambda$ and $g^*(\mathscr{I}_\lambda)\mathscr{O}_{\mathfrak{Y}} \subseteq \mathscr{L}_\lambda$ for any λ. Put $S_\lambda = (\mathfrak{S}, \mathscr{O}_{\mathfrak{S}}/\mathscr{I}_\lambda)$, $X_\lambda = (\mathfrak{X}, \mathscr{O}_{\mathfrak{X}}/\mathscr{K}_\lambda)$, $Y_\lambda = (\mathfrak{Y}, \mathscr{O}_{\mathfrak{Y}}/\mathscr{L}_\lambda)$; for $\mathscr{I}_\mu \subseteq \mathscr{I}_\lambda$, $\mathscr{K}_\mu \subseteq \mathscr{K}_\lambda$, $\mathscr{L}_\mu \subseteq \mathscr{L}_\lambda$, note that S_λ (resp. X_λ, Y_λ) is a closed subscheme of S_μ (X_μ, Y_μ) with the same underlying space.

As $S_\lambda \to S_\mu$ is a monomorphism of schemes, we then see that the products $X_\lambda \times_{S_\lambda} Y_\lambda$ and $X_\lambda \times_{S_\mu} Y_\lambda$ are identical (Corollary 22.3.2), because $X_\lambda \times_{S_\mu} Y_\lambda$ is identified with a closed subscheme of $X_\mu \times_{S_\mu} Y_\mu$ with the same underlying space. Now the product is the inductive limit of the schemes $X_\lambda \times_{S_\lambda} Y_\lambda$: in fact, we see as in Proposition 22.8.16, we can assume that $\mathfrak{S}$, $\mathfrak{X}$, $\mathfrak{Y}$ are formal affine schemes. In view of Proposition 22.8.13 and our hypotheses, immediately see that our assertion follows from the definition of the completed tensor product of two algebras.

Moreover, let $\mathfrak{Z}$ be a formal $\mathfrak{S}$-scheme, $(\mathscr{M}_\lambda)$ be a fundamental system of defining ideals of $\mathfrak{Z}$ with index set I, $u : \mathfrak{Z} \to \mathfrak{X}$, $v : \mathfrak{Z} \to \mathfrak{Y}$ be morphisms such that $u^*(\mathscr{K}_\lambda)\mathscr{O}_\mathfrak{Z} \subseteq \mathscr{M}_\lambda$ and $v^*(\mathscr{L}_\lambda)\mathscr{O}_\mathfrak{Z} \subseteq \mathscr{M}_\lambda$. If we put $Z_\lambda = (\mathfrak{Z}, \mathscr{O}_\mathfrak{Z}/\mathscr{M}_\lambda)$, and if $u_\lambda : Z_\lambda \to X_\lambda$ and $v_\lambda : Z_\lambda \to Y_\lambda$ are the corresponding S_λ-morphisms, we then verify that $(u, v)_\mathfrak{S}$ is the inductive limits of the S_λ-morphisms $(u_\lambda, v_\lambda)_{S_\lambda}$.

22.8.4 Formal completion of schemes

Let X be a (usual) scheme, Z be a subscheme of X, U be an open subset of X containing Z and such that Z is a closed subscheme of U; then Z is defined by a quasi-coherent ideal $\mathscr{I}_U$ of $\mathscr{O}_U$. For any integer $n > 0$, and any quasi-coherent $\mathscr{O}_X$-module $\mathscr{F}$, $(\mathscr{F}|_U) \otimes_{\mathscr{O}_U} (\mathscr{O}_U/\mathscr{I}_U^n)$ is then a quasi-coherent $\mathscr{O}_U$-module whose support is contained in Z, which is therefore often identified with its restriction to Z. The family $((\mathscr{F}|_U) \otimes_{\mathscr{O}_U} (\mathscr{O}_U/\mathscr{I}_U^n))_{n\geq 1}$ then forms a projective system of sheaves of abelian groups. The limit $\varprojlim((\mathscr{F}|_U) \otimes_{\mathscr{O}_U} (\mathscr{O}_U/\mathscr{I}_U^n))$ is called the **completion of $\mathscr{F}$ along the subscheme X' of X**, and denoted by $\widehat{\mathscr{F}}_{/Z}$ of simply $\widehat{\mathscr{F}}$ (if there is no confusion). The sections of $\widehat{\mathscr{F}}$ over Z are called the **formal sections** of $\mathscr{F}$ along Z.

This definition is justified by the fact that it obviously does not depend on the choice open subset U, because at every point x of $U - Z$, there is a neighborhood of x in which $\mathscr{O}_U/\mathscr{I}_U^n$ is zero for any integer n. We can therefore limit ourselves to the case where Z is a closed subscheme of X, and we will always assume this henceforth. Also, it is clear that for any open subset $U \subseteq X$, we have $(\mathscr{F}|_U)_{/(U\cap Z)} = (\mathscr{F}_{/Z})|_{U\cap Z}$.

By passing to projective limits, it is clear that $(\mathscr{O}_X)_{/Z}$ is a sheaf of rings, and that $\mathscr{F}_{/Z}$ can be considered as an $(\mathscr{O}_{/Z})$-module. Furthermore, as there existss a basis for Z formed by quasi-compact opens, we can consider $(\mathscr{O}_X)_{/Z}$ (resp. $\mathscr{F}_{/Z}$) as a sheaf of topological rings (resp. topological groups) which is the projective limit of the sheaf of discrete rings (resp. groups) $\mathscr{O}_X/\mathscr{I}^n$ (resp. $\mathscr{F} \otimes_{\mathscr{O}_X} (\mathscr{O}_X/\mathscr{I}^n) = \mathscr{F}/\mathscr{I}^n\mathscr{F}$), and by passing to projective limits, $\mathscr{F}_{/Z}$ is a topological $(\mathscr{O}_X)_{/Z}$-module. Note that for any quasi-compact open subset U of X, $\Gamma(U \cap Z, (\mathscr{O}_X)_{/Z})$ (resp. $\Gamma(U \cap Z, \mathscr{F}_{/Z})$) is then the projective limit of the discrete rings (resp. groups) $\Gamma(U, \mathscr{O}_X/\mathscr{I})$ (resp. $\Gamma(U, \mathscr{F}/\mathscr{I}\mathscr{F})$).

Now let $u : \mathscr{F} \to \mathscr{G}$ be a homomorphism of $\mathscr{O}_X$-modules, we then deduce a canonical homomorphism

$$u_{\mathscr{I}^n} : \mathscr{F} \otimes_{\mathscr{O}_X} (\mathscr{O}_X/\mathscr{I}^n) \to \mathscr{G} \otimes_{\mathscr{O}_X} (\mathscr{O}_X/\mathscr{I}^n)$$

for any $n \geq 1$, and these homomorphisms form a projective system. By passing to projective limits and restricting to Z, we obtain a continuous $(\mathscr{O}_X)_{/Z}$-homomorphism $\mathscr{F}_{/Z} \to \mathscr{G}_{/Z}$, denoted by $u_{/Z}$ of $\hat{u}$, and is called the completion of u along Z. It is clear that if $v : \mathscr{G} \to \mathscr{H}$ is a second homomorphism of $\mathscr{O}_X$-modules, then $(v \circ u)_{/Z} = (v_{/Z}) \circ (u_{/Z})$, so $\mathscr{F}_{/Z}$ is a covariant additive functor on $\mathscr{F}$ from the category of quasi-coherent $\mathscr{O}_X$-modules, with values in the category of $(\mathscr{O}_X)_{/Z}$-modules.

Proposition 22.8.23. *Let Z be a closed subscheme of X defined by a quasi-coherent ideal $\mathscr{I}$ of finite type. Then the support of $(\mathscr{O}_X)_{/Z}$ is Z, the topologically ringed space $(Z, (\mathscr{O}_X)_{/Z})$ is an adic formal scheme, and $\mathscr{I}_{/Z}$ is a defining ideal of this formal scheme. If $X = \mathrm{Spec}(A)$ is an affine scheme, $\mathscr{I} = \widetilde{\mathfrak{I}}$ where $\mathfrak{I}$ is an ideal of A, and $Z = V(\mathfrak{I})$, then $(Z, (\mathscr{O}_X)_{/Z})$ is canonically identified with $\mathrm{Spf}(\widehat{A})$ where $\widehat{A}$ is the Hausdorff completion of A for the $\mathfrak{I}$-adic topology.*

Proof. We can evidently assume that $X = \mathrm{Spec}(A)$ is affine. By **??** the the Hausdorff completion $\widehat{\mathfrak{I}}$ of $\mathfrak{I}$ for the $\mathfrak{I}$-adic topology is identified with the ideal $\mathfrak{I}\widehat{A}$ of $\widehat{A}$, and that $\widehat{A}$ is a $\widehat{A}$-adic ring such that $\widehat{A}/\widehat{\mathfrak{I}}^n = A/\mathfrak{I}^n$. This last relation (for $n = 1$) proves that the open prime ideals of $\widehat{A}$ are the ideals $\hat{\mathfrak{p}} = \mathfrak{p}\widehat{\mathfrak{I}}$, where $\mathfrak{p}$ is a prime ideal of A containing $\mathfrak{I}$, whence $\mathrm{Spf}(\widehat{A}) = Z$. As $\mathscr{O}_X/\mathscr{I}^n = \widetilde{A/\mathfrak{I}^n}$, the proposition then follows from the definition of $\mathrm{Spf}(\widehat{A})$. □

The formal scheme therefore defined is called the **completion** of X along Z and is denoted by $X_{/Z}$ of $\widehat{X}$. If $Z = X$, we can put $\mathscr{I} = 0$, and we then have $X_{/Z} = X$. It is clear that if U is an open subscheme of X, then $U_{/(U\cap Z)}$ is canonically identified with the formal subscheme of $X_{/Z}$ induced over the open subset $U \cap Z$ of Z.

Corollary 22.8.24. *Under the hypothesis of Proposition 22.8.23, assume that X is locally Noetherian; then the (usual) scheme $\widehat{X}_{\mathrm{red}}$ is the unique reduced subscheme of X with underlying space Z (Proposition 22.4.40). For $\widehat{X}$ to be Noetherian, it is necessary and sufficient that $\widehat{X}_{\mathrm{red}}$ is Noetherian, and it is sufficient that X is.*

Proof. The determination of $\widehat{X}_{\mathrm{red}}$ is local (Proposition 22.8.11), so we can assume that X is affine; with the notations of Proposition 22.8.23, the ideal $\mathfrak{T}$ of topological nilpotent elements of $\widehat{A}$ is the inverse image of the nilradical of $A/\mathfrak{T}$ under the canonical map $\widehat{A} \to \widehat{A}/\widehat{\mathfrak{I}} = A/\mathfrak{I}$, so $\widehat{A}/\mathfrak{T}$ is isomorphic to $(A/\mathfrak{I})_{\mathrm{red}}$. The first assertion then follows from Proposition 22.8.11 and Proposition 22.4.40. If $\widehat{X}_{\mathrm{red}}$ is Noetherian, its underlying space Z is also Noetherian, so the $Z_n = \mathrm{Spec}(\mathscr{O}_X/\mathscr{I}^n)$ are Noetherian and so is $\widehat{X}$ (Corollary 22.8.18); the converse of this is immeidate. □

The canonical homomorphisms $\mathscr{O}_X \to \mathscr{O}_X/\mathscr{I}^n$ form a projective system and therefore gives, by passing to limit, a homomorphism of sheaves of rings $\theta : \mathscr{O}_X \to i_*((\mathscr{O}_X)_{/Z}) = \varprojlim(\mathscr{O}_X/\mathscr{I}^n)$, where we denote by $i : Z \to X$ the canonical injection. We therefore obtain a morphism

$$(i, \theta) : X_{/Z} \to X$$

of ringed spaces, called the canonical morphism. By tensoring, for any coherent $\mathscr{O}_X$-module $\mathscr{F}$, the canonical homomorphisms $\mathscr{O}_X \to \mathscr{O}_X/\mathscr{I}^n$ give the homomorphisms $\mathscr{F} \to \mathscr{F} \otimes_{\mathscr{O}_X} (\mathscr{O}_X/\mathscr{I}^n)$ of $\mathscr{O}_X$-modules which form a projective system, so define a canonical functorial homomorphism $\gamma : \mathscr{F} \to i_*(\mathscr{F}_{/Z})$ of $\mathscr{O}_X$-modules.

Example 22.8.25. Let Z, Z' be closed subschemes of X, defined by quasi-coherent ideals $\mathscr{I}, \mathscr{I}'$ of $\mathscr{O}_X$. Suppose that for any affine open U of X, the ideals $\mathscr{I}|_U, \mathscr{I}'|_U$ of $\mathscr{O}_U$ are such that there exists an integer $m > 0$ such that $(\mathscr{I}|_U)' \subseteq \mathscr{I}'|_U$ and $(\mathscr{I}'|_U)^m \subseteq \mathscr{I}|_U$. It is clear that under this condition, for any quasi-coherent $\mathscr{O}_X$-module $\mathscr{F}$, the sheaf of abelian groups $\varprojlim(\mathscr{F} \otimes_{\mathscr{O}_X} (\mathscr{O}_X/\mathscr{I}^n))$ and $\varprojlim(\mathscr{F} \otimes_{\mathscr{O}_X} (\mathscr{O}_X/\mathscr{I}'^n))$ are canonically isomorphic, which means $\mathscr{F}_{/Z} = \mathscr{F}_{/Z'}$. Note that this condition on Z and Z' implies that these two closed subschemes have the same underlying space, but is not in general equivalent to the latter property.

However, if the quasi-coherent ideals $\mathscr{I}$ and $\mathscr{I}'$ are of finite type, then it follows from Proposition 22.6.17 that if the subschemes Z and Z' have the same underlying space, the above condition is satisfied. In particular, if X is locally Noetherian, so that any quasi-coherent ideal of $\mathscr{O}_X$ is of finite type, then for any closed subset (or locally closed) Z of X, we can define $\mathscr{F}_{/Z}$ to be equal to $\mathscr{F}_{/Y}$ for any subscheme Y of X with underlying space Z.

Proposition 22.8.26. *Suppose that X is locally Noetherian and let Z be a closed subset of X, $\mathscr{F}$ be a coherent $\mathscr{O}_X$-module.*

(i) The functor $\mathscr{F}_{/Z}$ is exact on the category of coherent $\mathscr{O}_X$-modules.

(ii) The functorial homomorphism $\gamma^\sharp : i^*(\mathscr{F}) \to \mathscr{F}_{/Z}$ of $(\mathscr{O}_X)_{/Z}$-modules is an isomorphism.

Proof. To prove (i), it suffices to prove that if $0 \to \mathscr{F}' \to \mathscr{F} \to \mathscr{F}'' \to 0$ is an exact sequence of coherent $\mathscr{O}_X$-modules and U is an affine open of X with Noetherian ring $A = \Gamma(U, \mathscr{O}_X)$, the sequence

$$0 \longrightarrow \Gamma(U \cap Z, \mathscr{F}'_{/Z}) \longrightarrow \Gamma(U \cap Z, \mathscr{F}_{/Z}) \longrightarrow \Gamma(U \cap Z, \mathscr{F}''_{/Z}) \to 0$$

is exact. Then $\mathscr{F}|_U = \widetilde{M}$, $\mathscr{F}'|_U = \widetilde{M}'$, $\mathscr{F}''|_U = \widetilde{M}''$, where M, M', M'' are A-modules of finite type such that the sequence $0 \to M' \to M \to M'' \to 0$ is exact. Let $\mathscr{I}$ be a quasi-coherent ideal of $\mathscr{O}_U$ defining a subscheme of U with underlying space $U \cap Z$, and $\mathfrak{I}$ be the ideal of A such that $\mathscr{I} = \widetilde{\mathfrak{I}}$. We have (Corollary 22.1.9)

$$\Gamma(U \cap Z, \mathscr{F} \otimes_{\mathscr{O}_X} (\mathscr{O}_X/\mathscr{I}^n)) = M \otimes_A (A/\mathfrak{I}^n);$$

so by the definition of projective limit,

$$\Gamma(U \cap Z, \mathscr{F}_{/Z}) = \varprojlim (M \otimes_A (A/\mathfrak{I}^n)) = \widehat{M}$$

where $\widehat{M}$ is the Huasdorff completion of M for the $\mathfrak{I}$-adic topology, and similarly

$$\Gamma(U \cap Z, \mathscr{F}'_{/Z}) = \widehat{M}', \quad \Gamma(U \cap Z, \mathscr{F}''_{/Z}) = \widehat{M}'';$$

our assertion then follows from the fact that A is Noetherian and the functor $\widehat{M}$ on M is exact on the category of finitely generated A-modules (Theorem 11.4.17).

For assertion (i), the assertion is local, so we can assume that there exists an exact sequence $\mathscr{O}_X^m \to \mathscr{O}_X^n \to \mathscr{F} \to 0$; as $\gamma^\sharp$ is functorial, and the functors $i^*(\mathscr{F})$ and $\mathscr{F}_{/Z}$ are right exact, we have a commutative diagram

$$\begin{tikzcd}
i^*(\mathscr{O}_X^m) \arrow[r] \arrow[d, "\gamma^\sharp"] & i^*(\mathscr{O}_X^n) \arrow[r] \arrow[d, "\gamma^\sharp"] & i^*(\mathscr{F}) \arrow[r] \arrow[d, "\gamma^\sharp"] & 0 \\
(\mathscr{O}_X^m)_{/Z} \arrow[r] & (\mathscr{O}_X^n)_{/Z} \arrow[r] & \mathscr{F}_{/Z} \arrow[r] & 0
\end{tikzcd} \tag{8.4.1}$$

with exact rows. Moreover, the functors $i^*(\mathscr{F})$ and $\mathscr{F}_{/Z}$ commutes with finite sums, so we are reduced to the case where $\mathscr{F} = \mathscr{O}_X$. We then have $i^*(\mathscr{O}_X) = (\mathscr{O}_X)_{/Z} = \mathscr{O}_{\widehat{X}}$, and $\gamma^\sharp$ is a homomorphism of $\mathscr{O}_{\widehat{X}}$-modules; it then suffices to verify that $\gamma^\sharp$ maps the unit section of $\mathscr{O}_{\widehat{X}}$ over an open subset of Z to itself, which is immediate and also shows that $\gamma^\sharp$ is the identity. □

Corollary 22.8.27. *Under the hypotheses of Proposition 22.8.26, the morphism $i : \widehat{X} \to X$ is flat.*

Corollary 22.8.28. *Let X be a locally Noetherian scheme. If $\mathscr{F}$ and $\mathscr{G}$ are coherent $\mathscr{O}_X$-modules, there exists a canonical functorial isomorphism*

$$(\mathscr{F}_{/Z}) \otimes_{(\mathscr{O}_X)_{/Z}} (\mathscr{G}_{/Z}) \xrightarrow{\sim} (\mathscr{F} \otimes_{\mathscr{O}_X} \mathscr{G})_{/Z}, \tag{8.4.2}$$

$$(\mathscr{H}om_{\mathscr{O}_X}(\mathscr{F}, \mathscr{G}))_{/Z} \xrightarrow{\sim} \mathscr{H}om_{(\mathscr{O}_X)_{/Z}}(\mathscr{F}_{/Z}, \mathscr{G}_{/Z}). \tag{8.4.3}$$

Proof. This follows from the canonical identification of $i^*(\mathscr{F})$ and $\mathscr{F}_{/Z}$; the existence of the first isomorphism is clear for any morphism of ringed spaces and the second is the homomorphism of (3.4.5), which is an isomorphism for any flat morphism. □

Proposition 22.8.29. *Let X be a locally Noetherian scheme. For any coherent $\mathscr{O}_X$-module $\mathscr{F}$, the kernel of the canonical homomorphism $\Gamma(X, \mathscr{F}) \to \Gamma(Z, \mathscr{F}_{/Z})$ induced from $\mathscr{F} \to \mathscr{F}_{/Z}$ is formed by the sections which are zero on an open neighborhood of Z.*

Proof. It follows from the definition of $\mathscr{F}_{/Z}$ that the canonical image of such a section is zero. Conversely, if the image of $s \in \Gamma(X, \mathscr{F})$ is zero in $\Gamma(Z, \mathscr{F}_{/Z})$, it suffices to see that any $x \in Z$ admits an open neighborhood in X over which s is zero, and we can therefore assume that $X = \operatorname{Spec}(A)$ is affine, A is Noetherian, $Z = V(\mathfrak{I})$ where $\mathfrak{I}$ is an ideal of A, and $\mathscr{F} = \widetilde{M}$, where M is a finitely generated A-module. Then $\Gamma(Z, \mathscr{F}_{/Z})$ is the Huasdorff completion $\widehat{M}$ of M for the $\mathfrak{I}$-topology, and the homomorphism $\Gamma(X, \mathscr{F}) \to \Gamma(Z, \mathscr{F}_{/Z})$ is the canonical homomorphism $M \to \widehat{M}$. We have seen that the kernel of this homomorphism (Corollary 11.4.16) consists of elements $z \in M$ which is annihilated by an element of $1 + \mathfrak{I}$. We then have $(1 + f)s = 0$ for $f \in \mathfrak{I}$, and for any $x \in Z$ we deduce that $(1_x + f_x)s_x = 0$; as $1_x + f_x$ is invertible in $\mathscr{O}_{X,x}$ ($\mathfrak{I}_x\mathscr{O}_{X,x}$ is contained in $\mathfrak{m}_x$), we then have $s_x = 0$, which proves the assertion. □

Corollary 22.8.30. *Let X be a locally Noetherian scheme and $u : \mathscr{F} \to \mathscr{G}$ be a homomorphism of coherent $\mathscr{O}_X$-modules. For the homomorphism $u_{/Z} : \mathscr{F}_{/Z} \to \mathscr{G}_{/Z}$ to be zero, it is necessary and sufficient that u is zero on an open neighborhood of Z.*

Proof. In fact, by Proposition 22.8.26, $u_{/Z}$ is identified with $i^*(u)$, so if we consider u as a section of $\mathscr{H} = \mathscr{H}om_{\mathscr{O}_X}(\mathscr{F}, \mathscr{G})$ over X, $u_{/Z}$ is the section of $i^*(\mathscr{H}) = \mathscr{H}_{/Z}$ over Z. It then suffices to apply Proposition 22.8.29 on $\mathscr{H}$. □

Corollary 22.8.31. *Let X be a locally Noetherian sceme and $u : \mathscr{F} \to \mathscr{G}$ be a homomorphism of coherent $\mathscr{O}_X$-modules. For the homomorphism $u_{/Z} : \mathscr{F}_{/Z} \to \mathscr{G}_{/Z}$ to be a monomorphism (resp. epimorphism), it is necessary and sufficient that u is a monomorphism (resp. epimorphism) on an open neighborhood of Z.*

Proof. Let $\mathscr{P}$ and $\mathscr{N}$ be the kernel and cokernel of u, so that we have an exact sequence

$$0 \longrightarrow \mathscr{P} \longrightarrow \mathscr{F} \xrightarrow{u} \mathscr{G} \longrightarrow \mathscr{N} \longrightarrow 0$$

By applying $(-)_{/Z}$, we then get an exact sequence

$$0 \longrightarrow \mathscr{P}_{/Z} \longrightarrow \mathscr{F}_{/Z} \xrightarrow{u_{/Z}} \mathscr{G}_{/Z} \longrightarrow \mathscr{N}_{/Z} \longrightarrow 0$$

That $u_{/Z}$ is a monomorphism (resp. epimorphism) is equivalent to $\mathscr{P}_{/Z} = 0$ (resp. $\mathscr{N}_{/Z} = 0$), so we can apply Proposition 22.8.29 to get the conclusion. □

Corollary 22.8.32. *Let X be a locally Noetherian scheme and $\mathscr{F}$ be a coherent $\mathscr{O}_X$-module. For $\mathscr{F}_{/Z}$ to be locally free (resp. locally free of rank n), it is necessary and sufficient that there exists an open neighborhood U of Z such that $\mathscr{F}|_Z$ is locally free (resp. locally free of rank n).*

Proof. To say that $\mathscr{F}_{/Z}$ is locally free signifies that any point $x \in Z$ admits an open neighborhood V in X such that there exists an isomorphism $v : (\mathscr{O}_X^n)_{/Z} \xrightarrow{\sim} \mathscr{F}_{/Z}|_{V\cap Z}$. We can evidently assume that $V = X$, and then it follows from (8.4.3) that v is of the form $u_{/Z}$, where u is a homomorphism $\mathscr{O}_X^n \to \mathscr{F}$; moreover, by replacing X with an open neigbourhood of Z, we can assume, in view of Corollary 22.8.31, that u is bijective, whence the corollary. □

Chapter 23

Global properties of morphisms of schemes

23.1 Affine morphisms

23.1.1 Schemes affine over a scheme

Let S be a scheme and X be an S-scheme. If $f : X \to S$ is the structural morphism, then the direct image $f_*(\mathscr{O}_X)$ is an $\mathscr{O}_S$-algebra, which we denote by $\mathscr{A}(X)$ if there is no confusion. If U is an open subset of S, we have

$$\mathscr{A}(f^{-1}(U)) = \mathscr{A}(X)|_U.$$

Similarly, for any $\mathscr{O}_X$-module $\mathscr{F}$ (resp. any $\mathscr{O}_X$-algebra $\mathscr{B}$), we denote by $\mathscr{A}(\mathscr{F})$ (resp. $\mathscr{A}(\mathscr{B})$) the direct image $f_*(\mathscr{F})$ (resp. $f_*(\mathscr{B})$) which is an $\mathscr{A}(X)$-module (resp. $\mathscr{A}(X)$-algebra), and also an $\mathscr{O}_S$-module (resp. $\mathscr{O}_S$-algebra).

Let Y be another S-scheme with $g : Y \to S$ the structural morphism, and $h : X \to Y$ be an S-morphism. We then have a commutative diagram

$$\begin{tikzcd} X \arrow[rr, "h"] \arrow[dr, "f"'] & & Y \arrow[dl, "g"] \\ & S & \end{tikzcd}$$

By definition we have a homomorphism $h^\# : \mathscr{O}_Y \to h_*(\mathscr{O}_X)$ of sheaves of rings, and we deduce from this a homomorphism of $\mathscr{O}_S$-algebras $g_*(h^\#) : g_*(\mathscr{O}_Y) \to g_*(h_*(\mathscr{O}_X)) = f_*(\mathscr{O}_X)$, which means, a homomorphism $\mathscr{A}(Y) \to \mathscr{A}(X)$ of $\mathscr{O}_S$-algebras, and we denote it by $\mathscr{A}(h)$. If $h' : Y \to Z$ is another S-morphism, it is immediate that $\mathscr{A}(h' \circ h) = \mathscr{A}(h) \circ \mathscr{A}(h')$. Therefore we have defined a contravariant functor $\mathscr{A}(X)$ from the category of S-schemes to the category of $\mathscr{O}_S$-algebras.

Now let $\mathscr{F}$ be an $\mathscr{O}_X$-module, $\mathscr{G}$ be an $\mathscr{O}_Y$-module, and $u : \mathscr{G} \to \mathscr{F}$ be an h-morphism, wihch is a homomorphism $\mathscr{G} \to h_*(\mathscr{F})$ of $\mathscr{O}_Y$-modules. Then $g_*(u) : g_*(\mathscr{G}) \to g_*(h_*(\mathscr{F})) = f_*(\mathscr{F})$ is a homomorphism $\mathscr{A}(\mathscr{G}) \to \mathscr{A}(\mathscr{F})$ of $\mathscr{O}_S$-modules, which we denote by $\mathscr{A}(u)$. The couple $(\mathscr{A}(h), \mathscr{A}(u))$ is then a bi-homomorphism of $\mathscr{A}(Y)$-modules $\mathscr{A}(\mathscr{G})$ ot the $\mathscr{A}(X)$-module $\mathscr{A}(\mathscr{F})$. If we fix S and consider the couples $(X, \mathscr{F})$, where X is an S-scheme and $\mathscr{F}$ is an $\mathscr{O}_X$-module, we then see that $(\mathscr{A}(X), \mathscr{A}(\mathscr{F}))$ defines a contravariant functor from the category of these couples to the category of couples of $\mathscr{O}_S$-algebras and modules of this algebra.

Consider now an S-scheme X and let $f : X \to S$ be a structural morphism. We say that X is **affine over S** if there exists a covering (S_α) of S by affine opens such that, for each α, the open subscheme $f^{-1}(S_\alpha)$ of X is affine. If this is true, we also say that X is an **affine S-scheme**, or the structural morphism f is affine.

Example 23.1.1. Any closed subscheme of S is an affine S-scheme. In fact, if Y is a closed subscheme of S, then for any affine open U of S, the intersection $U \cap Y$ is a closed subscheme of U, whence affine.

Remark 23.1.1. One should note that an affine S-scheme X is not necessary an affine scheme (for example S is affine over S, but note that this is ture if S itself is affine). On the other hand, if X is an S-scheme and is affine, it is not necessarily ture that X is an affine S-scheme (we will see this later). However, if S is a separated scheme, then any affine scheme is affine over S by Proposition 22.5.33.

Proposition 23.1.2. *Any affine S-scheme is separated over S.*

Proof. Recall that separatedness is local on target (Proposition 22.5.29), and if $f^{-1}(S_\alpha)$ is affine, then the restriction of f to $f^{-1}(S_\alpha)$ is a morphism between affine schemes, so is separated. □

Proposition 23.1.3. *Let X be an affine S-scheme and $f : X \to S$ be the structural morphism. Then for any open subset $U \subseteq S$, $f^{-1}(U)$ is affine over U. In particular, if U is affine, so is $f^{-1}(U)$.*

Proof. In view of the definition, we can reduce to the case $S = \mathrm{Spec}(A)$ and $X = \mathrm{Spec}(B)$, so that f corresponds to a homomorphism $\rho : A \to B$. As the standard opens $D(g)$ with $g \in A$ form a basis for S, we only need to prove the assertion for $U = D(g)$. But recall that $f^{-1}(D(g)) = D(\rho(g))$, so our assertion follows. □

Corollary 23.1.4. *Let S be an affine scheme. Then for an S-scheme X to be affine over S, it is necessary and sufficient that X is an affine scheme.*

Proposition 23.1.5. *Let X be an affine S-scheme and $f : X \to S$ be the structural morphism. For any quasi-coherent $\mathscr{O}_X$-module $\mathscr{F}$, $f_*(\mathscr{F})$ is a quasi-coherent $\mathscr{O}_S$-module. In particular, the $\mathscr{O}_S$-algebra $\mathscr{A}(X)$ is quasi-coherent.*

Proof. The morphism f is separted by Proposition 23.1.2 and quasi-compact by Proposition 23.1.3 (since any quasi-compact open subset is a finite union of affine opens), so we can apply Proposition 22.6.54. □

Proposition 23.1.6. *Let X ba an affine S-scheme. For any S-scheme Y, the map $h \mapsto \mathscr{A}(h)$ from $\mathrm{Hom}_S(Y, X)$ to $\mathrm{Hom}_{\mathscr{O}_S\text{-}\mathbf{alg}}(\mathscr{A}(X), \mathscr{A}(Y))$ is bijective.*

Proof. Let $f : X \to S$, $g : Y \to S$ be the structural morphisms. Suppose first that $S = \mathrm{Spec}(A)$ and $X = \mathrm{Spec}(B)$ are affine; we must shows that for any homomorphism $\omega : f_*(\mathscr{O}_X) \to g_*(\mathscr{O}_Y)$ of $\mathscr{O}_S$-algebras, there exists a unique S-morphism $h : Y \to X$ such that $\mathscr{A}(h) = \omega$. By definition, for any open subset $U \subseteq S$, ω defines a homomorphism $\omega_U : \Gamma(f^{-1}(U), \mathscr{O}_X) \to \Gamma(g^{-1}(U), \mathscr{O}_Y)$ of $\Gamma(U, \mathscr{O}_S)$-algebras. In particular, for $U = S$, this gives a homomorphism $\varphi : \Gamma(X, \mathscr{O}_X) \to \Gamma(Y, \mathscr{O}_Y)$, which by Proposition 22.2.4, since X is affine, corresponds to a morphism $h : Y \to X$. To see that $\mathscr{A}(h) = \omega$, we need to prove that for any open subset $U \subseteq S$, ω_U coincides with the algebra homomorphism φ_U, which corresponds to the S-morphism $h|_{g^{-1}(U)} : g^{-1}(U) \to f^{-1}(U)$.

We may assume that $U = D(\lambda)$ where $\lambda \in A$; then, if $f : X \to S$ corresponds to the ring homomorphism $\rho : A \to B$, we have $f^{-1}(U) = D(\mu)$ where $\mu = \rho(\lambda)$, and $\Gamma(f^{-1}(U), \mathscr{O}_X)$ is the fraction ring B_μ. Now the following diagram commutes

$$\begin{tikzcd} B = \Gamma(X, \mathscr{O}_X) \arrow[r, "\varphi"] \arrow[d] & \Gamma(Y, \mathscr{O}_Y) \arrow[d] \\ B_\mu = \Gamma(f^{-1}(U), \mathscr{O}_X) \arrow[r, bend left, "\varphi_U"] \arrow[r, bend right, "\omega_U"'] & \Gamma(g^{-1}(U), \mathscr{O}_Y) \end{tikzcd}$$

By the universal property of localization, we then conclude that $\varphi_U = \omega_U$, whence the assertion in this case.

In the general case, let (S_α) be a covering of S by affine opens such that $f^{-1}(S_\alpha)$ are affine. Then any homomorphism $\omega : \mathscr{A}(X) \to \mathscr{A}(Y)$ of $\mathscr{O}_S$-algebras restricts to a family of homomorphisms

$$\omega_\alpha : \mathscr{A}(f^{-1}(S_\alpha)) \to \mathscr{A}(g^{-1}(S_\alpha))$$

of $\mathscr{O}_{S_\alpha}$-algebras, so there is a family of S_α-morphisms $h_\alpha : g^{-1}(S_\alpha) \to f^{-1}(S_\alpha)$ such that $\mathscr{A}(h_\alpha) = \omega_\alpha$. It all boils down to seeing that for any affine open U of the base $S_\alpha \cap S_\beta$, the restriction of h_α and h_β to $g^{-1}(U)$ coincide, which is immediate since these restrictions both correspond to the restriction homomorphism $\mathscr{A}(X)|_U \to \mathscr{A}(Y)|_U$ of ω. □

Corollary 23.1.7. *Let X and Y be affine S-schemes. For an S-morphism $h : Y \to X$ to be an isomorphism, it is necessary and sufficient that $\mathscr{A}(h) : \mathscr{A}(X) \to \mathscr{A}(Y)$ is an isomorphism.*

Proof. This follows from Proposition 23.1.6 and the functoriality of $\mathscr{A}(X)$. □

23.1.2 Affine S-scheme associated with an $\mathscr{O}_S$-algebra

Proposition 23.1.8. *Let S be a scheme. For any quasi-coherent $\mathscr{O}_S$-algebra $\mathscr{B}$, there exists an affine S-scheme X, defined up to S-isomorphisms, such that $\mathscr{A}(X) = \mathscr{B}$. The affine S-scheme X is said to be* ***associated with the $\mathscr{O}_S$-algebra*** *$\mathscr{B}$, and denoted by* $\mathrm{Spec}(\mathscr{B})$.

Proof. The uniqueness follows from Corollary 23.1.7, so we only need to construct the affine S-scheme X. For any affine open $U \subseteq S$, let X_U be the scheme $\mathrm{Spec}(\Gamma(U, \mathscr{B}))$; as $\Gamma(U, \mathscr{B})$ is an $\Gamma(U, \mathscr{O}_S)$-algebra, X_U is an S-scheme, and is affine over U since U and X_U are both affine. Moreover, as $\mathscr{B}$ is quasi-coherent, the $\mathscr{O}_S$-algebra $\mathscr{A}(X_U)$ is canonically idnetified with $\mathscr{B}|_U$ (Proposition 22.1.11). Let V be another affine open of S, and $X_{U,V}$ be the open subscheme of X_U over $\varphi_U^{-1}(U \cap V)$, where $\varphi_U : X_U \to S$ is the structural morphism. Then $X_{U,V}$ and $X_{V,U}$ are affine over $U \cap V$ (Proposition 23.1.3), and by definition $\mathscr{A}(X_{U,V})$ and $\mathscr{A}(X_{V,U})$ are canonically identified with $\mathscr{B}|_{U\cap V}$. There then exists (Corollary 23.1.7) a canonical S-isomorphism $\theta_{U,V} : X_{V,U} \to X_{U,V}$; furthermore, if W is a third affine open of S, and if $\theta'_{U,V}, \theta'_{V,W}, \theta'_{U,W}$ are the restrictions of $\theta_{U,V}, \theta_{V,W}, \theta_{U,W}$ over the inverse images of $U \cap V \cap W$ in X_V, X_W, X_W, then $\theta'_{U,V} \circ \theta'_{V,W} = \theta'_{U,W}$. By glueing the $X_{U,V}$, there then exists a scheme X and an affine open cover (T_U) of X such that for each U there is an isomorphism $\varphi_U : X_U \to T_U$ such that φ_U maps $\varphi_U^{-1}(U \cap V)$ to $T_U \cap T_V$ and we have $\theta_{U,V} = \varphi_U^{-1} \circ \varphi_V$. The morphism $g_U = \varphi_U \circ \varphi_U^{-1}$ then makes T_U an S-scheme, and the morphisms g_U and g_V coincide on $T_U \cap T_V$, so X is an S-scheme. It is clear by definition that X is affine over S and $\mathscr{A}(T_U) = \mathscr{B}|_U$, so $\mathscr{A}(X) = \mathscr{B}$. □

Corollary 23.1.9. *Let S be a scheme. The functor $\mathscr{A}(X)$ defines an equivalence of categories between the category of affine S-schemes and the category of quasi-coherent $\mathscr{O}_S$-algebras.*

Proof. By Proposition 23.1.6 we now that $\mathscr{A}(X)$ is fully faithful, and Proposition 23.1.8 proves that it is essentially surjective, whence the claim. □

Corollary 23.1.10. *Let S be a scheme. Then for any quasi-coherent $\mathscr{O}_S$-algebra $\mathscr{B}$, the contravariant functor*

$$Y \mapsto \mathrm{Hom}_{\mathscr{O}_S-\mathbf{alg}}(\mathscr{B}, \mathscr{A}(Y)) = \mathrm{Hom}_{\mathscr{O}_Y-\mathbf{alg}}(\mathscr{B} \otimes_{\mathscr{O}_S} \mathscr{O}_Y, \mathscr{O}_Y)$$

from the category of S-schemes to the category of sets, is represented by $\mathrm{Spec}(\mathscr{B})$.

Proof. Let $X = \mathrm{Spec}(\mathscr{B})$, then we know that $\mathscr{B} = \mathscr{A}(X)$, so the claim follows from Proposition 23.1.6. □

Corollary 23.1.11. *Let X be an affine S-scheme and $f : X \to S$ be the structural morphism. For any affine open $U \subseteq S$, the open subscheme $f^{-1}(U)$ of X is an affine scheme with ring $\Gamma(U, \mathscr{A}(X))$.*

Proof. We can suppose that X is associated with the $\mathscr{O}_S$-algebra $\mathscr{A}(X)$, the corollary then follows from the construction of X in Proposition 23.1.8. □

Example 23.1.12. Let S be the affine plane for a field K with the point 0 is doubled (Example 22.5.34). With the notations there, S is the union of two affine opens Y_1, Y_2. If f is the open immersion $Y_1 \to S$, then $f^{-1}(Y_2) = Y_1 \cap Y_2$ and we have already seen in Example 22.5.34 that this is not affine. So we obtain an example of an affine scheme not affine over a scheme S.

Remark 23.1.2. Let S be a scheme and $f : X \to S$ be a quasi-compact and quasi-separated morphism, so that $\mathscr{A}(X) = f_*(\mathscr{O}_X)$ is a quasi-coherent $\mathscr{O}_S$-algebra (Proposition 22.6.54). The affine S-scheme

$$X^0 = \mathrm{Aff}(X/S) = \mathrm{Spec}(f_*(\mathscr{O}_X)) = \mathrm{Spec}(\mathscr{A}(X))$$

is called the **affine envelope** of the S-scheme X. If $f^0 : X^0 \to S$ is the structural morphism, by Proposition 23.1.8 we then have

$$\mathscr{A}(X^0) = f^0_*(\mathscr{O}_{X^0}) = \mathscr{A}(X) = f_*(\mathscr{O}_X);$$

by Corollary 23.1.10, the identity homomorphism on $\mathscr{A}(X)$ therefore corresponds to a canonical S-morphism $\iota_X : X \to X^0$ such that f factors into

$$X \xrightarrow{\iota_X} X^0 \xrightarrow{f^0} S$$

This factorization for f is called the **Stein factorization** of f. For the morphism i_X to be an isomorphism, it is necessary and sufficient that the morphism f is affine. Moreover, for any S-scheme Y affine over S, the map $u \mapsto u \circ i_X$ is then a bijection

$$\mathrm{Hom}_S(X^0, Y) \xrightarrow{\sim} \mathrm{Hom}_S(X, Y). \tag{1.2.1}$$

which is functorial on Y: this follows from the canonical bijections

$$\mathrm{Hom}_S(X, Y) \xrightarrow{\sim} \mathrm{Hom}_{\mathscr{O}_S-\mathbf{alg}}(\mathscr{A}(Y), \mathscr{A}(X)) = \mathrm{Hom}_{\mathscr{O}_S-\mathbf{alg}}(\mathscr{A}(Y), \mathscr{A}(X^0)) \xrightarrow{\sim} \mathrm{Hom}_S(X^0, Y).$$

That is, the S-affine scheme X^0 satisfies the universal property that any S-morphism $f : X \to Y$ such that Y is affine over S must factors through X^0, or equivalently that X^0 represents the covariant functor $Y \mapsto \mathrm{Hom}_S(X, Y)$ on the category of S-affine schemes. We also deduce that for S fixed, $X \mapsto \mathrm{Aff}(X/S)$ is a covariant functor from the category of S-schemes that are quasi-compact and quasi-separted over S to the cateogry of S-schemes affine over S. Consider a commutative diagram

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "\iota_X"'] & X' \arrow[d, "\iota_{X'}"] \\ X^0 \arrow[r, "f^0"] & X'^0 \end{tikzcd}$$

The relation (1.2.1) can then be interpreted as the following: the functor $X \mapsto \mathrm{Aff}(X/S)$ is the left adjoint of the forgetful functor from the category of S-schemes affine over S to the category of S-schemes. We then conclude that this functor commutes with inductive limits, hence finite sums.

Corollary 23.1.13. *Let X be an affine S-scheme and Y be an X-scheme. For Y to be affine over S, it is necessary and sufficient that Y is affine over X.*

Proof. We can assume that S is affine, and then X is also affine by Corollary 23.1.4. Then Y is affine over S if and only if it is affine over X, if and only if it is affine, so our claim follows. □

Let X be an affine S-scheme. Then by Corollary 23.1.13, to define of a scheme Y affine over X is equivalent to giving a scheme Y affine over S and an S-morphism $g : Y \to X$. In view of Proposition 23.1.8 and Proposition 23.1.6, this is equivalent to giving a quasi-coherent $\mathscr{O}_S$-algebra $\mathscr{B}$ and a homomorphism $\mathscr{A}(X) \to \mathscr{B}$ of $\mathscr{O}_S$-algebras (which dfines over $\mathscr{B}$ an $\mathscr{A}(X)$-algebra structure). If $f : X \to S$ is the structural morphism, we then have $\mathscr{B} = f_*(g_*(\mathscr{O}_Y))$.

Corollary 23.1.14. *Let X be an affine S-scheme. For X to be of finite type over S, it is necessary and sufficient that the quasi-coherent $\mathscr{O}_X$-algebra $\mathscr{A}(X)$ is of finite type.*

Proof. By definition, we can assume that S is affine. Then X is an affine scheme, hence quasi-compact; if $S = \mathrm{Spec}(A)$, $X = \mathrm{Spec}(B)$, $\mathscr{A}(X)$ is the $\mathscr{O}_S$-algebra $\widetilde{B}$. As $\Gamma(X, \tilde{B}) = B$, the corollary follows from Corollary 22.6.39. □

Corollary 23.1.15. *Let X be an affine S-scheme. For X to be reduced, it is necessary and sufficient that the quasi-coherent $\mathscr{O}_X$-algebra is reduced.*

Proof. The question is local on S so we can assume that S is affine, and the corollary then follows from Proposition 22.4.27. □

23.1.3 Quasi-coherent sheaves over affine S-schemes

Proposition 23.1.16. *Let X be an affine S-scheme, Y be an S-scheme, and $\mathscr{F}$ (resp. $\mathscr{G}$) be a quasi-coherent $\mathscr{O}_X$-module (resp. $\mathscr{O}_Y$-module). Then the map $(h, u) \mapsto (\mathscr{A}(h), \mathscr{A}(u))$ from the set of morphisms $(Y, \mathscr{G}) \to (X, \mathscr{F})$ to the set of bi-homomorphisms $(\mathscr{A}(X), \mathscr{A}(\mathscr{F})) \to (\mathscr{A}(Y), \mathscr{A}(\mathscr{G}))$ is bijective.*

Proof. The proof is the same as in Proposition 23.1.6, by using Proposition 22.2.5. □

Corollary 23.1.17. *Under the hypotheses of Proposition 23.1.16, suppose that Y is affine over S. Then for the couple (h, u) to be an isomorphism, it is necessary and sufficient that $(\mathscr{A}(h), \mathscr{A}(u))$ is a bi-isomorphism.*

Proposition 23.1.18. *For any couple $(\mathscr{B}, \mathscr{M})$ formed by a quasi-coherent $\mathscr{O}_S$-algebra $\mathscr{B}$ and a quasi-coherent $\mathscr{B}$-module $\mathscr{M}$, there exists a couple $(X, \mathscr{F})$ formed by an affine S-scheme and a quasi-coherent $\mathscr{O}_X$-module $\mathscr{F}$ such that $\mathscr{A}(X) = \mathscr{B}$ and $\mathscr{A}(\mathscr{F}) = \mathscr{M}$, and this couple is determined up to isomorphisms.*

Proof. The uniqueness part follows from Corollary 23.1.17. The existence for the scheme X follows from Proposition 23.1.8. To define $\mathscr{M}$, we can consider an affine open $U \subseteq S$ and set $\mathscr{F}|_{f^{-1}(U)} = \widetilde{\Gamma(U, \mathscr{M})}$, where $f : X \to S$ is the structural morphism. We will use $\widetilde{\mathscr{M}}$ to denote the quasi-coherent $\mathscr{O}_X$-module $\mathscr{F}$ associated with $\mathscr{M}$. □

Corollary 23.1.19. *In the category of quasi-coherent $\mathscr{B}$-modules, $\widetilde{\mathscr{M}}$ is an additive covariant functor which commutes with inductive limits and direct sums.*

Proof. We can in fact assume that S is affine, and the claim then reduces to the functor $\widetilde{M}$ for B-modules, where $B = \Gamma(S, \mathscr{B})$. □

Corollary 23.1.20. *Under the hypotheses of Proposition 23.1.18, assume that $\mathscr{B}$ is an $\mathscr{O}_X$-algebra of finite type. Then for $\widetilde{\mathscr{M}}$ to be an $\mathscr{O}_X$-module of finite type, it is necessary and sufficient that $\mathscr{M}$ is an $\mathscr{B}$-module of finite type.*

Proof. We can reduce to the case where $S = \operatorname{Spec}(A)$ is affine. Then $\mathscr{B} = \widetilde{B}$ where B is an A-algebra of finite type, and $\mathscr{M} = \widetilde{M}$ where M is an B-module. Over the scheme X, $\mathscr{O}_X$ is associated with the ring B and $\widetilde{\mathscr{M}}$ is associated with the B-module M. For $\widetilde{\mathscr{M}}$ to be of finite type, it is necessary and sufficient that M is of finite type, whence our claim. □

Proposition 23.1.21. *Let Y be an affine S-scheme and X, X' be two schemes affine over Y. Let $\mathscr{B} = \mathscr{A}(Y)$, $\mathscr{A} = \mathscr{A}(X)$, and $\mathscr{A}' = \mathscr{A}(X')$. Then $X \times_Y X'$ is affine over Y and $\mathscr{A}(X \times_Y X')$ is identified with $\mathscr{A} \otimes_{\mathscr{B}} \mathscr{A}'$.*

Proof. In fact, $\mathscr{A} \otimes_{\mathscr{B}} \mathscr{A}'$ is a quasi-coherent $\mathscr{B}$-algebra (Proposition 22.2.22), so is a quasi-coherent $\mathscr{O}_S$-algebra. Let Z be the spectral of $\mathscr{A} \otimes_{\mathscr{B}} \mathscr{A}'$. The canonical $\mathscr{B}$-homomorphisms $\mathscr{A} \to \mathscr{A} \otimes_{\mathscr{B}} \mathscr{A}'$ and $\mathscr{A}' \to \mathscr{A} \otimes_{\mathscr{B}} \mathscr{A}'$ corresponds to Y-morphisms $p : Z \to X$ and $p' : Z \to X'$ (Proposition 23.1.6). To see that the triple (Z, p, p') is a product $X \times_Y X'$, we can reduce to the case $S = \operatorname{Spec}(C)$ is affine. But then Y, X, X' are all affine schemes with rings B, A, A', which are C-algebras such that $\mathscr{B} = \widetilde{B}$, $\mathscr{A} = \widetilde{A}$, $\mathscr{A}' = \widetilde{A}$. We then see that $\mathscr{A} \otimes_{\mathscr{B}} \mathscr{A}'$ is identified with the $\mathscr{O}_S$-algebra $\widetilde{A \otimes_B A'}$ (Corollary 22.1.9), so the ring of Z is identified with $A \otimes_B A'$, and the morphisms p, p' correspond to the canonical homomorphisms $A \to A \otimes_B A'$ and $A' \to A \otimes_B A'$. The proposition then follows from Proposition 22.3.1. □

Corollary 23.1.22. *Let $\mathscr{F}$ (resp. $\mathscr{F}'$) be a quasi-coherent $\mathscr{O}_X$-module (resp. $\mathscr{O}_{X'}$-module). Then $\mathscr{A}(\mathscr{F} \otimes_Y \mathscr{F}')$ is canonically identified with $\mathscr{A}(\mathscr{F}) \otimes_{\mathscr{A}(Y)} \mathscr{A}(\mathscr{F}')$.*

Proof. The sheaf $\mathscr{F} \otimes_Y \mathscr{F}'$ is coherent over $X \times_Y X'$ by Proposition 19.4.1. Let $g : Y \to S$, $f : X \to Y$, $f' : X' \to Y$ be the structural morphisms, so the structural morphism $h : Z \to S$ is equal to $g \circ f \circ p$ and to $g \circ f' \circ p'$. We define a canonical homomorphism

$$\mathscr{A}(\mathscr{F}) \otimes_{\mathscr{A}(Y)} \mathscr{A}(\mathscr{F}') \to \mathscr{A}$$

by the following: for any open subset $U \subseteq S$, we have canonical homomorphisms

$$\Gamma(f^{-1}(g^{-1}(U)), \mathscr{F}) \to \Gamma(h^{-1}(U), p^*(\mathscr{F})), \quad \Gamma(f'^{-1}(g^{-1}(U)), \mathscr{F}') \to \Gamma(h^{-1}(U), p'^*(\mathscr{F}')),$$

whence a canonical homomorphism

$$\begin{array}{c} \Gamma(f^{-1}(g^{-1}(U)), \mathscr{F}) \otimes_{\Gamma(g^{-1}(U), \mathscr{O}_Y)} \Gamma(f'^{-1}(g^{-1}(U)), \mathscr{F}') \\ \downarrow \\ \Gamma(h^{-1}(U), p^*(\mathscr{F})) \otimes_{\Gamma(h^{-1}(U), \mathscr{O}_Z)} \Gamma(h^{-1}(U), p'^*(\mathscr{F}')) \end{array}$$

To see this is an isomorphism of $\mathscr{A}(Z)$-modules, we can assume that S is affine, and $\mathscr{F} = \widetilde{M}$, $\mathscr{F}' = \widetilde{M}'$, where M (resp. M') is an A-module (resp. A'-module). Then $\mathscr{F} \otimes_Y \mathscr{F}'$ is identified with the sheaf over $X \times_Y X'$ associated with the $(A \otimes_B A')$-module $M \otimes_B M'$ and the corollary follows from the canonical indentification $\widetilde{M \otimes_B M'}$ with $\widetilde{M} \otimes_{\widetilde{B}} \widetilde{M}'$. □

Corollary 23.1.23. *Let X and Y be affine S-schemes and $f : Y \to X$ be an S-morphism. Let $\mathscr{F}$ be a quasi-coherent $\mathscr{O}_X$-module, then $\mathscr{A}(f^*(\mathscr{F}))$ is identified with $\mathscr{A}(\mathscr{F}) \otimes_{\mathscr{A}(X)} \mathscr{A}(Y)$.*

Proof. This is a special case of Corollary 23.1.22, by replacing X' with Y and Y with X. □

In particular, if $X = X' = Y$ (where X is an affine S-scheme), we see that if $\mathscr{F}, \mathscr{G}$ are two quasi-coherent $\mathscr{O}_X$-modules, then

$$\mathscr{A}(\mathscr{F} \otimes_{\mathscr{O}_X} \mathscr{G}) = \mathscr{A}(\mathscr{F}) \otimes_{\mathscr{A}(X)} \mathscr{A}(\mathscr{G})$$

If moreover $\mathscr{F}$ is of finite presentation, then it follows from Proposition 22.1.11 and Corollary 22.1.9 that

$$\mathscr{A}(\mathscr{H}om_{\mathscr{O}_X}(\mathscr{F}, \mathscr{G})) = \mathscr{H}om_{\mathscr{A}(X)}(\mathscr{A}(\mathscr{F}), \mathscr{A}(\mathscr{G})).$$

Proposition 23.1.24. *If X and X' are two affine S-schemes with $\mathscr{B} = \mathscr{A}(X)$ and $\mathscr{B}' = \mathscr{A}(X')$. Then the coproduct $X \amalg X'$ is affine over S with $\mathscr{A}(X \amalg X') = \mathscr{B} \times \mathscr{B}'$.*

Proof. The coproduct is affine over S since the product of two affine schemes is affine, and the second assertion also follows from this, and the fact that $\mathrm{Spec}(A) \amalg \mathrm{Spec}(A') = \mathrm{Spec}(A \times A')$ for two rings A, A'. □

Proposition 23.1.25. *Let S be a scheme, $\mathscr{B}$ be a quasi-coherent $\mathscr{O}_S$-algebra, and $X = \mathrm{Spec}(\mathscr{B})$. For any quasi-coherent ideal $\mathscr{I}$ of $\mathscr{B}$, $\widetilde{\mathscr{I}}$ is a quasi-coherent ideal of $\mathscr{O}_X$, and the closed subschem of X defined by $\widetilde{\mathscr{I}}$ is canonically isomorphic to $\mathrm{Spec}(\mathscr{B}/\mathscr{I})$.*

Proof. In fact, it follows from Example 22.4.6 that Y is affine over S, and in view of Proposition 23.1.8, we can then assume that S is affine, and the proposition follows from the corresponding result in affine schemes. □

We can also express the result of Proposition 23.1.25 by saying that if $h : \mathscr{B} \to \mathscr{B}'$ is a surjective homomorphism of quasi-coherent $\mathscr{O}_S$-algebras, then $\mathscr{A}(h) : \mathrm{Spec}(\mathscr{B}') \to \mathrm{Spec}(\mathscr{B})$ is a closed immersion.

Proposition 23.1.26. *Let S be a scheme, $\mathscr{B}$ be a quasi-coherent $\mathscr{O}_S$-algebra, and $X = \mathrm{Spec}(\mathscr{B})$. For any quasi-coherent ideal $\mathscr{K}$ of $\mathscr{O}_S$, we have (where $f : X \to S$ is the structural morphism) $f^*(\mathscr{K})\mathscr{O}_X = \widetilde{\mathscr{K}\mathscr{B}}$.*

Proof. The question is local over S, so we can assume that $S = \mathrm{Spec}(A)$ is affine, and the proposition then follows Proposition 22.1.13. □

23.1.4 Base change of affine S-schemes

Proposition 23.1.27. *Let X be an affine S-scheme. For any extension $g : S' \to S$ of base scheme, $X' = X_{(S')}$ is affine over S'.*

Proof. If $f' : X' \to S'$ is the projection, it suffices to prove that $f'^{-1}(U')$ is an affine open for any affine open subset U' of S' such that $g(U')$ is contained in an affine open U of S. We can then assume that S and S' are affine, so X is affine. But then X' is affine, so the claim follows. □

Corollary 23.1.28. *Let $f : X \to S$ be the structural morphism, $f' : X' \to S'$, $g' : X' \to X$ the projections such that the diagram*

$$\begin{tikzcd} X' \arrow[r, "g'"] \arrow[d, "f'"'] & X \arrow[d, "f"] \\ S' \arrow[r, "g"] & S \end{tikzcd}$$

is commutative. For any quasi-coherent $\mathcal{O}_X$-module $\mathcal{F}$, there exists a canonical isomorphism $u : g^*(f_*(\mathcal{F})) \to f'_*(g'^*(\mathcal{F}))$ of $\mathcal{O}_{S'}$-modules. In particular, there exists a canonical isomorphism from $\mathcal{A}(X')$ to $g^*(\mathcal{A}(X))$.

Proof. To define u, it suffices to define a homomorphism

$$v : f_*(\mathcal{F}) \to g_*(f'^*(\mathcal{F})) = f_*(g'_*(g'^*(\mathcal{F})))$$

and let u be the homomorphism corresponding to v (via the adjointness). We set $v = f_*(\rho)$, where $\rho : \mathcal{F} \to g'_*(g'^*(\mathcal{F}))$ is the canonical homomorphism. To prove that u is an isomorphism, we can assume that S and S', hence X and X', are affine. Let A, A', B, B' be the ring of X, X', S, S', then $\mathcal{F} = \widetilde{M}$ where M is an B-module. We then see that $g^*(f_*(\mathcal{F}))$ and $f'_*(g'^*(\mathcal{F}))$ are equal to the $\mathcal{O}_{S'}$-module associated with the A'-module $A' \otimes_A M$, and u is the homomorphism associated with the identity. □

Corollary 23.1.29. *For any affine S-scheme X and $s \in S$, the fiber X_s is an affine scheme.*

Proof. It suffices to apply Proposition 23.1.27 on $\mathrm{Spec}(\kappa(s)) \to S$. □

Corollary 23.1.30. *Let X be an S-scheme and S' be an affine S-scheme. Then $X' = X_{(S')}$ is affine over X. Moreover, if $f : X \to S$ is the structural homomorphism, there exists a canonical isomorphism of $\mathcal{O}_X$-algebras $\mathcal{A}(X') \cong f^*(\mathcal{A}(S'))$, and for any quasi-coherent $\mathcal{A}(S')$-module $\mathcal{M}$, a canonical bi-isomorphism $f^*(\mathcal{M}) \cong \mathcal{A}(f'^*(\widetilde{\mathcal{M}}))$, where $f' = f_{(S')}$ is the structural morphism $X' \to S'$.*

Proof. It suffices to apply Proposition 23.1.27 and Corollary 23.1.28, with the role of X and S' exchanged. □

Let S, S' be two schemes, $q : S' \to S$ be a morphism, $\mathcal{B}$ (resp. $\mathcal{B}'$) be a quasi-coherent $\mathcal{O}_S$-algebra (resp. $\mathcal{O}_{S'}$-algebra), and $u : \mathcal{B} \to \mathcal{B}'$ be a q-morphism (which means a homomorphism

$\mathscr{B} \to q_*(\mathscr{B}')$ of $\mathscr{O}_S$-algebras). If $X = \operatorname{Spec}(\mathscr{B})$ and $X' = \operatorname{Spec}(\mathscr{B}')$, we deduce a canonical morphism $v = \operatorname{Spec}(u) : X' \to X$ such that the diagram

$$\begin{tikzcd} X' \arrow[r, "v"] \arrow[d] & X \arrow[d] \\ S' \arrow[r, "q"] & S \end{tikzcd} \tag{1.4.1}$$

is commutatie. In fact, the homomorphism u corresponds to a homomorphism $u^\sharp : q^*(\mathscr{B}) \to \mathscr{B}'$ by adjointness, and there then exists a canonical S'-morphism

$$w : \operatorname{Spec}(\mathscr{B}') \to \operatorname{Spec}(q^*(\mathscr{B}))$$

such that $\mathscr{A}(w) = u^\sharp$ (Proposition 23.1.6). On the other hand, it follows from Corollary 23.1.28 that $\operatorname{Spec}(q^*(\mathscr{B}))$ is canonically identified with $X \times_S S'$; the morphism v is the defined to be the composition

$$X' \xrightarrow{w} X \times_S S' \xrightarrow{p_1} X$$

where p_1 is the projection, and the commutativity of (1.4.1) is easily verified. Let U (resp. U') be an affine open of S (resp. S') such that $q(U') \subseteq U$, $A = \Gamma(U, \mathscr{O}_S)$, $A' = \Gamma(U', \mathscr{O}_{S'})$, $B = \Gamma(U, \mathscr{B})$, $B' = \Gamma(U'\mathscr{B}')$. The restriction of u is a $(q|_{U'})$-morphism $u|_U : \mathscr{B}|_U \to \mathscr{B}'|_{U'}$ corresponding to a bi-homomorphism $B \to B'$ of algebras. If V, V' are the inverse images of U, U' in X, X', respectively, the morphism $V' \to V$, which is the restriction of v, corresponds to the preceding bi-homomorphism.

Now let $\mathscr{M}$ be a quasi-coherent $\mathscr{B}$-module. There then exists a canonical isomorphism of $\mathscr{O}_{X'}$-modules

$$v^*(\widetilde{\mathscr{M}}) \cong (q^*(\mathscr{M}) \otimes_{q^*(\mathscr{B})} \mathscr{B}')^\sim. \tag{1.4.2}$$

In fact, the canonical isomorphism of Corollary 23.1.28 provides a canonical isomorphism of $p_1^*(\widetilde{\mathscr{M}})$ with the sheaf over $\operatorname{Spec}(q^*(\mathscr{B}))$ associated with $q^*(\mathscr{B})$-module $q^*(\mathscr{M})$, and it suffices to apply Corollary 23.1.22.

Recall that we say a morphism $f : X \to Y$ is affine if X is an affine scheme over Y. The properties of affine S-schemes then translate into properties of affine morphisms.

Proposition 23.1.31 (Properties of Affine Morphisms).

(i) A closed immersion is affine.

(ii) The composition of two affine morphisms is affine.

(iii) If $f : X \to Y$ is an affine S-morphism, then $f_{(S')}$ is affine for any base change $S' \to S$.

(iv) If $f : X \to Y$ and $f' : X' \to Y'$ are two affine S-morphisms, then $f \times_S f'$ is affine.

(v) If $f : X \to Y$ and $g : Y \to Z$ are two morphisms such that $g \circ f$ is affine and g is separated, then f is affine.

(vi) If f is affine, so is f_{red}.

Proof. In view of Proposition 22.5.22, it suffices to prove (i), (ii), and (iii). Now (i) follows from Example 22.4.6, (ii) follows from Corollary 23.1.4, and (iii) follows from Proposition 23.1.27. □

Corollary 23.1.32. *If X is an affine scheme and Y is a separated scheme, any morphism $f : X \to Y$ is affine.*

Proof. This is a direct concequence of Proposition 23.1.31(v). □

Proposition 23.1.33. *Let Y be a locally Noetherian scheme and $f : X \to Y$ be a morphism of finite type. Then for f to be affine, it is necessary and sufficient that f_{red} is affine.*

Proof. It suffcies to prove that f is affine if f_{red} is affine. For this, we can assume that Y is affine and Noetherian, and show that X is affine. Now Y_{red} is affine, and X_{red} is therefore affine by hypothesis. Since X is Noetherian, the assertion follows from Corollary 22.4.34. □

23.1.5 Vector bundles

Let A be a ring and E be an A-module. Recall that the symmetric algebra over E is the A-algebra $\boldsymbol{S}(E)$ (or $\boldsymbol{S}_A(E)$) which is the quotient of $\boldsymbol{T}(E)$ by the ideal generated by elements $x \otimes y - y \otimes x$, where x, y belongs to E. The algebra $\boldsymbol{S}(E)$ is characterized by the universal property that if $\sigma : E \to \boldsymbol{S}(E)$ is the canonical map, any A-linear map $E \to B$, where B is a commutative algebra, factors through $\boldsymbol{S}(E)$ and gives a homomorphism $\boldsymbol{S}(E) \to B$ of A-algebras. We deduce from this property that for two A-modules E, F, we have

$$\boldsymbol{S}(E \oplus F) = \boldsymbol{S}(E) \otimes \boldsymbol{S}(F).$$

Moreover, $\boldsymbol{S}(E)$ is a covariant functor on E from the category of A-modules to that of commutative A-algebras. Finally, the preceding characterization shows that if $E = \varinjlim E_\lambda$, then $\boldsymbol{S}(E) = \varinjlim \boldsymbol{S}(E_\lambda)$. By abuse of language, a product $\sigma(x_1) \cdots \sigma(x_n)$, where $x_i \in E$, is usually written as $x_1 \cdots x_n$. The algebra $\boldsymbol{S}(E)$ is graded, where $\boldsymbol{S}_n(E)$ is the set of linear combinations of products of n elements of E. In particular, the algebra $\boldsymbol{S}(A)$ is canonically isomorphic to the polynomial algebra $A[T]$ over A, and the algebra $\boldsymbol{S}(A^n)$ is the polynomial algebra $A[T_1, \dots, T_n]$ over A. More particularly, if E is free of rank 1, then $\boldsymbol{S}_n(E)$ is isomorphic to the tensor algebra $\boldsymbol{T}(E) = \bigoplus_{n \geq 0} E^{\otimes n}$.

Let $\varphi : A \to B$ be a ring homomorphism. If F is an B-module, the canonical map $F \to \boldsymbol{S}(F)$ then gives a canonical map $F_{(\varphi)} \to \boldsymbol{S}(F)_{(\varphi)}$, which factors into $F_{(\varphi)} \to \boldsymbol{S}(F_{(\varphi)}) \to \boldsymbol{S}(F)_{(\varphi)}$. The canonical homomorphism $\boldsymbol{S}(F_{(\varphi)}) \to \boldsymbol{S}(F)_{(\varphi)}$ is surjective, but not necessarily bijective. If E is an A-module, any bi-homomorphism $E \to F$ (which is an A-homomorphism $E \to F_{(\varphi)}$) then gives an A-homomorphism $\boldsymbol{S}(E) \to \boldsymbol{S}(F_{(\varphi)}) \to \boldsymbol{S}(F)_{(\varphi)}$ of algebras, which is a bi-homomorphism $\boldsymbol{S}(E) \to \boldsymbol{S}(F)$. Also, for any A-module E, $\boldsymbol{S}(E \otimes_A B)$ is canonically identified with the algebra $\boldsymbol{S}(E) \otimes_A B$, which follows from the universal property of $\boldsymbol{S}(E)$.

Let R be a multiplicative subset of A. Then apply the previous arguments for the ring $B = R^{-1}A$, and recall that $R^{-1}E = E \otimes_A R^{-1}A$, we see that $\boldsymbol{S}(R^{-1}E) = R^{-1}\boldsymbol{S}(E)$. Moreover, if $R' \supseteq R$ is another multiplicative subset of A, the diagram

$$\begin{tikzcd} R^{-1}E \arrow[r] \arrow[d] & R'^{-1}E \arrow[d] \\ \boldsymbol{S}(R^{-1}E) \arrow[r] & \boldsymbol{S}(R'^{-1}E) \end{tikzcd}$$

is commutative.

Now let $(S, \mathscr{A})$ be a ringed space and $\mathscr{E}$ be an $\mathscr{A}$-module over S. If for each open subset $U \subseteq S$, we associate the $\Gamma(U, \mathscr{A})$-module $\boldsymbol{S}(\Gamma(U, \mathscr{E}))$, we then define a presheaf of algebras. The associated sheaf is called the **symmetric $\mathscr{A}$-algebra** of the $\mathscr{A}$-module $\mathscr{E}$ and denoted by $\boldsymbol{S}(\mathscr{E})$. It follows immediately that $\boldsymbol{S}(\mathscr{E})$ satisfies the following universal property: any homomorphism $\mathscr{E} \to \mathscr{B}$ of $\mathscr{A}$-modules, where $\mathscr{B}$ is an $\mathscr{A}$-algebra, factors through $\boldsymbol{S}(\mathscr{E})$ to give a homomorphism $\boldsymbol{S}(\mathscr{E}) \to \mathscr{B}$ of $\mathscr{A}$-algebras. In particular, any homomorphism $u : \mathscr{E} \to \mathscr{F}$ of $\mathscr{A}$-modules defines a homomorphism $\boldsymbol{S}(u) : \boldsymbol{S}(\mathscr{E}) \to \boldsymbol{S}(\mathscr{F})$ of $\mathscr{A}$-algebras and $\boldsymbol{S}(\mathscr{E})$ is a covariant functor $\mathscr{E}$.

Now since the functor $\boldsymbol{S}$ commutes with inductive limits, we have $\boldsymbol{S}(\mathscr{E})_s = \boldsymbol{S}(\mathscr{E}_s)$ for any point $s \in S$. If $\mathscr{E}, \mathscr{F}$ are two $\mathscr{A}$-module, $\boldsymbol{S}(\mathscr{E} \oplus \mathscr{F})$ is canonically identified with $\boldsymbol{S}(\mathscr{E}) \otimes_{\mathscr{A}} \boldsymbol{S}(\mathscr{F})$, as we can check this for the corresponding presheaves.

We see that $\boldsymbol{S}(\mathscr{E})$ is a graded $\mathscr{A}$-algebra, and $\boldsymbol{S}_n(\mathscr{E})$ is the $\mathscr{A}$-module associated with the presheaf $U \mapsto \boldsymbol{S}_n(\Gamma(U, \mathscr{E}))$. In particular, if $\mathscr{E} = \mathscr{A}$, then $\boldsymbol{S}(\mathscr{A})$ is identified with $\mathscr{A}[T] = \mathscr{A} \otimes_{\mathbb{Z}} \mathbb{Z}[T]$, and if $\mathscr{E}$ is an invertible sheaf, then $\boldsymbol{S}(\mathscr{E})$ is isomorphic to the tensor algebra $\boldsymbol{T}(\mathscr{E}) = \bigoplus_{n \geq 0} \mathscr{E}^{\otimes n}$.

Proposition 23.1.34. *Let $f : (S, \mathscr{A}) \to (T, \mathscr{B})$ be a morphism of ringed spaces. If $\mathscr{F}$ is an $\mathscr{B}$-module, then $\boldsymbol{S}(f^*(\mathscr{F}))$ is canonically identified with $f^*(\boldsymbol{S}(\mathscr{F}))$*

Proof. To see this, we may make use the universal property of $\boldsymbol{S}$. By definition, $\boldsymbol{S}(f^*(\mathscr{F}))$ is defined to be the unique $\mathscr{A}$-algebra satisfying the following equality

$$\mathrm{Hom}_{\mathscr{A}-\mathbf{alg}}(\boldsymbol{S}(f^*(\mathscr{F})), \mathscr{C}) = \mathrm{Hom}_{\mathscr{A}}(f^*(\mathscr{F}), \mathscr{C})$$

for any $\mathscr{A}$-algebra $\mathscr{C}$. On the other hand, by the adjointness property of f_* and f^*, we have

$$\begin{aligned}\mathrm{Hom}_{\mathscr{A}-\mathbf{alg}}(f^*(\boldsymbol{S}(\mathscr{F})), \mathscr{C}) &= \mathrm{Hom}_{\mathscr{B}-\mathbf{alg}}(\boldsymbol{S}(\mathscr{F}), f_*(\mathscr{C})) \\ &= \mathrm{Hom}_{\mathscr{B}}(\mathscr{F}, f_*(\mathscr{C})) = \mathrm{Hom}_{\mathscr{A}}(f^*(\mathscr{F}), \mathscr{C}).\end{aligned}$$

This implies the desired isomorphism. □

Proposition 23.1.35. *Let A be a ring, $S = \mathrm{Spec}(A)$ be the spectrum, and $\mathscr{E} = \widetilde{M}$ be the $\mathscr{O}_S$-module assocaited with an A-module M. Then the $\mathscr{O}_S$-algebra $\boldsymbol{S}(\mathscr{E})$ is associated with the A-algebra $\boldsymbol{S}(M)$.*

Proof. In fact, for any $f \in A$, $\boldsymbol{S}(M_f) = \boldsymbol{S}(M)_f$, so the proposition follows from the definition of $\widetilde{\boldsymbol{S}(M)}$. □

Corollary 23.1.36. *If S is a scheme and $\mathscr{E}$ is a quasi-coherent $\mathscr{O}_S$-module. Then the $\mathscr{O}_S$-algebra $\boldsymbol{S}(\mathscr{E})$ is quasi-coherent. If moreover $\mathscr{E}$ is of finite type (resp. of finite presentation), then each $\mathscr{O}_S$-module $\boldsymbol{S}_n(\mathscr{E})$ is of finite type (resp. finite presentation) and the $\mathscr{O}_S$-algebra $\boldsymbol{S}(\mathscr{E})$ is of finite type (resp. of finite presentation).*

Proof. The first assertion is immediate by Proposition 23.1.35. The second one follows from the fact that, if E is a finitely generated A-module, $\boldsymbol{S}_n(E)$ is also finitely generated. For the last assertion, we are reduced to the case $S = \mathrm{Spec}(A)$ and $\mathscr{E} = \widetilde{E}$ where E is an A-module of finite type (resp. of finite presentation). Now if we have an exact sequence

$$0 \longrightarrow N \longrightarrow A^n \longrightarrow E \longrightarrow 0$$

then we deduce an exact sequence

$$0 \longrightarrow \mathfrak{I} \longrightarrow \boldsymbol{S}(A^n) \longrightarrow \boldsymbol{S}(E) \longrightarrow 0$$

where $\mathfrak{I}$ is the ideal of $\boldsymbol{S}(A^n)$ generated by $N \subseteq \boldsymbol{S}_1(A^n)$, whence our conclusion. □

Let S be a scheme and $\mathscr{E}$ be a quasi-coherent $\mathscr{O}_S$-module. For any S-scheme T, with structural morphism $f : T \to S$, let $\mathscr{E}_{(T)} = f^*(\mathscr{E})$, which is a quasi-coherent $\mathscr{O}_T$-module. The map

$$T \mapsto F_{\mathscr{E}}(T) = \mathrm{Hom}_{\mathscr{O}_T}(\mathscr{E}_{(T)}, \mathscr{O}_T) = \Gamma(T, \mathscr{E}^*_{(T)})$$

then defines a contravariant functor from the category of S-schemes to that of sets if for any S-morphism $g : T' \to T$ we define $F_{\mathscr{E}}(g) : F_{\mathscr{E}}(T) \to F_{\mathscr{E}}(T')$ to be the map $g^* : u \mapsto g^*(u)$ (note that the structural morphism $T' \to S$ is $f \circ g$ and we have $\mathscr{E}_{(T')} = g^*(\mathscr{E}_{(T)})$ and $\mathscr{O}_{T'} = g^*(\mathscr{O}_T)$).

Proposition 23.1.37. *For any quasi-coherent $\mathscr{O}_S$-module $\mathscr{E}$, the contravariant functor $F_{\mathscr{E}}$ is represented by the couple formed by the affine S-scheme $\mathbb{V}(\mathscr{E}) = \mathrm{Spec}(\boldsymbol{S}(\mathscr{E}))$. The S-scheme $\mathbb{V}(\mathscr{E})$ is called the* ***vector bundle over S defined by*** *$\mathscr{E}$.*

Proof. This follows from the following canonical isomorphisms for any S-scheme T:

$$\begin{aligned}\mathrm{Hom}_S(T, \mathbb{V}(\mathscr{E})) &= \mathrm{Hom}_{\mathscr{O}_S\text{-}\mathbf{alg}}(\boldsymbol{S}(\mathscr{E}), \mathscr{A}(T)) = \mathrm{Hom}_{\mathscr{O}_S}(\mathscr{E}, f_*(\mathscr{O}_T)) \\ &= \mathrm{Hom}_{\mathscr{O}_T}(f^*(\mathscr{E}), \mathscr{O}_T) = \mathrm{Hom}_{\mathscr{O}_T}(\mathscr{E}_{(T)}, \mathscr{O}_T).\end{aligned}$$ □

The canonical $\boldsymbol{S}(\mathscr{E})$-homomorphism $\mathscr{E} \otimes_{\mathscr{O}_S} \boldsymbol{S}(\mathscr{E}) \to \boldsymbol{S}(\mathscr{E})$ induced by Proposition 23.1.6 an $\mathscr{O}_{\mathbb{V}(\mathscr{E})}$-homomorphism $\mathscr{E}_{(\mathbb{V}(\mathscr{E}))} \to \mathscr{O}_{\mathbb{V}(\mathscr{E})}$, which is a section over $\mathbb{V}(\mathscr{E})$ of dual sheaf $\mathscr{E}^*_{(\mathbb{V}(\mathscr{E}))}$ of $\mathscr{E}_{(V(\mathscr{E}))}$, called the **universal section** of this dual. If $U = \mathrm{Spec}(A)$ is an affine open of S, its inverse image in $\mathbb{V}(\mathscr{E})$ is identified with $\mathrm{Spec}(\boldsymbol{S}(M))$, if $\mathscr{E}|_U = \widetilde{M}$ where M is an A-module. Over the scheme $\mathrm{Spec}(\boldsymbol{S}(M))$, the universal section is identified with the homomorphism $m \otimes p \mapsto mp$ of $M \otimes_A \boldsymbol{S}(M)$ to $\boldsymbol{S}(M)$, where M is identified with the subset $\boldsymbol{S}_1(M)$ of $\boldsymbol{S}(M)$.

Consider in particular an open subset U of S. Then the S-morphisms $U \to \mathbb{V}(\mathscr{E})$ are the U-sections of the U-scheme induced by $\mathbb{V}(\mathscr{E})$ over $p^{-1}(U)$ (where $p : \mathbb{V}(\mathscr{E}) \to S$ is the structural morphism). By the definition of $\mathbb{V}(\mathscr{E})$, these U-sections correspond bijectively to sections of the dual $\mathscr{E}^*$ of $\mathscr{E}$ over U. The functorial of $\mathbb{V}$ shows that this interpretation is compatible with the restriction to an open subset $U' \subseteq U$, so we can say that the dual $\mathscr{E}^*$ of $\mathscr{E}$ is canonically identified with the sheaf of germs of S-sections of $\mathbb{V}(\mathscr{E})$. In particular, if $T = S$, the zero homomorphism $\mathscr{E} \to \mathscr{O}_S$ corresponds to an S-section of $\mathbb{V}(\mathscr{E})$, called the **zero section**.

If now we choose T to be the spectrum $\{\xi\}$ of a field K, the structural morphism $f : T \to S$ corresponds to a monomorphism $\kappa(s) \to K$, where $s = f(\xi)$ (Corollary 22.2.15), and the S-morphisms $\{\xi\} \to \mathbb{V}(\mathscr{E})$ are none other than points of $\mathbb{V}(\mathscr{E})$ with values in the extension K of $\kappa(s)$, which all locate at some points of $p^{-1}(s)$. The set of these points, which is called the **rational fiber** of $\mathbb{V}(\mathscr{E})$ over K lying over the point s, is then identified (by the definition of $\mathbb{V}(\mathscr{E})$) with the dual of the K-vector space $\mathscr{E}_s \otimes_{\mathscr{O}_{S,s}} K = \mathscr{E}^s \otimes_{\kappa(s)} K$ where we set $\mathscr{E}^s = \mathscr{E}_s/\mathfrak{m}_s\mathscr{E}_s$. If $\mathscr{E}^s$ and K are of finite rank over $\kappa(s)$, this dual is identified with $(\mathscr{E}^s)^* \otimes_{\kappa(s)} K$, where $(\mathscr{E}^s)^*$ is the dual space of the $\kappa(s)$-vector space $\mathscr{E}^s$.

These properties justify the terminology of "vector bundle" introduced above, but note that the definition we obtained is dual to the classical definition, since one would expect to obtain

the space $\mathscr{E}^s \otimes_{\kappa(s)} K$ for the fiber of $\mathbb{V}(\mathscr{E})$, rather than its dual. This distinction is imposed for the need of defining $\mathbb{V}(\mathscr{E})$ for any quasi-coherent $\mathscr{O}_S$-module $\mathscr{E}$, not only for locally free $\mathscr{O}_S$-modules of finite rank. We can indeed show that the functor $T \mapsto \Gamma(T, \mathscr{E}_{(T)})$ is only representable if $\mathscr{E}$ is locally free of finite rank.

Proposition 23.1.38. *Let S be a scheme.*

(i) $\mathbb{V}$ is a contravariant functor on $\mathscr{E}$ from the category of quasi-coherent $\mathscr{O}_S$-modules to the category of affine S-schemes.

(ii) If $\mathscr{E}$ is of finite type (resp. of finite presentation), $\mathbb{V}(\mathscr{E})$ is of finite type (resp. of finite presentation) over S.

(iii) If $\mathscr{E}$ and $\mathscr{F}$ are two quasi-coherent $\mathscr{O}_S$-modules, $\mathbb{V}(\mathscr{E} \oplus \mathscr{F})$ is canonically identified with $\mathbb{V}(\mathscr{E}) \times_S \mathbb{V}(\mathscr{F})$.

(iv) Let $g : S' \to S$ be a morphism. For any quasi-coherent $\mathscr{O}_S$-module $\mathscr{E}$, $\mathbb{V}(g^*(\mathscr{E}))$ is canonically identified with $\mathbb{V}(\mathscr{E})_{(S')} = \mathbb{V}(\mathscr{E}) \times_S S'$.

(v) A surjective homomorphism $\mathscr{E} \to \mathscr{F}$ of quasi-coherent $\mathscr{O}_S$-modules corresponds to a closed immersion $\mathbb{V}(\mathscr{F}) \to \mathbb{V}(\mathscr{E})$.

Proof. Assertion (i) follows from Proposition 23.1.6, since for any homomorphism $\mathscr{E} \to \mathscr{F}$ of $\mathscr{O}_S$-modules we have a homomorphism $\boldsymbol{S}(\mathscr{E}) \to \boldsymbol{S}(\mathscr{F})$ of $\mathscr{O}_S$-algebras. Assertion (ii) follows immediately from Corollary 23.1.20 and Corollary 23.1.36. To prove (iii), it suffices to recall the canonical isomorphism $\boldsymbol{S}(\mathscr{E} \oplus \mathscr{F}) \cong \boldsymbol{S}(\mathscr{E}) \otimes_{\mathscr{O}_S} \boldsymbol{S}(\mathscr{F})$ and apply Proposition 23.1.21. Similarly, to prove (iv), it suffices to remark that if the homomorphism $\mathscr{E} \to \mathscr{F}$ is surjective, so is the corresponding homomorphism $\boldsymbol{S}(\mathscr{E}) \to \boldsymbol{S}(\mathscr{F})$ of $\mathscr{O}_S$-algebras, and apply Proposition 23.1.25. □

Example 23.1.39. Consider in particular $\mathscr{E} = \mathscr{O}_S$. The scheme $\mathbb{V}(\mathscr{O}_S)$ is the specturm of the $\mathscr{O}_S$-algebra $\boldsymbol{S}(\mathscr{O}_S)$, which is identified with $\mathscr{O}_S[T] = \mathscr{O}_S \otimes_{\mathbb{Z}} \mathbb{Z}[T]$. This is evident if $S = \operatorname{Spec}(\mathbb{Z})$, in view of Proposition 23.1.35, and we pass from this to the general case by considering the structural morphism $S \to \operatorname{Spec}(\mathbb{Z})$ and using Proposition 23.1.38(iv). Because of this result, we again set $\mathbb{V}(\mathscr{O}_S) = S[T]$, and we obtain the identification of the sheaf of germs of S-sections of $S[T]$ over $\mathscr{O}_S$ as a particular case.

For any S-scheme X, by the definition of $\mathbb{V}(\mathscr{O}_S)$, the set $\operatorname{Hom}_S(X, S[T])$ is canonically identified with $\operatorname{Hom}_{\mathscr{O}_S}(\mathscr{O}_S, \mathscr{A}(X))$, which is canonically isomorphic to $\Gamma(S, \mathscr{A}(X))$ and therefore has a ring structure. Moreover, any S-morphism $h : X \to Y$ corresponds to a homomorphism $\Gamma(\mathscr{A}(h)) : \Gamma(S, \mathscr{A}(Y)) \to \Gamma(S, \mathscr{A}(X))$, so we obtain a contravariant functor $\operatorname{Hom}_S(X, S[T])$ from the category of S-schemes to the cateogry of rings. On the other hand, $\operatorname{Hom}_S(X, \mathbb{V}(\mathscr{E}))$ is identified similarly with $\operatorname{Hom}_{\mathscr{O}_S}(\mathscr{E}, \mathscr{A}(X))$ (where $\mathscr{A}(X)$ is considered as an $\mathscr{O}_S$-module); we can then endow this set a $\operatorname{Hom}_S(X, S[T])$-module structure, and the couple

$$(\operatorname{Hom}_S(X, S[T]), \operatorname{Hom}_S(X, \mathbb{V}(\mathscr{E})))$$

is a contravariant functor on X with values in the category of couples (A, M) formed by a ring A and an A-module M, with morphisms being the bi-homomorphisms. In view of this, we say that $S[T]$ is the **S-scheme of ring** and $\mathbb{V}(\mathscr{E})$ is the **S-scheme of module** over the S-scheme of ring $S[T]$.

23.2 Homogeneous specturm of graded algebras

Let S be a graded ring and S_+ be the irrelevant ideal. We say a subset $\mathfrak{I}$ of S_+ is an **ideal of** S_+ if it is an ideal of S, and it is called a **graded prime ideal of** S_+ if it is the intersection with S_+ of a graded prime ideal of S not containing S_+ (in particular $\mathfrak{I} \neq S_+$, and this graded prime ideal of S is unique by Proposition 11.1.46). If $\mathfrak{I}$ is an ideal of S_+, the radical of $\mathfrak{I}$ in S_+, denoted by $\mathfrak{r}_+(\mathfrak{I})$, is the set of elements of S_+ which have some power contained in $\mathfrak{I}$, or equivalently, $\mathfrak{r}_+(\mathfrak{I}) = \sqrt{\mathfrak{I}} \cap S_+$. In particularm the radical of 0 in S_+ is called the **nilradical** of S_+ and denoted by $\mathfrak{n}_+$: this is the subset of nilpotent elements of S_+. If $\mathfrak{I}$ is a graded ideal of S_+, its radical $\mathfrak{r}_+(\mathfrak{I})$ is also graded: by passing to $S/\mathfrak{I}$, we may assume that $\mathfrak{I} = 0$, and note that if $x = x_h + x_{h+1} + \cdots + x_k$ is nilpotent, then so is each $x_i \in S_i$; we can suppose that $x_k = 0$ and the top degree component of x^n is then x_k^n, so x_k is nilpotent, and we then preceed by induction on k. We say the graded ring S is essentially reduced if $\mathfrak{n}_+ = 0$, which means S_+ contains no nonzero nilpotent elements.

We note that in a graded ring S, if an element x is a zero divisor, so is its homogeneous component of top degree. We then say that the ring S is **essentially integral** if the ring S_+ (with the unit element) does not contain nonzero zero divisors; it suffices for this that a nonzero homogeneous element in S_+ is not divisor of 0 in this ring. It is clear that if $\mathfrak{p}$ is a graded prime ideal of S_+, $S/\mathfrak{p}$ is essentially integral. Let S be an essentially integral graded ring, and let $x_0 \in S_0$. It there exists a homogeneous element $f \neq 0$ in S_+ such that $x_0 f = 0$, we then have $x_0 S_+ = 0$, because $(x_0 g)f = (x_0 f)g = 0$ for any $g \in S_+$, and the hypothesis on S implies that $x_0 g = 0$. Therfore, for that S is integral, it is necessary and sufficient that S_0 is integral and the annihilator of S_+ in S_0 reduces to zero.

23.2.1 Localization of graded rings

Let S be a graded ring with positive degrees, f be a homogeneous element of S of degree $d > 0$. Then the fraction ring S_f is graded, where $(S_f)_n$ is the set of elements x/f^k, where $x \in S_{n+kd}$ with $k \geq 0$ (note that n can be an arbitrary integer). We denote by $S_{(f)}$ the subring $(S_f)_0$ of S_f formed by elements of degree 0.

If $f \in S_d$, the monomials $(f/1)^h$ in S_f (where h is an integer) form a lineraly independent system over the ring $S_{(f)}$, and the set of their linear combinations over $S_{(f)}$ is exactly the ring $(S^{(d)})_f$ (recall that $S^{(d)}$ is the direct sum of S_{nd}), and then we get an isomorphism

$$(S^{(d)})_f \cong S_{(f)}[T, T^{-1}] = S_{(f)} \otimes_{\mathbb{Z}} \mathbb{Z}[T, T^{-1}] \tag{2.1.1}$$

(where T is an indeterminate). In fact, if we have a relatin

$$\sum_{h=-a}^{a} z_h (f/1)^h = 0$$

where $z_h = x_h/f^m \in S_{(f)}$, then there exists an integer $k > -a$ such that

$$\sum_{h=-a}^{b} f^{h+k} x_h = 0,$$

and as the degrees of these terms are distinct, we have $f^{h+k}x_h = 0$ for all h, so $z_h = 0$ for all h. Similarly, if M is a graded S-module, the localization M_f is a graded S_f-module with $(M_f)_n$ being the set of elements z/f^k where $z \in M_{n+kd}$. We denote by $M_{(f)}$ the set of elements of degree 0 in M_f. It is immediate that $M_{(f)}$ is an $S_{(f)}$-module and we have $(M^{(d)})_f = M_{(f)} \otimes_{S_{(f)}} (S^{(d)})_f$.

Lemma 23.2.1. *Let $f \in S_d$ and $g \in S_e$ be two homogeneous elements of S with positive degrees. Then there exists a canonical isomorphism*

$$S_{(fg)} \cong (S_{(f)})_{g^d/f^e}.$$

If we identify these two rings, then for any S-module M, we have a canonical isomorphism

$$M_{(fg)} \cong (M_{(f)})_{g^d/f^e}.$$

Proof. Note that (fg) divides $f^e g^d$ and $f^e g^d$ divides $(fg)^{de}$, so the rings S_{fg} and $S_{f^e g^d}$ are canonically identified. On the other hand, $S_{f^e g^d}$ is also identified with $(S_{f^e})_{g^d/1}$, and as $f^e/1$ is invertible in S_{f^e}, $s_{f^e g^d}$ is also identified with $(S_{f^e})_{g^d/f^e}$. Now the element g^e/f^e is of degree zero in S_{f^e}, so we can conclude that the subring of $(S_{f^e})_{g^d/f^e}$ formed by elements of degree zero is $(S_{(f^e)})_{g^d/f^e}$, and as we have $S_{(f^e)} = S_{(f)}$, we see the assertion follows. □

With the hypotheses of Lemma 23.2.1, it is clear that the canonical homomorphism $S_f \to S_{fg}$, which maps x/f^k to $xg^k/(fg)^k$, is of degree 0 so restricts to a canonical homomorphism $S_{(f)} \to S_{(fg)}$, such that the diagram

$$\begin{tikzcd} & S_{(f)} \arrow[dl] \arrow[dr] & \\ S_{(fg)} \arrow[rr, "\sim"] & & (S_{(f)})_{(g^d/f^e)} \end{tikzcd}$$

is commutative. We define similarly a canonical homomorphism $M_{(f)} \to M_{(fg)}$.

Lemma 23.2.2. *If f, g are two homogeneous elements of S_+, the ring $S_{(fg)}$ is generated by the union of the canonical images of $S_{(f)}$ and $S_{(g)}$.*

Proof. In view of Lemma 23.2.1, it suffices to show that $1/(g^d/f^e) = f^{d+e}/(fg)^d$ belongs to the canonical image of $S_{(g)}$ in $S_{(fg)}$, which is evident from the definition. □

Proposition 23.2.3. *Let $f \in S_d$ be a homogeneous element of positive degree. Then there exists a canonical isomorphism $S_{(f)} \cong S^{(d)}/(f-1)S^{(d)}$ of rings. If we identify these two rings, then for any S-module M, there exists a canonical isomorphism of modules $M_{(f)} \cong M^{(d)}/(f-1)M^{(d)}$*

Proof. The first isomorphism is defined by sending the element x/f^n, where $x \in S_{nd}$, to the element $\bar{x}$, the class of x mod $(f-1)S^{(d)}$. This map is well-defined, because we have the congruence $f^h x \equiv x$ mod $(f-1)S^{(d)}$ for any $x \in S^{(d)}$, so if $f^h x = 0$ for some $h > 0$ then $\bar{x} = 0$. On the other hand, if $x \in S_{nd}$ is such that $x = (f-1)y$ with $y = y_{hd} + y_{(h+1)d} \cdots + y_{kd}$, where $y_{jd} \in S_{jd}$ and $y_{hd} \neq 0$, we have necessarily $h = n$ and $x = -y_{hd}$, as well as the relations $y_{(j+1)d} = f y_{jd}$ for $h \leq j \leq k-1$ and $f_{ykd} = 0$; in particular, this implies $f^{k-n}x = 0$. We therefore have an inverse homomorphism from $S^{(d)}/(f-1)S^{(d)}$ to $S_{(f)}$ by corresponding a class $\bar{x}$ mod $(f-1)S^{(d)}$ (where $x \in S_{nd}$) the element x/f^n of $S_{(f)}$, since the preceding remark shows that this

map is well-defined. The first assertion is therefore proves, and the second one can be done similarly. □

Corollary 23.2.4. *If S is Noetherian, so is $S_{(f)}$ for any homogeneous element f of positive degree.*

Proof. This follows from Proposition 23.2.3 and Corollary 11.1.34. □

Let T be a multiplicative subset of S_+ formed by homogeneous elements; $T_0 = T \cup \{1\}$ is then a multiplicative subset of S. As the elements of T_0 are homogeneous, the ring $T_0^{-1}S$ is graded in a natrual way, and we denote by $S_{(T)}$ the subring of $T_0^{-1}S$ formed by elements of degree 0. We know that $T_0^{-1}S$ is identified with the inductive limit of the rings S_f, where $f \in T$ (with the canonical homomorphisms $S_f \to S_{fg}$). As this identification preserves the degrees, it identified $S_{(T)}$ as the inductive limit of $S_{(f)}$, where $f \in T$. For any graded S-module M, we define similarly the module $M_{(T)}$ (over the ring $S_{(T)}$) formed by degree zero elements of $T_0^{-1}M$, and we conclude that $M_{(T)}$ is the inductive limit of $M_{(f)}$ for $f \in T$.

If $\mathfrak{p}$ is a graded prime ideal of S_+, we denote by $S_{(\mathfrak{p})}$ and $M_{(\mathfrak{p})}$ the ring $S_{(T)}$ and the module $M_{(T)}$ respectively, where T is the homogeneous elements of S_+ not contained in $\mathfrak{p}$.

23.2.2 The homogeneous specturm of a graded ring

Given a graded ring S with positive degrees, we denote by $\mathrm{Proj}(S)$ the **homogeneous specturm** of S, which is the set of graded prime ideals of S_+, or, equivalently, the set of graded prime ideals of S not containing S_+. We will define a scheme structure on $\mathrm{Proj}(S)$, just as we have done for $\mathrm{Spec}(A)$ for a ring A.

For a subset E of S, let $V_+(E)$ be the set of graded prime ideals of S containing E and not containing S_+, which is also the subset $V(E) \cap \mathrm{Proj}(S)$ of $\mathrm{Spec}(S)$. We have immediately the following equalities:

$$V_+(0) = \mathrm{Proj}(S), \quad V_+(S) = V_+(S_+) = \varnothing,$$
$$V_+\Big(\bigcup_\lambda E_\lambda\Big) = \bigcap_\lambda V_+(E_\lambda),$$
$$V_+(EF) = V_+(E) \cup V_+(F).$$

Again, the set $V_+(E)$ remain unchanged if we replace E by the graded ideal it generates; moreover, if $\mathfrak{I}$ is a graded ideal of S, we have

$$V_+(\mathfrak{I}) = V_+\Big(\bigcup_{i\geq n}(\mathfrak{I} \cap S_i)\Big) \tag{2.2.1}$$

for any $n > 0$: in fact, if $\mathfrak{p} \in \mathrm{Proj}(S)$ contains the homogeneous elements of $\mathfrak{I}$ with degrees $\geq n$, as by hypothesis there exists a homogeneous element $f \in S_d$ not contained in $\mathfrak{p}$, for any $m \geq 0$ and any $x \in S_m \cap \mathfrak{I}$, we have $f^r x \in \mathfrak{I} \cap S_{m+rd}$ for r sufficiently large, hence $f^r x \in \mathfrak{p} \cap S_{m+rd}$, which implies $x \in \mathfrak{p} \cap S_m$. Finally, for any graded ideal $\mathfrak{I}$ of S, we have

$$V_+(\mathfrak{I}) = V_+(\mathfrak{r}_+(\mathfrak{I}))$$

where $\mathfrak{r}_+(\mathfrak{I})$ is the radical of $\mathfrak{I}$ in S_+.

By definition, $V_+(E)$ is a closed subset of $X = \mathrm{Proj}(S)$ for the topology induced by $\mathrm{Spec}(S)$. For each element $f \in S$, we set

$$D_+(f) = D(f) \cap \mathrm{Proj}(S) = \mathrm{Proj}(S) \setminus V_+(f).$$

Then for two elements $f, g \in S$, $D_+(fg) = D_+(f) \cap D_+(g)$, and the subsets $D_+(f)$, with $f \in S_+$, form a basis for the topology of $X = \mathrm{Proj}(S)$.

Let f be a homogeneous element of S_+ with degree $d > 0$. For any prime ideal $\mathfrak{p}$ of S not containing f, we see the set of x/f^n, where $x \in \mathfrak{p}$ and $n \geq 0$, is a prime ideal of the fraction ring S_f. Its trace on $S_{(f)}$ is then a prime ideal of this ring, which we denote by $\psi_f(\mathfrak{p})$: this is the set of elements x/f^n, for $n \geq 0$, $x \in \mathfrak{p}_{nd}$. We have therefore defined a map

$$\psi_f : D_+(f) \to \mathrm{Spec}(S_{(f)});$$

moreover, if g is another homogeneous element of S_+ with degree $e > 0$, we have a commutative diagram

$$\begin{tikzcd} D_+(fg) \arrow[r, "\psi_{fg}"] \arrow[d] & \mathrm{Spec}(S_{(fg)}) \arrow[d] \\ D_+(f) \arrow[r, "\psi_f"] & \mathrm{Spec}(S_{(f)}) \end{tikzcd} \tag{2.2.2}$$

where the left vertical maps are inclusions, and the right one is the map ${}^a\omega_{fg,f}$ induced from the canonical homomorphism $\omega_{fg,f} : S_{(f)} \to S_{(fg)}$. In fact, if $x/f^n \in \omega^{-1}(\psi_{fg}(\mathfrak{p}))$, where $fg \notin \mathfrak{p}$, we then have $g^n x/(fg)^n \in \psi_{fg}(\mathfrak{p})$, so $g^n x \in \mathfrak{p}$ and therefore $x \in \mathfrak{p}$, and the converse inclusion is evident.

Proposition 23.2.5. *The map ψ_f is a homeomorphism from $D_+(f)$ to* $\mathrm{Spec}(S_{(f)})$.

Proof. For $h \in S_{nd}$ is such that $h/f^n \in \psi_f(\mathfrak{p})$, by definition it is necessary and sufficient that $h \in \mathfrak{p}$, so $\psi^{-1}(D(h/f^n)) = D_+(fh) = D_+(h) \cap D_+(f)$ and the map ψ_f is therefore continuous. Moreover, the sets $D_+(hf)$, where h runs through the set S_{nd}, form a basis of the topology of $D_+(f)$, so the preceding argument proves, in view of the T_0-axiom for $D_+(f)$ and $\mathrm{Spec}(S_{(f)})$, that ψ_f is injective and the inverse map $\psi_f(D_+(f)) \to D_+(f)$ is continuous. Finally, to show that ψ_f is surjective, we remark that, if $\mathfrak{q}_0$ is a prime ideal of $S_{(f)}$ and if, for any $n > 0$, we denote by $\mathfrak{p}_n$ the set of elements $x \in_S n$ such that $x^d/f^n \in \mathfrak{q}_n$, the $\mathfrak{p}_n$ then verify the conditions Proposition 11.1.46: if $x \in S_n$, $y \in S_n$ are such that $x^d/f^n \in \mathfrak{q}_0$ and $y^d/f^n \in \mathfrak{q}_0$, we have $(x+y)^{2d}/f^{2n} \in \mathfrak{q}_0$, whence $(x+y)^d/f^n \in \mathfrak{q}_0$ since $\mathfrak{q}_0$ is prime; this proves that $\mathfrak{p}_n$ is a subgroup of S_n, and the verification of other conditions of Proposition 11.1.46 is immediate. If $\mathfrak{p}$ is the corresponding graded ideal of S, then $\psi_f(\mathfrak{p}) = \mathfrak{q}_0$, since if $x \in S_{nd}$, the relations $x/f^n \in \mathfrak{q}_0$ and $x^d/f^{nd} \in \mathfrak{q}_0$ are equivalent. □

Corollary 23.2.6. *For $D_+(f) \neq \varnothing$, it is necessary and sufficient that f is nilpotent.*

Proof. For $\mathrm{Spec}(S_{(f)}) = \varnothing$, it is necessary and sufficient that $S_{(f)} = 0$, which means $1 = 0$ in S_f, and this is equivalent to that f is nilpotent. □

Corollary 23.2.7. *Let E be a subset of S_+. The following conditions are equivalent:*

(i) $V_+(E) = X = \mathrm{Proj}(S)$.

(ii) Every element of E is nilpotent.

(iii) The homogeneous components of every element of E are nilpotent.

Proof. It is clear that (iii)⇒(ii)⇒(i). If $\mathfrak{I}$ is the graded ideal of S generated by E, conditions (i) is equivalent to that $V_+(\mathfrak{I}) = X$, and a fortiori, (i) implies that any homogeneous element $f \in \mathfrak{I}$ is such that $V_+(f) = X$, so f is nilpotent by Corollary 23.2.6. □

Corollary 23.2.8. *If $\mathfrak{I}$ is a graded ideal of S_+, $\mathfrak{r}_+(\mathfrak{I})$ is the intersection of graded prime ideals in $V_+(\mathfrak{I})$.*

Proof. By considering the ring $S/\mathfrak{I}$, we may assume that $\mathfrak{I} = 0$. It then suffices to prove that if $f \in S_+$ is not nilpotent, then there exists a graded prime ideal of S not containing f. Now, since there exists at least homogeneous component of f that is not nilpotent, we may assume that f is homogeneous, the result then follows from Corollary 23.2.6. □

For any subset Y of $X = \mathrm{Proj}(S)$, we denote by $I_+(Y)$ the subset of $f \in S_+$ such that $Y \subseteq V_+(f)$, which is in other words $I(Y) \cap S_+$; the set $I_+(Y)$ is then a radical ideal of S_+.

Proposition 23.2.9. *Let E be a subset of S and Y be a subset of X.*

(a) The ideal $I_+(V_+(E))$ is the radical in S_+ of the graded ideal of S_+ generated by E.

(b) The set $V_+(I_+(Y))$ is the closure of Y in X.

Proof. If $\mathfrak{I}$ is the graded ideal of S_+ generated by E, we have $V_+(E) = V_+(\mathfrak{I})$ and the first assertion follows from Corollary 23.2.8. As for (b), since $V_+(\mathfrak{I}) = \bigcap_{f\in\mathfrak{I}} V_+(f)$, the relation $Y \subseteq V_+(\mathfrak{I})$ implies $Y \subseteq V_+(f)$ for any $f \in \mathfrak{I}$, and therefore $I_+(Y) \supseteq \mathfrak{I}$, so $V_+(I_+(Y)) \subseteq V_+(\mathfrak{I})$, which implies (b) by the definition of closure. □

Corollary 23.2.10. *The closed subsets Y of $X = \mathrm{Proj}(S)$ and the graded radical ideals of S_+ correspond bijectively via $Y \mapsto I_+(Y)$ and $\mathfrak{I} \mapsto V_+(\mathfrak{I})$. Also, the union $Y_1 \cup Y_2$ of two closed subsets of X corresponds to $I_+(Y_1) \cap I_+(Y_2)$, and the intersection of a family (Y_λ) of closed subsets corresponds to the radical of the sum of $I_+(Y_\lambda)$.*

Corollary 23.2.11. *Let (f_α) be a family of homogeneous elements of S_+ and f be an element of S_+. The following conditions are equivalent:*

(i) $D_+(f) \subseteq \bigcup_\alpha D_+(f_\alpha)$;

(ii) $V_+(f) \supseteq \bigcap_\alpha V_+(f_\alpha)$;

(ii) a power of f is contained in the ideal generated by the f_α.

In particular, if $\mathfrak{I}$ is a graded ideal of S_+, then $V_+(\mathfrak{I}) = \varnothing$ if and only if $\mathfrak{r}_+(\mathfrak{I}) = S_+$.

Corollary 23.2.12. *For $X = \mathrm{Proj}(S)$ to be empty, it is necessary and sufficient that every element of S_+ is nilpotent.*

Corollary 23.2.13. *The closed irreducible subset of $X = \mathrm{Proj}(S)$ correspond to graded prime ideals of S_+.*

Proof. In fact, if $Y = Y_1 \cup Y_2$, where Y_1, Y_2 are closed and distinct in Y, then

$$I_+(Y) = I_+(Y_1) \cap I_+(Y_2)$$

the ideals $I_+(Y_1)$ and $I_+(Y_2)$ are distinct from $I_+(Y)$, so $I_+(Y)$ can not be prime. Conversely, if $\mathfrak{I}$ is a graded non-prime ideal of S_+, there exist elements f, g of S_+ such that $fg \in \mathfrak{I}$ but $f, g \notin \mathfrak{I}$. Then $V_+(f) \not\subseteq V_+(\mathfrak{I})$, $V_+(g) \not\subseteq V_+(\mathfrak{I})$, but $V_+(\mathfrak{I}) \subseteq V_+(f) \cup V_+(g)$. We then conclude that $V_+(\mathfrak{I})$ is the union of the closed subsets $V_+(f) \cap V_+(\mathfrak{I})$ and $V_+(g) \cap V_+(\mathfrak{I})$, both are distinct from $V_+(\mathfrak{I})$. □

We now define the scheme structure on the homogeneous specturm $\mathrm{Proj}(S)$. Let f, g be two homogeneous elements of S_+ and consider the affine schemes $Y_f = \mathrm{Spec}(S_{(f)})$, $Y_g = \mathrm{Spec}(S_{(g)})$, and $Y_{fg} = \mathrm{Spec}(S_{(fg)})$. In view of Lemma 23.2.1, the morphism $w_{fg,f} : Y_{fg} \to Y_f$ corresponding to the canonical homomorphism $\omega_{fg,f} : S_{(f)} \to S_{(fg)}$, is an open immersion. By the homeomorphism $\psi_f : D_+(f) \to Y_f$ (Proposition 23.2.5), we can transport to $D_+(f)$ the affine scheme structure of Y_f; in view of the commutative diagram (2.2.2), the affine scheme $D_+(fg)$ is identified with the subscheme induced over the open subset $D_+(fg)$ by the affine scheme $D_+(f)$. It is then clear that $X = \mathrm{Proj}(S)$ is endowed with a unique scheme structure such that each $D_+(f)$ is an affine open subscheme of X. When we speak of the homogeneous spectrum $\mathrm{Proj}(S)$ as a scheme, it will always be the structure defined in this way.

Proposition 23.2.14. *The scheme* $\mathrm{Proj}(S)$ *is separated.*

Proof. By Proposition 22.5.30, it suffices to show that for any homogeneous elements f, g of S_+, $D_+(f) \cap D_+(g) = D_+(fg)$ is affine and the canonical images of the rings of $D_+(f)$ and $D_+(g)$ in $D_+(fg)$ generate the ring of $D_+(fg)$. The first one is clear by definition, and the second one follows from Lemma 23.2.2, □

Example 23.2.15. Let $S = K[T_1, T_2]$ where K is a field and T_1, T_2 are indeterminates. Then it follows from Corollary 23.2.11 that $\mathrm{Proj}(S)$ is the union of $D_+(T_1)$ and $D_+(T_2)$. We see that each of these affine subscheme is isomorphic to $K[T]$, and that $\mathrm{Proj}(S)$ is obtained by glueing these two schemes as described in Example 22.2.8.

Proposition 23.2.16. *Let S be a graded ring with positive degrees and $X = \mathrm{Proj}(S)$.*

(i) If $\mathfrak{n}_+$ is the nilradical of S_+, the scheme X_{red} is canonically isomorphic to $\mathrm{Proj}(S/\mathfrak{n}_+)$. *In particular, if S is essentially reduced, then* $\mathrm{Proj}(S)$ *is reduced.*

(ii) Suppose that S is essentially reduced, then for X to be integral, it is necessary and sufficient that S is essentially integral.

Proof. Let $\bar{S} = S/\mathfrak{n}_+$, and denote by $x \mapsto \bar{x}$ the canonical homomorphism $S \to \bar{S}$, of degree 0. For any $f \in S_d$ $(d > 0)$, the canonical homomorphism $S_f \to \bar{S}$ is surjective and of degree 0, hence restricts to a surjection $S_{(f)} \to \bar{S}_{(\bar{f})}$. If we suppose that $f \notin \mathfrak{n}_+$, then $\bar{S}_{(\bar{f})}$ is reduced and the kenrel of the preceding homomorphism is the nilradical of $S_{(f)}$, whence $\bar{S}_{(\bar{f})} = (S_{(f)})_{\mathrm{red}}$. This homomorphism then corresponds to a closed immersion $D_+(\bar{f}) \to D_+(f)$ which identifies $D_+(\bar{f})$ with $(D_+(f))_{\mathrm{red}}$ (Corollary 22.4.26), and in particular is a homeomorphism of affine

scheme. Further, if $g \notin \mathfrak{n}_+$ is another homogeneous element of S_+, the diagram

$$\begin{tikzcd} S_{(f)} \arrow[r] \arrow[d] & \bar{S}_{(\bar{f})} \arrow[d] \\ S_{(fg)} \arrow[r] & \bar{S}_{(\overline{fg})} \end{tikzcd}$$

is commutative. As the sets $D_+(f)$ for f homogeneous in S_+ and $f \notin \mathfrak{n}_+$ form a covering for $X = \mathrm{Proj}(S)$, we conclude that the morphisms $D_+(\bar{f}) \to D_+(f)$ glue together to a closed immersion $\mathrm{Proj}(\bar{S}) \to \mathrm{Proj}(S)$ which is a homeomorphism on the underlying spaces, whence the conclusion of (i) by Corollary 22.4.26.

Suppose now that S is essentially integral, which means (0) is a graded ideal of S_+ distinct from S_+. Then X is reduced by (a) and irreducible by Corollary 23.2.13. Conversely, if S is essentially reduced and X is integral, then for any $f \neq 0$ homogeneous in S_+, we have $D_+(f) \neq \varnothing$ by Corollary 23.2.6; the hypothesis that X is irreducible implies that $D_+(f) \cap D_+(g) \neq \varnothing$ for any f, g homogeneous and nonzero in S_+, so in particular $fg \neq 0$, and we then conclude that S_+ is integral. □

Proposition 23.2.17. *Suppose that S is a graded A-algebra where A is a ring. Then over $X = \mathrm{Proj}(S)$ the structural sheaf $\mathcal{O}_X$ is an A-algebra, which means X is a scheme over* $\mathrm{Spec}(A)$.

Proof. It suffices to note that for any f homogeneous in S_+, $S_{(f)}$ is an A-algebra and the homomorphism $S_{(f)} \to S_{(fg)}$ is an A-algebra homomorphism for any f, g homogeneous in S_+. □

Proposition 23.2.18. *Let S be a graded ring with positive degrees.*

(a) For any integer $d > 0$, there exists a canonical isomorphism $\mathrm{Proj}(S) \cong \mathrm{Proj}(S^{(d)})$.

(b) Let S' be the graded ring such that $S'_0 = \mathbb{Z}$ and $S'_n = S_n$ for $n > 0$, then there exists a canonical isomorphism $\mathrm{Proj}(S) \cong \mathrm{Proj}(S')$.

Proof. We have already seen in Proposition 11.1.47 that the map $\mathfrak{p} \mapsto \mathfrak{p} \cap S^{(d)}$ is a bijection from $\mathrm{Proj}(S)$ to $\mathrm{Proj}(S^{(d)})$. As for any f homogeneous in S_+, we have $V_+(f) = V_+(f^d)$, this bijection is a homeomorphism of topological spaces. Finally, with the same notations, $S_{(f)}$ and $S_{(f^d)}$ are canonically identified by Lemma 23.2.1, so $\mathrm{Proj}(S)$ and $\mathrm{Proj}(S^{(d)})$ are canonically identified as schemes.

If to any $\mathfrak{p} \in \mathrm{Proj}(S)$, we correspond the unique prime ideal $\mathfrak{p}' \in \mathrm{Proj}(S')$ such that $\mathfrak{p}' \cap S_n = \mathfrak{p} \cap S_n$ for $n > 0$, then it is clear that this defines a homeomorphism $\mathrm{Proj}(S) \cong \mathrm{Proj}(S')$ of the underlying spaces, since $V_+(f)$ is the same set for S and S' if f is a homogeneous element of S_+. We also note that $S_{(f)} = S'_{(f)}$: to see this it suffices to note that if $x/1$ is an element of $S_{(f)}$ with $x \in S_0$, then $x/1 = xf/f \in S'_{(f)}$; we then conclude that $\mathrm{Proj}(S)$ and $\mathrm{Proj}(S')$ are identified as schemes. □

Corollary 23.2.19. *Let S be a graded A-algebra and S_A be the graded A-algebra such that $(S_A)_0 = A$ and $(S_A)_n = S_n$ for $n > 0$, then there exists a canonical isomorphism* $\mathrm{Proj}(S) \cong \mathrm{Proj}(S_A)$.

Proof. In fact, these two schemes are isomorphic to $\mathrm{Proj}(S')$, where $S'_0 = \mathbb{Z}$ and $S'_n = S_n$ for $n > 0$, in view of Proposition 23.2.18. □

23.2.3 Sheaf associated with a graded module

Let M be a graded S-module. For any homogeneous element f of S_+, $M_{(f)}$ is an $S_{(f)}$-module, and it therefore corresponds to a quasi-coherent sheaf $\widetilde{M_{(f)}}$ over the affine $\mathrm{Spec}(S_{(f)})$, identified with $D_+(f)$.

Proposition 23.2.20. *There existss a unique quasi-coherent $\mathcal{O}_X$-module $\widetilde{M}$ such that for any homogeneous element $f \in S_+$, we have $\Gamma(D_+(f), \widetilde{M}) = M_{(f)}$, and the restriction homomorphism $\Gamma(D_+(f), \widetilde{M}) \to \Gamma(D_+(fg), \widetilde{M})$ for f, g homogeneous in S_+ corresponds to the canonical homomorphism $M_{(f)} \to M_{(fg)}$.*

Proof. Suppose that $f \in S_d$, $g \in S_e$. As $D_+(fg)$ is identified with the prime specturm $(S_{(f)})_{g^d/f^e}$ by Lemma 23.2.1, the restriction of $\widetilde{M_{(f)}}$ to $D_+(fg)$ is canonically identified with the sheaf associated with the module $(M_{(f)})_{(g^d/f^e)}$, hence to $\widetilde{M_{(fg)}}$ (Lemma 23.2.1). We then conclude that there is a canonical isomorphism

$$\theta_{g,f} : \widetilde{M_{(f)}}|_{D_+(fg)} \to \widetilde{M_{(g)}}|_{D_+(fg)}$$

such that, if g is another homogeneous element of S_+, we have $\theta_{f,h} = \theta_{f,g} \circ \theta_{g,h}$ over $D_+(fgh)$. By glueing, there then exists a quasi-coherent sheaf $\mathscr{F}$ over X such that for any homogeneous element $f \in S_+$, we have an isomorphism $\eta_f : \mathscr{F}|_{D_+(f)} \cong \widetilde{M_{(f)}}$ and $\theta_{g,f} = \eta_g \circ \eta_f^{-1}$. Since over $D_+(f)$ we have $\Gamma(D_+(f), \widetilde{M})$, $\mathscr{F}$ can be identified with the sheaf extended from the presheaf $D_+(f) \mapsto M_{(f)}$ over the basis of standard open sets of X, whence the assertions of the proposition. In particular, we have $\widetilde{S} = \mathcal{O}_X$. □

We say the quasi-coherent $\mathcal{O}_X$-module $\widetilde{M}$ is **associted** with the graded S-module M. Recall that the graded S-modules form a category whose morphisms are graded homomorphisms of degrees. With this convention:

Proposition 23.2.21. *The functor $\widetilde{M}$ is a covariant exact functor from the category of graded S-modules to the category of quasi-coherent $\mathcal{O}_X$-modules, which commutes with inductive limits and direct sums.*

Proof. Since the properties are local, it suffices to verify over the sheaf $\widetilde{M}|_{D_+(f)} = \widetilde{M_{(f)}}$. Now the functor M_f on M, the functor N_0 on N, and the functor $\widetilde{P}$ on P all satisfy the stated properties, whence the claim. □

We denote by $\tilde{u} : \widetilde{M} \to \widetilde{N}$ the homomorphism corresponding to a graded homomorphism $u : M \to N$ of degree 0. We also deduce from Proposition 23.2.21 that the results of Corollary 22.1.6 and Corollary 22.1.7 are also true for graded S-modules and homomorphism of degree 0, via the same demonstration.

Proposition 23.2.22. *For any $\mathfrak{p} \in X = \mathrm{Proj}(S)$, we have $\widetilde{M}_{\mathfrak{p}} = M_{(\mathfrak{p})}$.*

Proof. By definition we have $\widetilde{M}_{\mathfrak{p}} = \varinjlim \Gamma(D_+(f), \widetilde{M})$, where f runs through homogeneous elements $f \in S_+$ such that $f \notin \mathfrak{p}$. As $\Gamma(D_+(f), \widetilde{M}) = M_{(f)}$, the proposition follows from the definition of $M_{(\mathfrak{p})}$. □

In particular, the local ring $\mathcal{O}_{X,\mathfrak{p}}$ is just the ring $S_{(\mathfrak{p})}$, the set of elements x/f where f is homogeneous in S_+ and not contained in $\mathfrak{p}$, and x is homogeneous with the same degree as f.

If moreover S is essentially integral, then $\mathrm{Proj}(S) = X$ is integral (Proposition 23.2.16), and if $\xi = (0)$ is the generic point of X, the rational function field $K(X) = \mathscr{O}_{X,\xi}$, is the field formed by f/g where f, g are homogeneous elements of S_+ and $g \neq 0$.

Proposition 23.2.23. *If, for any $z \in M$ and any homogeneous element $f \in S_+$, there exists a power of f annihilating z, then $\widetilde{M} = 0$. This condition is also necessary if $S = S_0[S_1]$.*

Proof. The condition $\widetilde{M} = 0$ is equivalent to $M_{(f)} = 0$ for any homogeneous element of S_+. Now if $f \in S_d$, the condition $M_{(f)} = 0$ signifies that for any $z \in M$ homogeneous whose degree is a multiple of d, there exists power f^n such that $f^n z = 0$; this implies the first claim. Conversely, if moreover S is generated by S_1, then condition then implies that $f^n z = 0$ for any $z \in M$ and any $f \in S_+$, since any element $f \in S_+$ is a finite linear combination of elements of S_1. □

Proposition 23.2.24. *Let $f \in S_d$ with $d > 0$. Then for any $n \in \mathbb{Z}$, the $(\mathscr{O}_X|_{D_+(f)})$-module $\widetilde{S(nd)}|_{D_+(f)}$ is canonically isomorphic to $\mathscr{O}_X|_{D_+(f)}$.*

Proof. The multiplication by the invertible element $(f/1)^n$ of S_f defines a bijection from $S_{(f)} = (S_f)_0$ to the ring

$$(S_f)_{nd} = (S_f(nd))_0 = (S(nd)_f)_0 = S(nd)_{(f)},$$

whence the assertion. □

Corollary 23.2.25. *Over the open subset $U = \bigcup_{f \in S_d} D_+(f)$, the restriction of the $\mathscr{O}_X$-module $\widetilde{S(nd)}$ is an invertible $(\mathscr{O}_X|_U)$-module.*

Corollary 23.2.26. *If the ideal S_+ of S is generated by S_1, then the $\mathscr{O}_X$-module $\widetilde{S(n)}$ is invertible for any $n \in \mathbb{Z}$.*

Proof. It suffices to note that under the hypothesis we have $X = \bigcup_{f \in S_1} D_+(f)$ by Corollary 23.2.11. □

The quasi-coherent $\mathscr{O}_X$-modules $\widetilde{S(n)}$ is of particular interest in the theory of projective schemes, so for each $n \in \mathbb{Z}$, we put $\mathscr{O}_X(n) = \widetilde{S(n)}$ and for an open subset U of X and any $(\mathscr{O}_X|_U)$-module $\mathscr{F}$, set

$$\mathscr{F}(n) = \mathscr{F} \otimes_{\mathscr{O}_X|_U} (\mathscr{O}_X(n)|_U).$$

If the ideal S_+ is generated by S_1, the functor $\mathscr{F}(n)$ is exact on $\mathscr{F}$ for any $n \in \mathbb{Z}$, since $\mathscr{O}_X(n)$ is then an invertible $\mathscr{O}_X$-module.

Example 23.2.27. Let k be a field and consider the graded algebra $S = k[x_0, \ldots, x_n]$; let $X = \mathrm{Proj}(S)$. Let d be an inter and consider the twist sheaf $\mathscr{O}_X(d)$. We compute the global sections for $\mathscr{O}_X(d)$: by definition, for each $x_i \in S$, the section of $\mathscr{O}_X(d)$ over $U_i = D_+(x_i)$ is given by

$$\Gamma(U_i, \mathscr{O}_X(d)) = S(d)_{(x_i)} = (S_{(x_i)})_d = \{f/x_i^n : f \in S_{n+d}\} = \{x_i^d f : f \in S^{(i)}\},$$

where $S^{(i)} = k[x_0/x_i, \ldots, x_n/x_i]$. Therefore a section of $\mathscr{O}_X(d)$ is a family of rational polynomials (f_i) with $f_i \in S^{(i)}$ such that $x_i^d f_i = x_j^d f_j$ for each $i \neq j$; let f be this common rational polynomial. Then by construction, we have $f/x_i^d \in S^{(i)}$ for each i, which implies that f is a polynomial in S of degree d when $d \geq 0$. If on the other hand $d < 0$, then f can only have poles at x_i for each i, which is impossible, so there is no global sections for $\mathscr{O}_X(d)$ when $d < 0$.

Let M, N be graded S-modules. For any $f \in S_d$ we define a canonical homomorphism of $S_{(f)}$-modules

$$\lambda_f : M_{(f)} \otimes_{S_{(f)}} N_{(f)} \to (M \otimes_S N)_{(f)}$$

by composing the homomorphism $M_{(f)} \otimes_{S_{(f)}} N_{(f)} \to M_f \otimes_{S_f} N_f$ (induced from the canonical injections) with the canonical isomorphism $M_f \otimes_{S_f} N_f \cong (M \otimes_S N)_{(f)}$, and note that by the definition of the grading of tensor products, these isomorphisms preserve degrees. Unwinding the definitions, for $x \in M_{md}$, $y \in N_{nd}$, we have

$$\lambda_f((x/f^m) \otimes (y/f^n)) = (x \otimes y)/f^{m+n}.$$

It then follows that, if $g \in S_e$ is another homogeneous element, the diagram

$$\begin{tikzcd}
M_{(f)} \otimes_{S_{(f)}} N_{(f)} \arrow[r, "\lambda_f"] \arrow[d] & (M \otimes_S N)_{(f)} \arrow[d] \\
M_{(fg)} \otimes_{S_{(fg)}} N_{(fg)} \arrow[r, "\lambda_{fg}"] & (M \otimes_S N)_{(fg)}
\end{tikzcd}$$

(wher the vertical homomorphism are canonical) is commutative. We then deduce that λ is a canonical homomorphism of $\mathcal{O}_X$-modules

$$\lambda : \widetilde{M} \otimes_{\mathcal{O}_X} \widetilde{N} \to \widetilde{M \otimes_S N}.$$

Consider in particular two graded ideals $\mathfrak{I}, \mathfrak{K}$ of S. As $\widetilde{\mathfrak{I}}$ and $\widetilde{\mathfrak{K}}$ are two quasi-coherent ideals of $\mathcal{O}_X$, we have a canonical homomorphism $\widetilde{\mathfrak{I}} \otimes_{\mathcal{O}_X} \widetilde{\mathfrak{K}} \to \mathcal{O}_X$, and the diagram

$$\begin{tikzcd}
\widetilde{\mathfrak{I}} \otimes_{\mathcal{O}_X} \widetilde{\mathfrak{K}} \arrow[rr, "\lambda"] \arrow[dr] & & \widetilde{\mathfrak{I} \otimes_S \mathfrak{K}} \arrow[dl] \\
& \mathcal{O}_X &
\end{tikzcd} \tag{2.3.1}$$

is commutative. Finally, note that if M, N, P are graded S-modules, the diagram

$$\begin{tikzcd}
\widetilde{M} \otimes_{\mathcal{O}_X} \widetilde{N} \otimes_{\mathcal{O}_X} \widetilde{P} \arrow[r, "\lambda \otimes 1"] \arrow[d, "1 \otimes \lambda"'] & \widetilde{M \otimes_S N} \otimes_{\mathcal{O}_X} \widetilde{P} \arrow[d, "\lambda"] \\
\widetilde{M} \otimes_{\mathcal{O}_X} \widetilde{N \otimes_S P} \arrow[r, "\lambda"] & (M \otimes_S N \otimes_S P)^{\sim}
\end{tikzcd} \tag{2.3.2}$$

is commutative. Simialrly, we define a canonical homomorphism of $S_{(f)}$-modules

$$\mu_f : \mathrm{Hom}_S(M, N)_{(f)} \to \mathrm{Hom}_{S_{(f)}}(M_{(f)}, N_{(f)})$$

which sends an element u/f^n, where u is a homomorphism of degre nd, the homomorphism $M_{(f)} \to N_{(f)}$ which sends x/f^m ($x \in M_{md}$) to $u(x)/f^{m+n}$. For $g \in S_e$, we have the following

commutative diagram

$$\begin{array}{ccc} \mathrm{Hom}_S(M,N)_{(f)} & \xrightarrow{\mu_f} & \mathrm{Hom}_{S_{(f)}}(M_{(f)},N_{(f)}) \\ \downarrow & & \downarrow \\ \mathrm{Hom}_S(M,N)_{(fg)} & \xrightarrow{\mu_{fg}} & \mathrm{Hom}_{S_{(fg)}}(M_{(fg)},N_{(fg)}) \end{array} \tag{2.3.3}$$

We then conclude that the μ_f define a canonical homomorphism

$$\mu : (\mathrm{Hom}_S(M,N))^{\sim} \to \mathscr{H}om_{\mathscr{O}_X}(\widetilde{M},\widetilde{N}).$$

Proposition 23.2.28. *Suppose that the ideal S_+ is generated by S_1. Then the homomorphism λ is an isomorphism; this holds for μ if the graded S-module M is of finite presentation.*

Proof. As X is the union of $D_+(f)$ for $f \in S_1$, we are reduced to prove tht λ_f and μ_f are isomorphisms for f homogeneous of degree 1. We then define a $\mathbb{Z}$-linear map $M_n \times N_n \to M_{(f)} \otimes_{S_{(f)}} N_{(f)}$ that send a pair (x,y) to the element $(x/f^m)\otimes(y/f^n)$. This then defines a $\mathbb{Z}$-linear map $M \otimes_{\mathbb{Z}} N \to M_{(f)} \otimes_{S_{(f)}} N_{(f)}$, and if $s \in S_q$, this map send $(sx)\otimes y$ to $(s/f^q)((x/f^m)\otimes(y/f^n))$ (where $x \in M_m$, $y \in N_n$), so we get a bi-homomorphism $\gamma_f : M \otimes_S N \to M_{(f)} \otimes_{S_{(f)}} N_{(f)}$ relative to the canonical homomorphism $S \to S_{(f)}$ (sending $s \in S_q$ to s/f^q). Suppose that for an element $\sum_i (x_i \otimes y_i)$ of $M \otimes_S N$ (where x_i, y_i are homogeneous elements of degrees m_i, n_i, respectively) we have $f^r \sum_i (x_i \otimes y_i) = 0$, which means $\sum_i (f^r x_i \otimes y_i) = 0$. Then we deduce from the isomorphism $M_f \otimes_{S_f} N_f \cong (M \otimes_S N)_f$ that $\sum_i (f^r x^i / f^{m_i+r}) \otimes (y_i/f^{n_i}) = 0$, which means $\gamma_i(\sum_i (x_i \otimes y_i)) = 0$. Therefore γ_f factors through $(M \otimes_S N)_f$ and give a homomorphism $\tilde{\gamma}_f : (M \otimes_S N)_f \to M_{(f)} \otimes_{S_{(f)}} N_{(f)}$; if $\tilde{\lambda}_f$ is the restriction of $\tilde{\gamma}_f$ to $(M \otimes_S N)_{(f)}$, we then verify that λ_f and $\tilde{\lambda}_f$ are inverses of each other, so the first assertion follows.

To demonstrate the second assertion, we now assume that M is of finite presentation, so is the cokernel of a homomorphism $P \to Q$ of graded S-module, P, Q being direct sums of finitely many modules of the form $S(n)$. By using the left exactness of $\mathrm{Hom}_S(-,N)$ and the exactness of $M_{(f)}$ on M, we are reduced to prove that μ_f is an isomorphism in the case $M = S(n)$. Now for any homogeneous $z \in N$, let u_z be the homomorphism from $S(n)$ to N such that $u_z(1) = z$; we then see that $\eta : z \mapsto u_z$ is an isomorphism of degree 0 from $N(-n)$ to $\mathrm{Hom}_S(S(n),N)$. It thus corresponds to an isomorphism

$$\eta_f : N(-n)_{(f)} \to \mathrm{Hom}_S(S(n),N)_{(f)}.$$

On the other hand, let $\tilde{\eta}_f$ be the isomorphism $N_{(f)} \to \mathrm{Hom}_{S_{(f)}}(S(n)_{(f)}, N_{(f)})$ which send $z' \in N_{(f)}$ to the homomorphism $v_{z'}$ such that $v_{z'}(s/f^k) = sz'/f^{n+k}$ (for $s \in S_{n+k} = S(n)_k$). We consider the composition

$$N(-n)_{(f)} \xrightarrow{\eta_f} \mathrm{Hom}_S(S(n),N)_{(f)} \xrightarrow{\mu_f} \mathrm{Hom}_{S_{(f)}}(S(n)_{(f)},N_{(f)}) \xrightarrow{\tilde{\eta}_f^{-1}} N_{(f)}$$

is the isomorphism $z/f^h \mapsto z/f^{h-n}$ from $N(-n)_{(f)} \to N_{(f)}$, so μ_f is an isomorphism. □

If the ideal S_+ is generated by S_1, we deduce from Proposition 23.2.28 that for any graded ideal $\mathfrak{I}$ of S and any graded S-module M, we have $\widetilde{\mathfrak{I}}\widetilde{M} = \widetilde{\mathfrak{I}M}$.

Corollary 23.2.29. *Suppose that the ideal S_+ is generated by S_1. Then for integers m, n, we have canonical isomorphisms*

$$\mathscr{O}_X(m) \otimes_{\mathscr{O}_X} \mathscr{O}_X(n) = \mathscr{O}_X(m+n), \quad \mathscr{O}_X(n) = (\mathscr{O}_X(1))^{\otimes n}.$$

Proof. The first formula follows from Proposition 23.2.28 and the existence of the canonical isomorphism $S(m) \otimes_S S(n) \cong S(m+n)$, which sends the element $1 \otimes 1 \in S(m)_{-m} \otimes S(n)_{-n}$ to the element $1 \in S(m+n)_{-(m+n)}$. It then suffices to demonstrate the second formula for $n = -1$, and in view of Proposition 23.2.28, this follows from the fact that $\mathrm{Hom}_S(S(1), S)$ is canonically isomorphic to $S(-1)$. □

Corollary 23.2.30. *Suppose that the ideal S_+ is generated by S_1. For any graded S-module M and $n \in \mathbb{Z}$, we have a canonical isomorphism $\widetilde{M(n)} = \widetilde{M}(n)$.*

Proof. This follows from Proposition 23.2.28 and the canonical isomorphism $M(n) \cong M \otimes_S S(n)$ which send $z \in M(n)_h = M_{n+h}$ to $z \otimes 1 \in M_{n+h} \otimes S(n)_{-n} \subseteq (M \otimes_S S(n))_h$. □

Example 23.2.31. Let S' be the graded ring such that $S'_0 = \mathbb{Z}$ and $S'_n = S_n$ for $n > 0$. Then if $f \in S_d$ $(d > 0)$, we have $S(n)_{(f)} = S'(n)_{(f)}$ for any $n \in \mathbb{Z}$, because an element of $S'(n)_{(f)}$ is of the form x/f^k where $x \in S'_{n+kd}$ $(k > 0)$, and we can always choose k such that $n + kd \neq 0$. As $X = \mathrm{Proj}(S)$ and $X' = \mathrm{Proj}(S')$ are canonically identified, we see that for any $n \in \mathbb{Z}$, $\mathscr{O}_X(n)$ and $\mathscr{O}_{X'}(n)$ are canonically isomorphic under this identification.

On the other hand, for any $d > 0$ and $n \in \mathbb{Z}$, we have

$$S^{(d)}(n)_h = S_{(n+h)d} = S(nd)_{hd};$$

so for any $f \in S_d$ we have $S^{(d)}(n)_{(f)} = S(nd)_{(f)}$. We have seen that the schemes $X = \mathrm{Proj}(S)$ and $X^{(d)} = \mathrm{Proj}(S^{(d)})$ are canonically identified, so under this identification, $\mathscr{O}_X(nd)$ and $\mathscr{O}_{X^{(d)}}(n)$ are canonically isomorphic, for any $n \in \mathbb{Z}$.

Proposition 23.2.32. *Let $d > 0$ be an integer and $U = \bigcup_{f \in S_d} D_+(f)$. Then the restriction to U of the canonical homomorphism $\mathscr{O}_X(nd) \otimes_{\mathscr{O}_X} \mathscr{O}_X(-nd) \to \mathscr{O}_X$ is an isomorphism for each $n \in \mathbb{Z}$.*

Proof. In view of Corollary 23.2.30, we can assume that $d = 1$, and the conclusion then follows the proof of Proposition 23.2.24. □

23.2.4 Graded S-module associated with a sheaf

In this part, for simplicity, we always assume that the ideal S_+ is generated by S_1, which also means that $S = S_0[S_1]$ by Proposition 11.1.33. The $\mathscr{O}_X$-module $\mathscr{O}_X(1)$ is then inveritble by Corollary 23.2.26; we then put, for any $\mathscr{O}_X$-module $\mathscr{F}$, that

$$\Gamma_*(\mathscr{F}) = \Gamma_*(\mathscr{O}_X(1), \mathscr{F}) = \bigoplus_{n \in \mathbb{Z}} \Gamma(X, \mathscr{F}(n))$$

Recall that $\Gamma_*(\mathscr{O}_X)$ is endowed with a graded ring structure and $\Gamma_*(\mathscr{F})$ is a graded module over $\Gamma_*(\mathscr{O}_X)$. Since $\mathscr{O}_X(n)$ is locally free, $\Gamma_*(\mathscr{F})$ is a covariant left-exact functor on $\mathscr{F}$; in particular, if $\mathscr{J}$ is a sheaf of ideals of $\mathscr{O}_X$, $\Gamma_*(\mathscr{F})$ is canonically a graded ideal of $\Gamma_*(\mathscr{O}_X)$.

Suppose that M is a graded S-module. For any $f \in S_d$ with $d > 0$, $x \mapsto x/1$ is a homomorphism of abelian groups $M_0 \mapsto M_{(f)}$, and as $M_{(f)}$ is canonically identified with $\Gamma(D_+(f), \widetilde{M})$, we obtain a homomorphism $\alpha_0^f : M_0 \to \Gamma(D_+(f), \widetilde{M})$ of abelian groups. It is clear that, for any $g \in S_e$ with $e > 0$, the diagram

$$\begin{tikzcd} & \Gamma(D_+(f), \widetilde{M}) \arrow[d] \\ M_0 \arrow[ur, "\alpha_0^f"] \arrow[r, "\alpha_0^{fg}"'] & \Gamma(D_+(fg), \widetilde{M}) \end{tikzcd}$$

is commutative, and this signifies that for any $x \in M_0$, the sections $\alpha_0^f(x)$ and $\alpha_0^{fg}(x)$ of M coincide over $D_+(fg)$, and therefore there exists a unique section $\alpha_0(x) \in \Gamma(X, \widetilde{M})$ whose restriction on $D_+(f)$ is $\alpha_0^f(x)$. We then define (under the hypothesis that S_+ is generated by S_1) a homomorphism

$$\alpha_0 : M_0 \to \Gamma(X, \widetilde{M}).$$

By applying this result on each graded S-module $M(n)$ (where $n \in \mathbb{Z}$), we then obtain homomorphisms of abelian groups

$$\alpha_n : M_n = M(n)_0 \to \Gamma(X, \widetilde{M}(n))$$

and therefore a homomorphism of graded abelian groups

$$\alpha : M \to \Gamma_*(\widetilde{M})$$

(also denoted by α_M) such that α_M coincides with α_n on each M_n.

If we consider in particular $M = S$, then it is easy to see that (by the definition of the multiplication of $\Gamma_*(\mathscr{O}_X)$) $\alpha : S \to \Gamma_*(\mathscr{O}_X)$ is a homomorphism of graded rings, therefore, for any S-module M, α is a bi-homomorphism of graded modules.

Proposition 23.2.33. *For any $f \in S_d$ with $d > 0$, $D_+(f)$ is identified with the subset of $\mathfrak{p} \in X$ such that the section $\alpha_d(f)$ of $\mathscr{O}_X(d)$ is nonzero at $\mathfrak{p}$.*

Proof. As $X = \bigcup_{g \in S_1} D_+(g)$, it suffices to prove that for any $g \in S_d$, the set $\mathfrak{p} \in D_+(g)$ where $\alpha_d(f)$ is nonzero is identified with $D_+(fg)$. Now the restriction of $\alpha_d(f)$ to $D_+(g)$ is by definition the section corresponding to the element $f/1$ of $S(d)_{(g)}$; by the canonical isomorphism $S(d)_{(g)} \cong S_{(g)}$, this section of $\mathscr{O}_X(d)$ over $D_+(g)$ is identified with the section of $\mathscr{O}_X$ over $D_+(g)$ corresponding to the element f/g^d of $S_{(g)}$. To see that this section is zero on $\mathfrak{p} \in D_+(g)$ then signifies that $f/g^d \in \mathfrak{q}$, where $\mathfrak{q}$ is the prime ideal of $S_{(g)}$ corresponding to $\mathfrak{p}$; by definition this means $f \in \mathfrak{p}$, whence the proposition. □

Now let $\mathscr{F}$ be an $\mathscr{O}_X$-module and put $M = \Gamma_*(\mathscr{F})$. In view of the homomorphism $\alpha : S \to \Gamma_*(\mathscr{O}_X)$ of graded rings, M can also be considered as a graded S-module. For any $f \in S_d$ $(d > 0)$, it follows from Proposition 23.2.33 that the restriction of the section $\alpha_d(f)$ of $\mathscr{O}_X(d)$ to $D_+(f)$ is invertible, and so is the restriction to $D_+(f)$ of $\alpha_d(f^n)$ for any $n > 0$. Let $z \in M_{nd} = \Gamma(X, \mathscr{F}(nd))$, if there existss an integer $k \geq 0$ such that the restriction to $D_+(f)$ of $f^k z$, which is the section $(\alpha_d(f^k)z)|_{D_+(f)}$ of $\mathscr{F}((n+k)d)$, is zero, then we conclude that $z|_{D_+(f)} = 0$. This shows that we can define an $S_{(f)}$-homomorphism $\beta_f : M_{(f)} \to \Gamma(D_+(f), \mathscr{F})$ which corresponds the element

$z/f^n \in M_{(f)}$ the section $(z|_{D_+(f)})(\alpha_d(f^n)|_{D_+(f)})^{-1}$ of $\mathscr{F}$ over $D_+(f)$. We also verify that for $g \in S_e$ ($e > 0$), the diagram

$$\begin{tikzcd} M_{(f)} \arrow[r, "\beta_f"] \arrow[d] & \Gamma(D_+(f), \mathscr{F}) \arrow[d] \\ M_{(fg)} \arrow[r, "\beta_{fg}"] & \Gamma(D_+(fg), \mathscr{F}) \end{tikzcd}$$

is commutative. Since $M_{(f)}$ is canonically identified with $\Gamma(D_+(f), \widetilde{M})$ and the $D_+(f)$ form a basis for the topological space X, the homomorphisms β_f glue together to a unique canonical homomorphism of $\mathscr{O}_X$-modules

$$\beta : \widetilde{\Gamma_*(\mathscr{F})} \to \mathscr{F}$$

(also denoted by $\beta_{\mathscr{F}}$) which is evidently functorial.

Proposition 23.2.34. *Let M be a graded S-module and $\mathscr{F}$ be an $\mathscr{O}_X$-module. Then the composition homomorphisms*

$$\widetilde{M} \xrightarrow{\tilde{\alpha}} (\Gamma_*(\widetilde{M}))^{\sim} \xrightarrow{\beta} \widetilde{M} \tag{2.4.1}$$

$$\Gamma_*(\mathscr{F}) \xrightarrow{\alpha} \Gamma_*(\widetilde{\Gamma_*(\mathscr{F})}) \xrightarrow{\Gamma_*(\beta)} \Gamma_*(\mathscr{F}) \tag{2.4.2}$$

are isomorphisms.

Proof. The verification of (2.4.1) is local: on an open subset $D_+(f)$, this result follows from the definition and the fact that the action of β is determined by its action of sections over $D_+(f)$ (Corollary 22.1.3). The verification of (2.4.2) can be done at each degree: if we put $M = \Gamma_*(\mathscr{F})$, we have $M_n = \Gamma(X, \mathscr{F}(n))$ and $\Gamma_*(\widetilde{M})_n = \Gamma(X, \widetilde{M}(n)) = \Gamma(X, \widetilde{M(n)})$. If $f \in S_1$ and $z \in M_n$, $\alpha_n^f(z)$ is the element $z/1$ of $M(n)_{(f)}$, and equals to $(f/1)^n(z/f^n)$; it then corresponds by β_f to the section

$$(\alpha_1(f)^n|_{D_+(f)})(z|_{D_+(f)})(\alpha_1(f)^n|_{D_+(f)})^{-1}$$

over $D_+(f)$, which is the restriction of z to $D_+(f)$. □

In general, the homomorphisms α and β are not isomorphisms (for example, a graded S-module M can be nonzero with $\widetilde{M}$ being zero). To obtain some nice results about these two homomorphisms, we need to impose further conditions on the graded ring S and the graded S-module M.

Proposition 23.2.35. *Let S be a graded ring and A be a ring.*

(a) If S is Noetherian, then $X = \mathrm{Proj}(S)$ is a Noetherian scheme.

(b) If S is a graded A-algebra of finite type, then $X = \mathrm{Proj}(S)$ is a scheme of finite type over $Y = \mathrm{Spec}(A)$.

Proof. If S is Noetherian, the ideal S_+ is generated by finitely many homogeneous elements $(f_i)_{1\le i\le p}$, so the space X is the union of $D_+(f_i) = \mathrm{Spec}(S_{(f_i)})$, and since each $S_{(f_i)}$ is Noetherian by Corollary 23.2.4, we see X is Noetherian.

Now assume that S is an A-algebra of finite type, then S_0 is an A-algebra of finite type and S is an S_0-algebra of finite type, so S_+ is a finitely generated ideal by Corollary 11.1.34. We are

then reduced to prove as in (a) that for any $f \in S_d$, $S_{(f)}$ is an A-algebra of finite type. In view of Proposition 23.2.3, it suffices to show that $S^{(d)}$ is an A-algebra of finite type, which follows from Proposition 11.1.35. □

Let M be a graded S-module. We say M is **eventually null** if there exists an integer n such that $M_i = 0$ for $i \neq n$, and is **eventually finite** if there exists an integer n such that $\bigoplus_{i \geq n} M_i$ is a finitely generated S-module, or equivalently, that there exists a finitely generated graded sub-S-module M' of M such that M/M' is eventually null. We also note that if M is eventually null, then $M_{(f)} = 0$ for any homogeneous element f in S_+, so $\widetilde{M} = 0$.

Let M, N be two graded S-modules. We say a homomorphism $u : M \to N$ of degree 0 is **eventually injective** (resp. **eventually surjective**, **eventually bijective**) if there exists an integer n such that $u_i : M_i \to N_i$ is injective (resp. surjective, bijective) for $i \geq n$. Equivalently, the homomorphism u is eventually injective (resp. eventually surjective) if and only if $\ker u$ (resp. $\operatorname{coker} u$) is eventually null. If u is eventually bijective, we say it is an **eventual isomorphism**.

Proposition 23.2.36. *Let S be a graded ring such that S_+ is finitely generated and M be a graded S-module.*

(a) If M is eventually finite, the $\mathscr{O}_X$-module $\widetilde{M}$ is of finite type.

(b) Suppose that M is eventually finite, then for $\widetilde{M} = 0$, it is necessary and sufficient that M is eventually null.

Proof. If $M_n = 0$ for $n \geq n_0$ then $M_{(f)} = 0$ for any homogeneous element $f \in S_+$, so if M is eventually null, then $\widetilde{M} = 0$. On the other hand, if M is eventually finite, then for $n \gg 0$ the graded submodule $M' = \bigoplus_{k \geq n} M_k$ is finitely generated by hypothesis, and M/M' is eventually null, so $\widetilde{(M/M')} = 0$ and therefore $\widetilde{M} = \widetilde{M}'$ by the exactness of the functor $\widetilde{M}$ (Proposition 23.2.21). Therefore, to prove that $\widetilde{M}$ is of finite type, we may assume that M is finitely generated. Now since this question is local, we only need to show that $M_{(f)}$ is finitely genrated over $S_{(f)}$ for any homogeneous $f \in S_d$ with $d > 0$. But $M^{(d)}$ is a finitely generated $S^{(d)}$ module by Proposition 11.1.35, and the assertion follows from Proposition 23.2.3.

Suppose now that M is eventually finite and $\widetilde{M} = 0$; then we have $\widetilde{M}' = 0$, so the condition that M' is eventually null is equivalent to that of M. We may therefore assume that M is finitely generated over S by homogeneous elements x_i $(1 \leq i \leq p)$; let $(f_j)_{1 \leq j \leq q}$ be a system of generators of the ideal S_+. We have by hypothesis $M_{(f_j)} = 0$ for any j, so there exists an integer n such that $f_j^n x_i = 0$ for any i, j. Let $n_j = \deg(f_j)$ and m be the supremum of $\sum_j r_j n_j$ for any finite system of integers (r_j) such that $\sum_j r_j \leq nq$. It is then clear that if $k > m$, we have $S_k x_i = 0$ for any i; if d is the supremum of the degrees of x_i, we then conclude that $M_k = 0$ for $k > d + m$, which proves our assertion. □

Corollary 23.2.37. *Let S be a graded ring such that S_+ is finitely generated. For $X = \operatorname{Proj}(S) = \varnothing$, it is necessary and sufficient that S is eventually null.*

Proof. The condition $X = \varnothing$ is in fact equivalent to $\mathscr{O}_X = \widetilde{S} = 0$, and S is clearly a finite generated S-module. □

Example 23.2.38. To give a counterexample of Proposition 23.2.36, let k be a field and $S = k[x_1, \ldots, x_n]$ be the polynomial ring with n variables. Consider the graded S-module M given

by

$$M = k[x_1, x_2, \dots, x_n, \dots]/(x_1, x_2^2, \dots, x_n^n, \dots)$$

with the usual multiplication of polynomials. Then M is not finitely generated over S, and for every homogeneous polynomial f of degree 1, we see $f^N M = 0$ for sufficiently large N. Therefore $\widetilde{M} = 0$. However, note that $M_n \neq 0$ for every n.

Theorem 23.2.39. *Suppose that S is a graded ring such that the ideal S_+ is finitely generated by S_1, and let $X = \mathrm{Proj}(S)$. Then, for any quasi-coherent $\mathscr{O}_X$-module $\mathscr{F}$, the canonical homomorphisms $\beta : \widetilde{\Gamma_*(\mathscr{F})} \to \mathscr{F}$ is an isomorphism.*

Proof. If S_+ is generated by finitely many $f_i \in S_1$, then X is the union of $\mathrm{Spec}(S_{(f_i)})$ which are quasi-compact, so X is quasi-compact. Also, $\mathscr{O}_X(n)$ is invertible for any $n \in \mathbb{Z}$ by Corollary 23.2.29, and since X is separated, by Corollary 22.6.15 and Proposition 23.2.33, we have for any $f \in S_d$ a canonical isomorphism $\Gamma_*(\mathscr{F})_{(\alpha_d(f))} \cong \Gamma(D_+(f), \mathscr{F})$ (the first module (considered as a $\Gamma_*(\mathscr{O}_X)$-module) is none other than $\Gamma_*(\mathscr{F})_{(f)}$ (considered as an S-module)). If we trace the definition of this isomorphism, we see that it coincides with β_f, whence our assertion. □

Corollary 23.2.40. *Under the hypotheses of Theorem 23.2.39, any quasi-coherent $\mathscr{O}_X$-module (of finite type) is isomorphic to an $\mathscr{O}_X$-module of the form $\widetilde{M}$, where M is a (finitely generated) graded S-module.*

Proof. Let $\mathscr{F}$ be a quasi-coherent $\mathscr{O}_X$-module, then $\mathscr{F} = \widetilde{M}$ for a graded S-module M by Theorem 23.2.39. Let $(f_\lambda)_{\lambda \in I}$ be a system of homogeneous generators of M; for each finite subset H of I, let M_H be the graded submodule of M generated by f_λ for $\lambda \in H$. It is clear that M is the inductive limit of the submodules M_H, so $\mathscr{F}$ is the inductive limit of the sub-$\mathscr{O}_X$-modules $\widetilde{M}_H$ (Proposition 23.2.21). If $\mathscr{F}$ is of finite type, we conclude from Proposition 19.4.10. □

Corollary 23.2.41. *Under the hypotheses of Theorem 23.2.39, for any quasi-coherent $\mathscr{O}_X$-module $\mathscr{F}$ of finite type, there exists an integer n_0 such that for any $n \geq n_0$, $\mathscr{F}(n)$ is isomorphic to a quotient of $\mathscr{O}_X^r$ (where $r > 0$ depends on n), and therefore is generated by finitely many global sections.*

Proof. By Corollary 23.2.40, we can assume that $\mathscr{F} = \widetilde{M}$ where M is a quotient of a finite dierct sum of $S(m_i)$. By Proposition 23.2.21, we are therefore reduced to the case where $M = S(m)$, so $\mathscr{F}(n) = (S(m+n))^\sim = \mathscr{O}_X(m+n)$. It then suffices to prove that for each $n \geq 0$ there exists r and a surjective homomorphism $\mathscr{O}_X^r \to \mathscr{O}_X(n)$. For this, it suffcies to prove that, for a suitable r, there exists an eventually surjective homomorphism $u : S^r \to S(n)$ of degree zero. Now we have $S(n)_0 = S_n$, and by hypothesis $S_h = S_1^h$ for any $h > 0$, so $SS_n = \bigoplus_{h \geq n} S_h$. As S_n is a finitely generated S_0-module (Corollary 11.1.34), consider a system $(a_i)_{1 \leq i \leq r}$ of generators of this module, and let $u : S^r \to S(n)$ be the homomorphism that sends the i-th basis e_i of S^r to a_i. Then the image of u contains $\bigoplus_{h \geq 0} S(n)_h$, so u satisfies the requirement and the proof is complete. □

Corollary 23.2.42. *Under the hypotheses of Theorem 23.2.39, for any quasi-coherent $\mathscr{O}_X$-module $\mathscr{F}$ of finite type, there exists an integer n_0 such that for any $n \geq n_0$, $\mathscr{F}$ is isomorphic to a quotient of an $\mathscr{O}_X$-module of the form $\mathscr{O}_X(-n)^r$ (where $r > 0$ depends on n).*

Proof. This follows from Corollary 23.2.41 by tensoring with the invertible sheaf $\mathscr{O}_X(-n)$, which preserves the exactness. □

Proposition 23.2.43. *Assume the hypotheses of Theorem 23.2.39 and let M be a graded S-module.*

(a) *The cannical homomorphism* $\tilde{\alpha} : \widetilde{M} \to (\Gamma_*(\widetilde{M}))^{\sim}$ *is an isomorphism.*

(b) *Let* $\mathscr{G}$ *be a quasi-coherent sub-*$\mathscr{O}_X$*-module of* $\widetilde{M}$ *and let* N *be the graded sub-*S*-module of* M *which is the inverse image of* $\Gamma_*(\mathscr{G})$ *under* α*. Then we have* $\widetilde{N} = \mathscr{G}$*.*

Proof. As $\beta : (\Gamma_*(\widetilde{M}))^{\sim} \to \widetilde{M}$ is an isomorphism, $\tilde{\alpha}$ is its inverse isomorphism in view of (2.4.1), whence (a). Let P be the graded submodule $\alpha(M)$ of $\Gamma_*(\widetilde{M})$; as $\widetilde{M}$ is an exact functor, the image of $\widetilde{M}$ under $\tilde{\alpha}$ is equal to $\widetilde{P}$, so in view of (a), $\widetilde{P} = (\Gamma_*(\widetilde{M}))^{\sim}$. Put $Q = \Gamma_*(\mathscr{G}) \cap P$, so that $N = \alpha^{-1}(Q)$. Then by the preceding argument and Proposition 23.2.21, the image of $\widetilde{N}$ under $\tilde{\alpha}$ is $\widetilde{Q}$, and we have $\widetilde{Q} = \widetilde{\Gamma_*(\mathscr{G})}$. Since the image of $\widetilde{\Gamma_*(\mathscr{G})}$ under β is $\mathscr{G}$ and $\tilde{\alpha}$ is the inverse of β, we conclude that $\widetilde{N} = \mathscr{G}$. □

23.2.5 Functorial properties of $\mathrm{Proj}(S)$

Let S, S' be two graded rings with positive degree and $\varphi : S' \to S$ be a homomorphisms of graded rings. We denote by $G(\varphi)$ the open subset of $X = \mathrm{Proj}(S)$ which is the complement of $V_+(\varphi(S'_+))$, or, the union of $D_+(\varphi(f'))$ where f' runs through homogeneous elements of S'_+. The restriction to $G(\varphi)$ of the continuous map ${}^a\varphi : \mathrm{Spec}(S') \to \mathrm{Spec}(S)$ is then a continuous map from $G(\varphi)$ to $\mathrm{Proj}(S')$, which is still denoted by ${}^a\varphi$. If $f' \in S'_+$ is homogeneous, we have

$$ {}^a\varphi^{-1}(D_+(f')) = D_+(\varphi(f')) \tag{2.5.1} $$

since ${}^a\varphi$ maps $G(\varphi)$ into $\mathrm{Proj}(S')$. On the other hand, the homomorphism φ defines canonically a homomorphism of graded rings $S'_{f'} \to S_f$ of degree 0 (where $f = \varphi(f')$), whence a homomorphism $S'_{(f')} \to S_{(f)}$, which we denote by $\varphi_{(f)}$. It then corresponds to a morphism $({}^a\varphi_{(f)}, \tilde{\varphi}_{(f)}) : \mathrm{Spec}(S_{(f)}) \to \mathrm{Spec}(S'_{(f')})$ of affine schemes. If we identify $\mathrm{Spec}(S_{(f)})$ with the open subscheme $D_+(f)$ of $\mathrm{Proj}(S)$, we then obtain a morphism $\Phi_f : D_+(f) \to D_+(f')$ and ${}^a\varphi_{(f)}$ is identified with the restriction of ${}^a\varphi$ to $D_+(f)$. If g' is another homogeneous element of S'_+ and $g = \varphi(g')$, it is immediate that the diagram

$$ \begin{tikzcd} D_+(fg) \arrow[r, "\Phi_{fg}"] \arrow[d] & D_+(f'g') \arrow[d] \\ D_+(f) \arrow[r, "\Phi_f"] & D_+(f') \end{tikzcd} $$

is commutative.

Proposition 23.2.44. *Let* $\varphi : S' \to S$ *be a homomorphism of graded rings. There exists a unique morphism* $({}^a\varphi, \tilde{\varphi}) : G(\varphi) \to \mathrm{Proj}(S')$ *(called the morphism associated with* φ *and denoted by* $\mathrm{Proj}(\varphi)$*), such that for any homogeneous element* $f' \in S'_+$*, the restriction of this morphism to* $D_+(\varphi(f'))$ *coincides with the morphism associated with the homomorphism* $\varphi_{(f)} : S'_{(f')} \to S_{(\varphi(f'))}$*.*

Proof. The morphism $({}^a\varphi, \tilde{\varphi})$ is obtained form glueing the morphisms Φ_f over $D_+(f)$, and the claim property is immediate. □

Corollary 23.2.45. *Let* $\varphi : S' \to S$ *be a homomorphism of graded rings.*

(a) *The morphism* $\mathrm{Proj}(\varphi)$ *is affine.*

(b) *If* $\ker \varphi$ *is nilpotent (and in particular if* φ *is injective), the morphism* $\mathrm{Proj}(\varphi)$ *is dominant.*

(c) *If φ is eventually surjective, then $G(\varphi) = \mathrm{Proj}(S)$.*

Proof. The first assertion follows from Corollary 23.2.45 and the relation ${}^a\varphi^{-1}(D_+(f')) = D_+(\varphi(f'))$. On the other hand, if $\ker\varphi$ is nilpotent, for any f' homogeneous in S'_+, we verify that $\ker\varphi_f$ is also nilpotent, and so is $\ker\varphi_{(f)}$. The conclusion then follows from Corollary 10.4.19. Finally, if φ is eventually surjective, then every homogeneous element $f \in S_+$ has some power contained in the image of φ, so by Corollary 23.2.11 we conclude that $G(\varphi) = \bigcup_{f'\in S'_+} D_+(\varphi(f')) = \mathrm{Proj}(S)$, whence the claim. □

Remark 23.2.1. Note that there are in general morphisms from $\mathrm{Proj}(S)$ to $\mathrm{Proj}(S')$ which are not affine, and therefore do not come from graded ring homomorphisms $S' \to S$; an example is the structural morphism $\mathrm{Proj}(S) \to \mathrm{Spec}(A)$, where A is field ($\mathrm{Spec}(A)$ being identified with $\mathrm{Proj}(A[T])$ (cf. Corollary 23.3.5)).

Let $\varphi' : S'' \to S'$ be another homomorphism of graded rings, and put $\varphi'' = \varphi \circ \varphi'$. Then by the formula ${}^a\varphi'' = {}^a\varphi' \circ {}^a\varphi$ and $G(\varphi'') \subseteq G(\varphi)$, if Φ, Φ', and Φ'' are the associated morphisms of φ, φ' and φ'', we have $\Phi'' = \Phi' \circ (\Phi|_{G(\varphi'')})$.

Suppose that S (resp. S') is a graded A-algebra (resp. a graded A'-algebra), and let $\psi : A' \to A$ be a homomorphism of rings such that the diagram

$$\begin{tikzcd} A' \arrow[r, "\psi"] \arrow[d] & A \arrow[d] \\ S' \arrow[r, "\varphi"] & S \end{tikzcd}$$

is commutative. We can then consider $G(\varphi)$ and $\mathrm{Proj}(S')$ as schemes over $\mathrm{Spec}(A)$ and $\mathrm{Spec}(A')$, respectively. If Φ and Ψ are the associated morphisms of φ and ψ, respectively, the diagram

$$\begin{tikzcd} G(\varphi) \arrow[r, "\Phi"] \arrow[d] & \mathrm{Proj}(S') \arrow[d] \\ \mathrm{Spec}(A) \arrow[r, "\Psi"] & \mathrm{Spec}(A') \end{tikzcd}$$

is commutative.

Now let M be a graded S-module and consider the S'-module $\varphi^*(M)$, which is clearly graded. Let f' be a homogeneous element in S'_+, and set $f = \varphi(f')$. We then have a canonical isomorphism $(\varphi^*(M))_{f'} \cong \varphi^*_f(M_f)$, and it is clear that this isomorphism preserves degrees, so induces an isomorphism $(\varphi^*(M))_{(f')} \cong \varphi^*_{(f)}(M_{(f)})$. There is then canonically an isomorphism of sheaves $\widetilde{\varphi^*(M)}|_{D_+(f')} \cong (\Phi_f)_*(\widetilde{M}|_{D_+(f)})$ (Proposition 22.1.11). Moreover, if g' is another homogeneous element of S'_+ and $g = \varphi(g')$, the diagram

$$\begin{tikzcd} (\varphi^*(M))_{(f')} \arrow[r, "\sim"] \arrow[d] & (M_{(f)})_{(\varphi_{(f)})} \arrow[d] \\ (\varphi^*(M))_{(f'g')} \arrow[r, "\sim"] & (M_{(fg)})_{(\varphi_{(fg)})} \end{tikzcd}$$

is commutative, whence we conclude that the isomorphism

$$\widetilde{\varphi^*(M)}|_{D_+(f'g')} \cong (\Phi_{fg})_*(\widetilde{M}|_{D_+(fg)})$$

is the restriction to $D_+(f'g')$ of the isomorphism $\widetilde{\varphi^*(M)}|_{D_+(f')} \cong (\Phi_f)_*(\widetilde{M}|_{D_+(f)})$. As Φ_f is the restriction of Φ on $D_+(f)$, we then obtain the following result:

Proposition 23.2.46. *There exists a canonical isomorphism $\widetilde{\varphi^*(M)} \cong \Phi_*(\widetilde{M}|_{G(\varphi)})$ of $\mathcal{O}_X$-modules.*

We also deduce a canonical functorial map from the set of φ-homomorphisms $M' \to M$ from a graded S'-module to a graded S-module M, to the set of Φ-morphisms $\widetilde{M}' \to \widetilde{M}|_{G(\varphi)}$. If $\varphi' : S'' \to S'$ is another ring homomorphism and M'' is a graded S''-module, the composition of a φ-morphism $M' \to M$ and a φ'-morphism $M'' \to M'$ canonically corresponds to the composition of $\widetilde{M}'|_{G(\varphi')} \to \widetilde{M}|_{G(\varphi'')}$ and $\widetilde{M}'' \to \widetilde{M}'|_{G(\varphi')}$.

Proposition 23.2.47. *Let $\varphi : S' \to S$ be a homomorphism of graded rings and M' be a graded S'-module. Then there exists a canonical homomorphism $\nu : \Phi^*(\widetilde{M}') \to \widetilde{\varphi_*(M)}|_{G(\varphi)}$. If the ideal S'_+ is generated by S'_1, then ν is an isomorphism.*

Proof. For $f' \in S'_d$ with $d > 0$, we define a canonical homomorphism of $S_{(f)}$-modules (where $f = \varphi(f')$)

$$\nu_f : M'_{(f)} \otimes_{S'_{(f)}} S_{(f)} \to (M' \otimes_{S'} S)_{(f)}$$

by composing the homomorphism $M'_{(f)} \otimes_{S'_{(f)}} S_{(f)} \to M_{f'} \otimes_{S'_{f'}} S_f$ with the canonical homomorphism $M'_{f'} \otimes_{S'_{f'}} S_f \cong (M' \otimes_{S'} S)_f$. It is immediate to verify that compatibility of ν_f with the restriction homomorphisms $D_+(f)$ to $_+(fg)$ (for $g' \in S'_+$ and $g = \varphi(g')$), so we obtain a homomorphism

$$\nu : \Phi^*(\widetilde{M}') \to \widetilde{\varphi_*(M)}|_{G(\varphi)}.$$

For the second assertion, it suffices to prove that ν_f is an isomorphism for each $f' \in S'_1$, since $G(\varphi)$ is the union of $D_+(\varphi(f'))$. We first define a $\mathbb{Z}$-bilinear map $M'_m \times S_n \to M'_{(f')} \otimes_{S'_{f'}} S_{(f)}$ which sends (x', s) to the element $(x'/f'^m) \otimes (s/f^n)$. As in the proof of Proposition 23.2.28, this map then induces a bi-homomorphism

$$\eta_f : M' \otimes_{S'} S \to M'_{(f')} \otimes_{S'_{(f')}} S_{(f)}.$$

Moreover, if, for $r > 0$, we have $f^r \sum_i (x'_i \otimes s_i) = 0$, then $\sum_i (f'^r x'_i \otimes s_i) = 0$, so $\sum_i (f'^r x_i / f'^{m_i+r}) \otimes (s_i/f^{n_i}) = 0$, which means $\eta_f(\sum_i x_i \otimes y_i) = 0$; the homomorphism then factors through $(M' \otimes_{S'} S)_f$ and gives a homomorphism $\tilde{\eta}_f : (M' \otimes_{S'} S)_f \to M'_{(f')} \otimes_{S'_{(f')}} S_{(f)}$. It is easy to verify that $\tilde{\eta}_f$ is the inverse of ν_f, whence our assertion. □

In particular, since $\varphi_*(S'(n)) = S(n)$ for each $n \in \mathbb{Z}$, it follows from Proposition 23.2.47 that we have a canonical homomorphism $\Phi^*(\mathcal{O}_{X'}(n)) \to \mathcal{O}_X(n)|G(\varphi)$, and this an isomorphism if S'_+ is generated by S'_1.

Remark 23.2.2. We note that it follows from Proposition 23.2.18 that the morphism Φ is unchanged if we replace S by $S^{(d)}$, S' by $S'^{(d)}$, and φ by $\varphi^{(d)}$. Also, it is also unchanged if we replace S_0 and S'_0 by $\mathbb{Z}$ and φ_0 be the identity map.

Let A, A' be two rings and $\psi : A' \to A$ be a homomorphism of rings, which defines a morphism $\Psi : \mathrm{Spec}(A) \to \mathrm{Spec}(A')$. Let S' be an A'-algebra with positive degrees, and put $S = S' \otimes_{A'} A$, which is a graded A-algebra by setting $S_n = S'_n \otimes_{A'} A$. The map $s' \mapsto s' \otimes 1$ is then a homomorphism of graded rings and also a bi-homomorphism. Since S_+ is the A-module

generated by $\varphi(S'_+)$, we have $G(\varphi) = \mathrm{Proj}(S) = X$, so, if we put $X' = \mathrm{Proj}(S')$, we have a commutative diagram

$$\begin{tikzcd} X \arrow[r, "\Phi"] \arrow[d, "p"'] & X' \arrow[d] \\ Y \arrow[r, "\Psi"] & Y' \end{tikzcd} \tag{2.5.2}$$

Now let M' be a graded S'-module, and set $M = M' \otimes_{A'} A = M' \otimes_{S'} S$.

Proposition 23.2.48. *The commutative diagram (2.5.2) is cartesian and the canonical homomorphism $\nu : \Phi^*(\widetilde{M}') \to \widetilde{M}$ in Proposition 23.2.47 is an isomorphism.*

Proof. The first assertion follows if we can prove that for any f' homogeneous in S'_+ and $f = \varphi(f')$, the restriction of Φ and p to $D_+(f)$ identify this scheme as $D_+(f') \times_{Y'} Y$; in other words, it suffices to prove that $S_{(f)}$ is canonically identified with $S'_{(f')} \otimes_{A'} A$, which is immedaite from the fact that the canonical isomorphism $S_f \cong S'_{f'} \otimes_{A'} A$ preserves degrees. The second assertion follows from the isomorphism $M'_{(f')} \otimes_{S'_{(f')}} S_{(f)} \cong M'_{(f')} \otimes_{A'} A$, and the later one is isomorphic to $M_{(f)}$ since M_f is canonically identified with $M'_{f'} \otimes_{A'} A$. □

Corollary 23.2.49. *For any integer $n \in \mathbb{Z}$, $\widetilde{M}(n)$ is identified with $\Phi^*(\widetilde{M}'(n)) = \widetilde{M}'(n) \otimes_{Y'} \mathscr{O}_Y$. In particular, $\mathscr{O}_X(n) = \Phi^*(\mathscr{O}_{X'}(n)) = \mathscr{O}_{X'}(n) \otimes_{Y'} \mathscr{O}_Y$.*

Proof. This follows from Proposition 23.2.48 and Corollary 23.2.30. □

Now let $\mathscr{F}'$ be an $\mathscr{O}_{X'}$-module and $\mathscr{F} = \Phi^*(\mathscr{F}')$. Then we have for each $n \in \mathbb{Z}$ that $\mathscr{F}(n) = \Phi^*(\mathscr{F}'(n))$ in view of Corollary 23.2.49. Therefore, by the definition of Φ^*, we have a canonical homomorphism

$$\Gamma(\rho) : \Gamma(X', \mathscr{F}'(n)) \to \Gamma(X, \mathscr{F}(n))$$

which then gives a canonical bi-homomorphism $\Gamma_*(\mathscr{F}') \to \Gamma_*(\mathscr{F})$ of graded modules.

Suppose that the ideal S'_+ is generated by S'_1 and $\mathscr{F}' = \widetilde{M}'$, so $\mathscr{F} = \widetilde{M}$ where $M = M' \otimes_{A'} A$. If f' is homogeneous in S'_+ and $f = \varphi(f')$, we have $M_{(f)} = M'_{(f')} \otimes_{A'} A$ and the diagram

$$\begin{tikzcd} M'_0 \arrow[r] \arrow[d] & M'_{(f')} = \Gamma(D_+(f), \widetilde{M}') \arrow[d] \\ M_0 \arrow[r] & M_{(f)} = \Gamma(D_+(f), \widetilde{M}) \end{tikzcd}$$

is commutative. We then conclude from the definition of the homomorphism $\alpha : M \to \Gamma_*(\widetilde{M})$ that the following diagram

$$\begin{tikzcd} M' \arrow[r, "\alpha_{M'}"] \arrow[d] & \Gamma_*(\widetilde{M}') \arrow[d] \\ M \arrow[r, "\alpha_M"] & \Gamma_*(\widetilde{M}) \end{tikzcd} \tag{2.5.3}$$

is commutative. Similarly, the diagram

$$\begin{tikzcd} \widetilde{\Gamma_*(\mathscr{F}')} \arrow[r, "\beta_{\mathscr{F}'}"] \arrow[d] & \mathscr{F}' \arrow[d] \\ \widetilde{\Gamma_*(\mathscr{F})} \arrow[r, "\beta_{\mathscr{F}}"] & \mathscr{F} \end{tikzcd} \tag{2.5.4}$$

is commutative (where the vertical is the canonical Φ-morphism $\mathscr{F}' \to \Phi^*(\mathscr{F}') = \mathscr{F}$).

Now let N' be another graded S'-module and $N = N' \otimes_{A'} A$. It is immediate that the canonical bi-homomorphisms $M' \to M$, $N' \to N$ give a bi-homomorphism $M' \otimes_{S'} N' \to M \otimes_S N$, and therefore an S-homomorphism $(M' \otimes_{S'} N') \otimes_{A'} A \to M \otimes_S N$ of degree 0, which then corresponds to an $\mathscr{O}_X$-homomorphism

$$\Phi^*((M' \otimes_{S'} N')^{\sim}) \to (M \otimes_S N)^{\sim}.$$

Moreover, it is immedaite to verify that the following diagram

$$\begin{tikzcd} \Phi^*(\widetilde{M}' \otimes_{\mathscr{O}_{X'}} \widetilde{N}') \arrow[r, "\sim"] \arrow[d, "\Phi^*(\lambda)"] & \widetilde{M} \otimes_{\mathscr{O}_X} \widetilde{N} = \Phi^*(\widetilde{M}') \otimes_{\mathscr{O}_X} \Phi^*(\widetilde{N}') \arrow[d, "\lambda"] \\ \Phi^*((M' \otimes_{S'} N')^{\sim}) \arrow[r] & (M \otimes_S N)^{\sim} \end{tikzcd} \tag{2.5.5}$$

is commutative (where the first row is an isomorphism by (3.3.1)). If the ideal S'_+ is generated by S'_1, it is clear that S_+ is generated by S_1, so the two vertical homomorphisms are isomorphisms, so the second row is also an isomorphism.

We have similarly a cannical bi-homomorphism $\mathrm{Hom}_{S'}(M', N') \to \mathrm{Hom}_S(M, N)$, which sends a homomorphism u' of degree k the homomorphism $u' \otimes 1$, which is also of degree k. We then deduce an S-homomorphism of degree 0:

$$\mathrm{Hom}_{S'}(M', N') \otimes_{A'} A \to \mathrm{Hom}_S(M, N)$$

which corresponds to a homomorphism of $\mathscr{O}_X$-modules:

$$\Phi^*((\mathrm{Hom}_{S'}(M', N'))^{\sim}) \to (\mathrm{Hom}_S(M, N))^{\sim}.$$

Similarly, the diagram

$$\begin{tikzcd} \Phi^*((\mathrm{Hom}_{S'}(M', N'))^{\sim}) \arrow[r] \arrow[d, "\Phi^*(\mu)"] & (\mathrm{Hom}_S(M, N))^{\sim} \arrow[d, "\mu"] \\ \Phi^*(\mathscr{H}om_{\mathscr{O}_{X'}}(\widetilde{M}', \widetilde{N}')) \arrow[r] & \mathscr{H}om_{\mathscr{O}_X}(\widetilde{M}, \widetilde{N}) \end{tikzcd} \tag{2.5.6}$$

is commutative (where the second row is the canonical homomorphism of (3.4.5)).

23.2.6 Closed subschemes of $\mathrm{Proj}(S)$

Recall that if $\varphi : S \to S'$ is a homomorphism of graded rings, we say that φ is eventually surjective (resp. eventually injective, eventually bijective) if $\varphi_i : S_i \to S'_i$ is surjective (resp. injective, bijective) for sufficiently large i. It follows from Proposition 23.2.18 that the study of Φ can be reduced to the case where φ is surjective (resp. injectij, bijective). Instead of saying that φ is eventually bijective, we also say that it is then an eventual isomorphism.

Proposition 23.2.50. *Let S, S' be graded rings with positive degrees and set $X = \mathrm{Proj}(S)$, $X' = \mathrm{Proj}(S')$.*

(a) If $\varphi : S \to S'$ is an eventually surjective homomorphism of graded rings, the corresponding

morphism Φ is defined over $\mathrm{Proj}(S')$ *and is a closed immersion. If $\mathfrak{I}$ is the kernel of φ, the closed subscheme of X associated with Φ is defined by the quasi-coherent ideal $\widetilde{\mathfrak{I}}$ of $\mathscr{O}_X$.*

(b) *Suppose moreover that the ideal S_+ is finitely generated by S_1. Let X' be a closed subscheme of X defined by a quasi-coherent ideal $\mathscr{I}$ of $\mathscr{O}_X$. Let $\mathfrak{I}$ be the graded ideal of S which is the inverse image of $\Gamma_*(\mathscr{I})$ under the canonical homomorphism $\alpha : S \to \Gamma_*(\mathscr{O}_X)$, and put $S' = S/\mathfrak{I}$. Then X' is the subscheme associated with the closed immersion* $\mathrm{Proj}(S') \to X$ *corresponding to the canonical homomorphism $S \to S'$ of graded rings.*

Proof. Let $\varphi : S \to S'$ be an eventually surjective homomorphism of graded rings. We can suppose that φ is surjective, so $\varphi(S_+)$ is generated by S'_+, we have $G(\varphi) = \mathrm{Proj}(S')$. Now the second assertion in (a) can be verified locally over X; let f be a homogeneous element of S_+ and put $f' = \varphi(f)$. As φ is a surjective homomorphism of rings, $\varphi_{(f')} : S_{(f)} \to S'_{(f')}$ is surjective with kernel $\mathscr{I}_{(f)}$, so the corresponding morphism is closed.

We now consider the case of (b); in view of (a), we only need to verify that the homomorphism $\tilde{j} : \widetilde{\mathscr{I}} \to \mathscr{O}_X$ induced from the injection $j : \mathscr{I} \to S$ is an isomorphism from $\widetilde{\mathscr{I}}$ to $\mathscr{I}$, which follows from Proposition 23.2.43(b). □

Remark 23.2.3. Note that $\mathfrak{I}$ is the largest graded ideal $\mathfrak{I}'$ of S such that $\widetilde{\mathscr{I}'} = \mathscr{I}$ (where we identify $\widetilde{\mathscr{I}'}$ as a subsheaf of $\mathscr{O}_X$), since one immedaitely verify that this relation implies $\alpha(\mathfrak{I}') \subseteq \Gamma_*(\mathscr{I})$.

Corollary 23.2.51. *Assume the hypotheses of Proposition 23.2.50(a) and that S_+ is generated by S_1. Then $\Phi^*(\widetilde{S(n)})$ is canonically isomorphic to $\widetilde{S'(n)}$ for any $n \in \mathbb{Z}$, and therefore $\Phi^*(\mathscr{F}(n))$ is isomorphic to $\Phi^*(\mathscr{F})(n)$ for any $\mathscr{O}_X$-module $\mathscr{F}$.*

Proof. This is a partiuclar case of Proposition 23.2.47, in view of the definition of $\mathscr{F}(n)$ and Proposition 23.2.50(a). □

Corollary 23.2.52. *Assume the hypotheses of Proposition 23.2.50(a). Then for the closed subscheme X' of X to be integral, it is necessary and sufficient that the graded ideal $\mathfrak{I}$ is prime in S.*

Proof. As X' is isomorphic to $\mathrm{Proj}(S/\mathfrak{I})$, this condition is sufficient in view of Proposition 23.2.16. To see the necessity, assume that $\mathrm{Proj}(S')$ is integral and consider the exact sequence $0 \to \mathscr{I} \to \mathscr{O}_X \to \mathscr{O}_X/\mathscr{I} \to 0$, which gives an exact sequence

$$0 \longrightarrow \Gamma_*(\mathscr{I}) \longrightarrow \Gamma_*(\mathscr{O}_X) \longrightarrow \Gamma_*(\mathscr{O}_X/\mathscr{I})$$

by the left-exactness of the global section functor. In view of the canonical homomorphism $\alpha : S/\mathfrak{I} \to \Gamma_*(\mathscr{O}_X/\mathscr{I})$, it then suffices to prove that if $f \in S_m$, $g \in S_n$ are such that the image in $\Gamma_*(\mathscr{O}_X/\mathscr{I})$ of $\alpha_{n+m}(fg)$ is zero, then one of the images of $\alpha_m(f)$, $\alpha_n(g)$ is zero. Now by definition, these images are sectins of the invertible $(\mathscr{O}_X/\mathscr{I})$-modules $\mathscr{L} = (\mathscr{O}_X/\mathscr{I})(m)$ and $\mathscr{L}' = (\mathscr{O}_X/\mathscr{I})(n)$ over the integral scheme X'. The hypotheses implies that their product is zero in $\mathscr{L} \otimes \mathscr{L}'$ (Corollary 23.2.29), so one of them is zero by Corollary 22.7.25. □

Corollary 23.2.53. *Let A be a ring, M be an A-module, and S be a graded A-algebra generated by S_1. Let $u : M \to S_1$ be a surjective homomorphism of A-modules and $\bar{u} : \boldsymbol{S}(M) \to S$ be the unique homomorphism of A-algebras extending u. Then the morphism corresponding to $\bar{u}$ is a closed immersion from* $\mathrm{Proj}(S)$ *to* $\mathrm{Proj}(\boldsymbol{S}(M))$.

Proof. The homomorphism $\bar{u}$ is surjective by hypothesis, so it suffices to apply Proposition 23.2.50. □

23.3 Homogeneous spectrum of sheaves of graded algebras

Let Y be a scheme and $\mathscr{S}$ be an $\mathscr{O}_Y$-algebra. We say that $\mathscr{S}$ is **graded** if $\mathscr{S}$ is the direct sum of a family $(\mathscr{S}_n)$ of $\mathscr{O}_Y$-algebras such that $\mathscr{S}_m\mathscr{S}_n \subseteq \mathscr{S}_{m+n}$. If $\mathscr{S}$ is a graded $\mathscr{O}_Y$-algebra, by a **graded $\mathscr{S}$-module** $\mathscr{M}$ we mean an $\mathscr{S}$-module $\mathscr{M}$ which is the direct sum of a family $(\mathscr{M}_n)_{n\in\mathbb{Z}}$ such that $\mathscr{S}_m\mathscr{M}_n \subseteq \mathscr{M}_{m+n}$. We say $\mathscr{S}$ is a graded $\mathscr{O}_Y$-algebra with positive degrees if $\mathscr{S}_n = 0$ for $n < 0$, and $\mathscr{M}$ is a graded $\mathscr{S}$-module if $\mathscr{M}_n = 0$ for $n < 0$. In this section, without further specifications, we will only consider graded algebras with positive degree.

23.3.1 Homogeneous spectrum of a graded $\mathscr{O}_Y$-algebra

Let $\mathscr{S}$ be a graded $\mathscr{O}_Y$-algebra (with positive degrees) and $\mathscr{M}$ be a graded $\mathscr{S}$-module. If $\mathscr{S}$ is quasi-coherent, each homogeneous component $\mathscr{S}_n$ is also a quasi-coherent $\mathscr{O}_Y$-module, since it is the image of $\mathscr{S}$ under the projection of $\mathscr{S}$ onto $\mathscr{S}_n$. Similarly, if $\mathscr{M}$ is quasi-coherent as an $\mathscr{O}_Y$-module, so is each of its homogeneous components, and the converse also holds. If $d > 0$ is an integer, we denote by $\mathscr{S}^{(d)}$ the direct sum of the $\mathscr{O}_Y$-modules $\mathscr{S}_{nd}$, which is quasi-coherent if $\mathscr{S}$ is; for any integer k such that $0 \leq k \leq d-1$, we denote by $\mathscr{M}^{(d,k)}$ (or $\mathscr{M}^{(d)}$ if $k = 0$) the direct sum of $\mathscr{M}_{nd+k}$ (for $n \in \mathbb{Z}$). If $\mathscr{S}$ and $\mathscr{M}$ are quasi-coherent sheaves, $\mathscr{M}(n)$ is a quasi-coherent $\mathscr{S}$-module by Proposition 22.2.22.

We say that $\mathscr{M}$ is a graded $\mathscr{S}$-module **of finite type** (resp. **of finite presentation**) if for any $y \in Y$, there exists an open neighborhood U of y and integers n_i (resp. integers m_i and n_i) such that there exists a surjective homomorphism $\bigoplus_{i=1}^r(\mathscr{S}(n_i)|_U) \to \mathscr{M}|_U$ of degree 0 (resp. such that $\mathscr{M}|_U$ is isomorphic to the cokernel of a homomorphism $\bigoplus_{i=1}^r \mathscr{S}(m_i)|_U \to \bigoplus_{j=1}^r \mathscr{S}(n_j)|_U$ of degree 0).

Let U be an affine open of Y and $A = \Gamma(U, \mathscr{O}_Y)$ by its ring. By hypothesis, the graded $(\mathscr{O}_Y|_U)$-algebra $\mathscr{S}|_U$ is isomorphic to $\widetilde{S}$ where $S = \Gamma(U, \mathscr{S})$ is a graded A-algebra; we put $X_U = \mathrm{Proj}(\Gamma(U, \mathscr{S}))$. Let $U' \subseteq U$ be another affine open subset of Y and $j : U' \to U$ the canonical injection, which corresponds to a homomorphism $A \to A'$, we have $\mathscr{S}|_{U'} = j^*(\mathscr{S}|_U)$, and therefore $S' = \Gamma(U', \mathscr{S})$ is identified with $S \otimes_A A'$ by Proposition 22.1.13. We then conclude from Proposition 23.2.48 that $X_{U'}$ is canonically identified with $X_U \times_U U'$, and therefore with $p_U^{-1}(U')$, where p_U is the structural morphism $X_U \to U$. Let $\sigma_{U',U}$ be the canonical isomorphism $p_U^{-1}(U') \cong X_{U'}$ thus defined, and $\rho_{U',U}$ be the open immersion $X_{U'} \to X_U$ obtained by composing $\sigma_{U',U}^{-1}$ with the canonical injectin $p_U^{-1}(U') \to X_U$. It is immediate that if $U'' \subseteq U'$ is a third affine open of Y, we have $\rho_{U'',U} = \rho_{U'',U'} \circ \rho_{U',U}$.

Proposition 23.3.1. *Let Y be a scheme and $\mathscr{S}$ be a quasi-coherent graded $\mathscr{O}_Y$-algebra. Then there exists a unique scheme X over Y such that, if $p : X \to Y$ is the structural morphism, for any affine open U of Y, there exists an isomorphism $\eta_U : p^{-1}(U) \xrightarrow{\sim} X_U = \mathrm{Proj}(\Gamma(U, \mathscr{S}))$ such that, if V is another affine*

open of Y contained in U, the following diagram

$$\begin{tikzcd} p^{-1}(V) \arrow[r, "\eta_V"] \arrow[d] & X_V \arrow[d, "\rho_{V,U}"] \\ p^{-1}(U) \arrow[r, "\eta_U"] & X_U \end{tikzcd}$$

is commutative. The scheme X is called the ***homogeneous specturm*** *of the quasi-coherent $\mathscr{O}_Y$-algebra $\mathscr{S}$ and denoted by* $\mathrm{Proj}(\mathscr{S})$.

Proof. For two affine opens U, V of Y, let $X_{U,V}$ be the scheme induced over $p_U^{-1}(U \cap V)$ by X_U; we shall define a Y-isomorphism $\theta_{U,V} : X_{V,U} \to X_{U,V}$. For this, consider an affine open $W \subseteq U \cap V$; by composing the isomorphisms

$$p_U^{-1}(W) \xrightarrow{\sigma_{W,U}} X_W \xrightarrow{\sigma_{W,V}^{-1}} p_V^{-1}(W)$$

we obtain an isomorphism $\tau_W : p_U^{-1}(W) \to p_V^{-1}(W)$, and we can verify that if $W' \subseteq W$ is an affine open, $\tau_{W'}$ is the restriction of τ_W to $p_U^{-1}(W')$; the morphisms τ_W then glue together to a Y-isomorphism $\theta_{V,U}$, which is what we want. Moreover, if U, V, W are affine opens of Y and $\theta'_{U,V}$, $\theta'_{V,W}$, and $\theta'_{U,W}$ are restrictions of $\theta_{U,V}, \theta_{V,W}, \theta_{U,W}$ on the inverse images of $U \cap V \cap W$ in X_V, X_W, X_W, respectively, it follows from the preceding definition that $\theta'_{U,V} \circ \theta'_{V,W} = \theta'_{U,W}$. The existence of X then follows from glueing these schemes via the isomorphisms $\theta_{U,V}$, and the uniqueness is clear. □

It is clear that the Y-scheme $\mathrm{Proj}(\mathscr{S})$ is separated over Y since homogeneous specturms are separated. If $\mathscr{S}$ is an $\mathscr{O}_Y$-algebra of finite type, it follows from Proposition 23.2.35 and Proposition 22.6.33 that $\mathrm{Proj}(\mathscr{S})$ is of finite type over Y. If $p : X \to Y$ is the structural morphism, it is immediate that for any open subschem U of Y, $p^{-1}(U)$ is identified with the homogeneous specturm $\mathrm{Proj}(\mathscr{S}|_U)$.

Proposition 23.3.2. *Let $f \in \Gamma(Y, \mathscr{S}_d)$ with $d > 0$ and $X = \mathrm{Proj}(\mathscr{S})$. Then there exists an open subset X_f of X such that, for any affine open subset U of Y, we have $X_f \cap p^{-1}(U) = D_+(f|_U)$ in $X_U = \mathrm{Proj}(\Gamma(U, \mathscr{S}))$ (where $p : X \to Y$ is the structural morphism). Moreover, the Y-scheme induced over X_f by X is canonically isomorphic to* $\mathrm{Spec}(\mathscr{S}^{(d)}/(f-1)\mathscr{S}^{(d)})$.

Proof. For any affine open U, we have $f|_U \in \Gamma(U, \mathscr{S}_d) = \Gamma(U, \mathscr{S})_d$ since U is quasi-compact. If U, U' are two affine opens of Y such that $U' \subseteq U$, $f|_{U'}$ is the image of $f|_U$ by the restriction homomorphism $\Gamma(U, \mathscr{S}) \to \Gamma(U', \mathscr{S})$, so $D_+(f|_{U'})$ is equal to the open subscheme $\rho_{U',U}^{-1}(D_+(f|_U))$ of $X_{U'}$. The subset X_f can be then defined by glueing these subschemes, and the first assertion is then obvious. On the other hand, the open subscheme $D_+(f|_U)$ of X_U is canonically identified with $\mathrm{Spec}(\Gamma(U, \mathscr{S})_{(f|_U)})$, and this identification is clearly compatible with restrictions; the second assertion then follows from Proposition 23.2.3. □

Corollary 23.3.3. *If $f \in \Gamma(Y, \mathscr{S}_d)$ and $g \in \Gamma(Y, \mathscr{S}_e)$, we have $X_{fg} = X_f \cap X_g$.*

Proof. It suffices to consider the intersection of two members of $p^{-1}(U)$, where U is an affine open of Y, and the assertion follows from $D_+(fg) = D_+(f) \cap D_+(g)$ for a graded ring S. □

Corollary 23.3.4. *Let (f_α) be a family of sections of $\mathcal{S}$ over Y such that $f_\alpha \in \Gamma(Y, \mathcal{S}_{d_\alpha})$. If the sheaf of ideals of $\mathcal{S}$ generated by this family containes all the $\mathcal{S}_n$ for sufficiently large n, then the underlying space X is the union of X_{f_α}.*

Proof. In fact, for any affine open U of Y, $p^{-1}(U)$ is the union of $X_{f_\alpha} \cap p^{-1}(U)$ by Corollary 23.2.11, so the claim follows from the construction of X_{f_α}. □

Corollary 23.3.5. *Let $\mathcal{A}$ be a quasi-coherent $\mathcal{O}_Y$-algebra and put*

$$\mathcal{S} = \mathcal{A}[T] = \mathcal{A} \otimes_{\mathbb{Z}} \mathbb{Z}[T]$$

where T is an indeterminate. Then $X = \mathrm{Proj}(\mathcal{S})$ is canonically identified with $\mathrm{Spec}(\mathcal{A})$. In particular, $\mathrm{Proj}(\mathcal{O}_Y[T])$ is identified with Y.

Proof. By applying Corollary 23.3.4 to the unique section $f \in \Gamma(Y, \mathcal{S})$ equal to T on each point of Y, we see that $X_f = X$. Moreover, we have $f \in \mathcal{S}_1$, and $\mathcal{S}^{(1)}/(f-1)\mathcal{S}^{(1)} = \mathcal{S}/(f-1)\mathcal{S}$ is canonically isomorphic to $\mathcal{A}$, whence the corollary □

Let $g \in \Gamma(Y, \mathcal{O}_Y)$; if we put $\mathcal{S} = \mathcal{O}_Y[T]$, then $g \in \Gamma(Y, \mathcal{S}_0)$; let

$$h = gT \in \Gamma(Y, \mathcal{S}_1).$$

If $X = \mathrm{Proj}(\mathcal{S})$, the canonical identification of Corollary 23.3.5 identifies X_h with the open subset Y_g of Y: in fact, we can assume that $Y = \mathrm{Spec}(A)$ is affine, and this then follows from the fact that the ring A_g is canonically identified with $A[T]/(gT-1)A[T]$.

Proposition 23.3.6. *Let $\mathcal{S}$ be a quasi-coherent graded $\mathcal{O}_Y$-algebra.*

(a) For any $d > 0$, there exists a canonical Y-isomorphism from $\mathrm{Proj}(\mathcal{S})$ to $\mathrm{Proj}(\mathcal{S}^{(d)})$.

(b) Let $\mathcal{S}'$ be the graded $\mathcal{O}_Y$-algebra $\mathcal{O}_Y \oplus \bigoplus_{n>0} \mathcal{S}_n$, then the schemes $\mathrm{Proj}(\mathcal{S}')$ and $\mathrm{Proj}(\mathcal{S})$ are canonically Y-isomorphic.

(c) Let $\mathcal{L}$ be an invertible $\mathcal{O}_Y$-module and $\mathcal{S}_{(\mathcal{L})}$ be the graded $\mathcal{O}_Y$-algebra $\bigoplus_{d>0} \mathcal{S}_d \otimes \mathcal{L}^{\otimes d}$; then the schemes $\mathrm{Proj}(\mathcal{S})$ and $\mathrm{Proj}(\mathcal{S}_{(\mathcal{L})})$ are canonically Y-isomorphic.

Proof. In all three cases, it suffices to define an isomorphism locally over Y and verifying the compatibility of restriction morphisms is immediate. We can then assume that Y is affine, and assertions (a) and (b) then follow from Proposition 23.2.18. As for (c), if the invertible sheaf $\mathcal{L}$ is just isomorphic to $\mathcal{O}_Y$ then the isomorphism between $\mathrm{Proj}(\mathcal{S})$ and $\mathrm{Proj}(\mathcal{S}_{(\mathcal{L})})$ is evident. To define a canonical isomorphism, let $Y = \mathrm{Spec}(A)$, $\mathcal{S} = \widetilde{S}$, where S is a graded A-algebra, and let c be a generator of the free A-module L such that $\mathcal{L} = \widetilde{L}$. Then for any $n > 0$, $x_n \mapsto x_n \otimes c^{\otimes n}$ is an A-isomorphism from S_n to $S_n \otimes L^{\otimes n}$, and these A-isomorphisms define an A-isomorphism of graded algebras

$$p_c : S \to S_{(L)} = \bigoplus_{n \geq 0} S_n \otimes L^{\otimes n}.$$

Let $f \in S_+$ be homogeneous of degree d; for any $x \in S_{nd}$, we have $(x \otimes c^{nd})/(f \otimes c^d)^n = (x \otimes (\varepsilon c)^{nd})/(f \otimes (\varepsilon c)^d)^n$ for any invertible element $\varepsilon \in A$, which implies that the isomorphism $S_{(f)} \to (S_{(L)})_{(f \otimes c^d)}$ induced by p_c is independent from the generator c of L, whence the assertion. □

Recall that for the quasi-coherent graded $\mathscr{O}_Y$-algebra $\mathscr{L}$ to be *generated* by the $\mathscr{O}_Y$-module $\mathscr{S}_1$, it is necessary and sufficient that there exists a covering (U_α) of Y by affine opens such that the graded algebra $\Gamma(U_\alpha, \mathscr{S})$ over $\Gamma(U_\alpha, \mathscr{S}_0)$ is generated by $\Gamma(U_\alpha, \mathscr{S}_1)$. If this is true, then for any open subset V of Y, $\mathscr{S}|_V$ is then generated by $(\mathscr{O}_Y|_V)$-algebra $\mathscr{S}_1|_V$.

Proposition 23.3.7. *Suppose that there exists a finite affine open cover (U_i) of Y such that the graded algebra $\Gamma(U_i, \mathscr{S})$ is of finite type over $\Gamma(U_i, \mathscr{O}_Y)$. Then there exists $d > 0$ such that $\mathscr{S}^{(d)}$ is generated by $\mathscr{S}_d$, which is an $\mathscr{O}_Y$-module of finite type.*

Proof. In fact, it follows from Corollary 11.1.38 that for each i, there exist an integer m_i such that $\Gamma(U_i, \mathscr{S}_{nm_i}) = (\Gamma(U_i, \mathscr{S}_{m_i}))^n$ for all $n > 0$; it suffices to take d a common multiple of the m_i. □

Corollary 23.3.8. *Under the hypotheses of Proposition 23.3.7,* $\operatorname{Proj}(\mathscr{S})$ *is Y-isomorphic to a homogeneous specturm* $\operatorname{Proj}(\mathscr{S}')$*, where $\mathscr{S}'$ is a graded $\mathscr{O}_Y$-algebra generated by $\mathscr{S}'_1$, where $\mathscr{S}'$ is an $\mathscr{O}_Y$-algebra of finite type.*

Proof. It suffices to take $\mathscr{S}' = \mathscr{S}^{(d)}$, where d is determined by the properties of Proposition 23.3.7, and apply Proposition 23.3.6(a). □

If $\mathscr{S}$ is a quasi-coherent graded $\mathscr{O}_Y$-algebras, we have seen in Proposition 22.4.25 that its nilradical is a quasi-coherent $\mathscr{O}_Y$-module. We say that $\mathscr{N}_+ = \mathscr{N} \cap \mathscr{S}_+$ is the nilradical of $\mathscr{S}_+$, which is a quasi-coherent graded $\mathscr{S}_0$-module, since this is the case if Y is affine. For any $y \in Y$, $(\mathscr{N}_+)_y$ is then the nilradical of $(\mathscr{S}_+)_y = (\mathscr{S}_y)_+$. Similar to the local case, we say the graded $\mathscr{O}_Y$-algebra $\mathscr{S}$ is **essentially reduced** if $\mathscr{N}_+ = 0$, which means $\mathscr{S}_y$ is an essentially reduced graded $\mathscr{O}_{Y,y}$-algebra for any $y \in Y$. It is clear that for any quasi-coherent graded $\mathscr{O}_Y$-algebra $\mathscr{S}$, $\mathscr{S}/\mathscr{N}_+$ is essentially reduced. Finally, we say $\mathscr{S}$ is **integral** if $\mathscr{S}_y$ is an integral ring for each $y \in Y$ and if $(\mathscr{S}_+)_y = (\mathscr{S}_y))_+ \neq 0$ for all $y \in Y$.

Proposition 23.3.9. *Let $\mathscr{S}$ be a graded $\mathscr{O}_Y$-algebra. If $X = \operatorname{Proj}(\mathscr{S})$, the Y-scheme X_{red} is canonically isomorphic to* $\operatorname{Proj}(\mathscr{S}/\mathscr{N}_+)$*. In particular, if $\mathscr{S}$ is essentially reduced, then X is reduced.*

Proof. The fact that $X' = \operatorname{Proj}(\mathscr{S}/\mathscr{N}_+)$ is reduced follows from Proposition 23.2.16, since the question is local. Moreover, for any affine open $U \subseteq Y$, $p'^{-1}(U)$ is equal to $(p^{-1}(U))_{\mathrm{red}}$ (where p and p' are the structural morphisms $X \to Y$, $X' \to Y$, respectively); we also verify t hat the canonical U-morphisms $p'^{-1}(U) \to p^{-1}(U)$ is compatible with restrictions and define therefore a closed immersion $X' \to X$, which is a homeomorphism on underlying spaces. Our assertion then follows from Corollary 22.4.26. □

Proposition 23.3.10. *Let Y be an integral scheme and $\mathscr{S}$ be a quasi-coherent graded $\mathscr{O}_Y$-algebra such that $\mathscr{S}_0 = \mathscr{O}_Y$.*

(a) If $\mathscr{S}$ is integral then $X = \operatorname{Proj}(\mathscr{S})$ is integral and the structural morphism $p : X \to Y$ is dominant.

(b) Suppose moreover that $\mathscr{S}$ is essentially reduced. Then, conversely, if X is integral and p is dominant, then $\mathscr{S}$ is integral.

Proof. We first assume that $\mathscr{S}$ is integral. Then if (U_α) is a basis of Y formed by affine opens, it suffices to prove for Y being replaced by U_α and $\mathscr{S}$ by $\mathscr{S}|_{U_\alpha}$: in fact, is this is true, the underlying space $p^{-1}(U_\alpha)$ is an open irreducible subset of X such that $p^{-1}(U_\alpha) \cap p^{-1}(U_\beta) \neq \varnothing$ for any couple of indices α, β (since $U_\alpha \cap U_\beta$ contains an U_γ and $\mathscr{S}$ is integral), so X is irreducible by Proposition 4.1.5; it is clear that X is reduced since $\mathscr{S}$ is reduced, so X is integral. It is clear that $p(X)$ is dense in Y since this holds for each U_α.

Suppose then that $Y = \operatorname{Spec}(A)$ where A is integral (Proposition 22.4.27) and $\mathscr{S} = \widetilde{S}$, where S is a graded A-algebra; the hypotheses on $\mathscr{S}$ is that for any $y \in Y$, $\widetilde{S}_y = S_y$ is an integral graded ring such that $(S_y)_+ \neq 0$. It then suffices to prove that S is an integral ring, since then $S_+ \neq 0$ and we can apply Proposition 23.2.16. Now, let f, g be two nonzero elements of S and suppose that $fg = 0$; for any $y \in Y$ we have $(f/1)(g/1) =$ in S_y, so $f/1 = 0$ or $g/1 = 0$ by hypothesis. Suppose for example that $f/1 = 0$ in S_y, so there exists $a \in A$ such that $a \notin \mathfrak{p}_y$ and $af = 0$. We then see that for each $z \in Y$, $(a/1)(f/1) = 0$ in the integral ring S_z, and as $a/1 \neq 0$ (since A is integral), $f/1 = 0$, which implies $f = 0$.

Now consider the hypothesis in (b) and assume that X is integral and p is dominant. Since the question is local over Y, we can assume that $Y = \operatorname{Spec}(A)$, where A is an integral ring, and $\mathscr{S} = \widetilde{S}$. By hypothesis for any $y \in Y$, $(S_y)_+$ is reduced, and so is $(S_0)_y = A_y$ by hypothesis, so S_y is a reduced ring and we conclude that S is reduced. The hypothesis that X is integral implies that S is essentially integral (Proposition 23.2.16). The proposition then boils down to see that the annihilator $\mathfrak{I}$ of S_+ over $A = S_0$ is reduced to zero. In the contrary case, we would have $(S_h)_+ = 0$ for an $h \neq 0$ in $\mathfrak{I}$, which implies $p^{-1}(D(h)) = \varnothing$ by Proposition 23.3.1, and $p(X)$ is then not dense in Y, contradicting the hypothesis (since $D(h) \neq \varnothing$, h is not nilpotent). We then see that the ring S is integral, which conclude our assertion. □

23.3.2 Sheaves associated with a graded $\mathscr{S}$-module

Let Y be a scheme, $\mathscr{S}$ be a quasi-coherent $\mathscr{O}_Y$-algebra, and $\mathscr{M}$ be a quasi-coherent graded $\mathscr{S}$-module over the ringed space $(Y, \mathscr{S})$. With the notations of Proposition 23.3.1, we denote by $\widetilde{\mathscr{M}}_U$ the quasi-coherent $\mathscr{O}_{X_U}$-module $\widetilde{\Gamma(U, \mathscr{M})}$. For $U' \subseteq U$, $\Gamma(U', \mathscr{M})$ is canonically identified with $\Gamma(U, \mathscr{M}) \otimes_A A'$ by Proposition 22.1.13, so $\widetilde{M}_{U'} = \rho^*_{U',U}(\widetilde{\mathscr{M}}_U)$ by Proposition 23.2.48.

Proposition 23.3.11. *There exists over* $\operatorname{Proj}(\mathscr{S}) = X$ *a unique quasi-coherent* $\mathscr{O}_X$*-module* $\widetilde{\mathscr{M}}$ *such that, for any affine open* U *of* Y*, we have* $\eta^*_U(\widetilde{\mathscr{M}}_U) = \widetilde{\mathscr{M}}|_{p^{-1}(U)}$*, where* $p : X \to Y$ *is the structural morphism and* η_U *is the isomorphism* $p^{-1}(U) \cong \operatorname{Proj}(\Gamma(U, \mathscr{S}))$*. We say that* $\widetilde{\mathscr{M}}$ *is the* $\mathscr{O}_X$*-module associated with* $\mathscr{M}$*.*

Proof. As $\rho_{U',U}$ is identified with the injection morphism $p^{-1}(U') \to p^{-1}(U)$, the proposition follows from the relation $\widetilde{M}_{U'} = \rho^*_{U',U}(\widetilde{\mathscr{M}}_U)$ and glueing the $\widetilde{\mathscr{M}}_U$. □

Proposition 23.3.12. *Let* $\mathscr{M}$ *be a quasi-coherent* $\mathscr{S}$*-module and* $f \in \Gamma(Y, \mathscr{S}_d)$ *with* $d > 0$*. If* ξ_f *is the canonical isomorphism from* X_f *to the* Y*-scheme* $Z_f = \operatorname{Spec}(\mathscr{S}^{(d)}/(f-1)\mathscr{S}^{(d)})$ *in Proposition 23.3.2, then* $(\xi_f)_*(\widetilde{\mathscr{M}}|_{X_f})$ *is the* $\mathscr{O}_{Z_f}$*-module* $(\mathscr{M}^{(d)}/(f-1)\mathscr{M}^{(d)})^{\sim}$*.*

Proof. The question is local over Y we we are reduced to Proposition 23.2.3, and its compatibility with restrictions. □

Proposition 23.3.13. *The $\mathscr{O}_X$-module $\widetilde{\mathscr{M}}$ is an additive exact covariant functor from the category of quasi-coherent graded $\mathscr{S}$-modules to the category of quasi-coherent $\mathscr{O}_X$-modules, which commutes with direct sums and inductive limits.*

Proof. This follows from Corollary 22.1.6 and Proposition 23.2.34, since the question is local on Y. □

In particular, if $\mathscr{N}$ is a quasi-coherent graded sub-$\mathscr{S}$-module of $\mathscr{M}$, $\widetilde{\mathscr{N}}$ is cannically identified with a quasi-coherent sub-$\mathscr{O}_X$-module of $\widetilde{\mathscr{M}}$; if we take $\mathscr{M} = \mathscr{S}$, then for any quasi-coherent ideal $\mathscr{I}$ of $\mathscr{S}$, $\widetilde{\mathscr{I}}$ is a quasi-coherent ideal of $\mathscr{O}_X$.

If $\mathscr{M}$ is a quasi-coherent graded $\mathscr{S}$-module and $\mathscr{I}$ is a quasi-coherent ideal of $\mathscr{O}_Y$, then $\mathscr{I}\mathscr{M}$ is a quasi-coherent graded sub-$\mathscr{S}$-module of $\mathscr{M}$ and we have $\widetilde{\mathscr{I}\mathscr{M}} = \mathscr{I} \cdot \widetilde{\mathscr{M}}$: it suffices to verify this formula if $Y = \operatorname{Spec}(A)$, $\mathscr{S} = \widetilde{S}$, where S is a graded A-algebra, $\mathscr{M} = \widetilde{M}$ where M is a graded S-module, and $\mathscr{I} = \widetilde{\mathfrak{a}}$, where $\mathfrak{a}$ is an ideal of A. For any homogeneous element f of S_+, the restriction to $D_+(f) = \operatorname{Spec}(S_{(f)})$ of $\widetilde{\mathscr{I}\mathscr{M}}$ is the assocaited sheaf of $(\mathfrak{a}M)_{(f)} = \mathfrak{a} \cdot M_{(f)}$, and the identification is compatible with restrictions.

Proposition 23.3.14. *Let $f \in \Gamma(Y, \mathscr{S}_d)$ with $d > 0$. Over the open subset X_f, the $(\mathscr{O}_X|_{X_f})$-module $\widetilde{\mathscr{S}(nd)}|_{X_f}$ is canonically isomorphic to $\mathscr{O}_X|_{X_f}$ for any $n \in \mathbb{Z}$. In particular, if the $\mathscr{O}_Y$-algebra $\mathscr{S}$ is generated by $\mathscr{S}_1$, the $\mathscr{O}_X$-module $\widetilde{\mathscr{S}(n)}$ is invertible for all $n \in \mathbb{Z}$.*

Proof. For any affine open U of Y, by Proposition 23.2.24 we have a canonical isomorphism $\widetilde{\mathscr{S}(nd)}|_{X_f \cap p^{-1}(U)} \cong \mathscr{O}_X|_{X_f \cap p^{-1}(U)}$, in view of Proposition 23.3.2 (where $p : X \to Y$ is the structural morphism). It is immediate that this isomorphism is compatible with restrictions, whence the first assertion. For the second one, if $\mathscr{S}$ is generated by $\mathscr{S}_1$, there exists an affine open cover (U_α) of Y such that $\Gamma(U_\alpha, \mathscr{S})$ is generated by $\Gamma(U_\alpha, \mathscr{S}_1) = \Gamma(U_\alpha, \mathscr{S})_1$, and we can then use Corollary 23.2.26. □

Again, for any integer $n \in \mathbb{Z}$ and any $\mathscr{O}_X$-module $\mathscr{F}$, we set

$$\mathscr{O}_X(n) = \widetilde{\mathscr{S}(n)}, \quad \mathscr{F}(n) = \mathscr{F} \otimes_{\mathscr{O}_X} \mathscr{O}_X(n).$$

It follows from this definition that, for any open subset U of Y,

$$\widetilde{\mathscr{S}|_U(n)} = \mathscr{O}_X|_{p^{-1}(U)},$$

where $p : X \to Y$ is the structural morphism.

Proposition 23.3.15. *Let $\mathscr{M}$ and $\mathscr{N}$ be quasi-coherent graded $\mathscr{S}$-modules. Then there exists cannical homomorphisms*

$$\lambda : \widetilde{M} \otimes_{\mathscr{O}_X} \widetilde{\mathscr{N}} \to (\mathscr{M} \otimes_{\mathscr{S}} \mathscr{N})^{\sim}$$
$$\mu : (\mathscr{H}om_{\mathscr{S}}(\mathscr{M}, \mathscr{N}))^{\sim} \to \mathscr{H}om_{\mathscr{O}_X}(\widetilde{\mathscr{M}}, \widetilde{\mathscr{N}}).$$

If $\mathscr{S}$ is generated by $\mathscr{S}_1$, then λ is an isomorphism; if moreover $\mathscr{M}$ is of finite presentation, μ is an isomorphism.

Proof. The isomorphisms λ and μ are defined in the arguments before Proposition 23.2.28 if Y is affine, and this definition is local and then glue together to define global morphisms, in view of the diagrams (2.5.5) and (2.5.6). □

Corollary 23.3.16. *If $\mathscr{S}$ is generated by $\mathscr{S}_1$, for any integers $m, n \in \mathbb{Z}$, we have*

$$\mathscr{O}_X(m) \otimes_{\mathscr{O}_X} \mathscr{O}_X(n) = \mathscr{O}_X(m+n), \quad \mathscr{O}_X(n) = \mathscr{O}_X^{\otimes 1}.$$

Corollary 23.3.17. *If $\mathscr{S}$ is generated by $\mathscr{S}_1$, for any quasi-coherent graded $\mathscr{S}$-module $\mathscr{M}$ and $n \in \mathbb{Z}$, we have*

$$\widetilde{\mathscr{M}(n)} = \widetilde{\mathscr{M}}(n).$$

Remark 23.3.1. If $\mathscr{S} = \mathscr{A}[T]$ where $\mathscr{A}$ is a quasi-coherent $\mathscr{O}_Y$-algebra, we verify immediately that the invertible $\mathscr{O}_X$-module $\mathscr{O}_X(n)$ is canonically isomorphic to $\mathscr{O}_X$. Moreover, let $\mathscr{N}$ be a quasi-coherent $\mathscr{A}$-module, and put $\mathscr{M} = \mathscr{N} \otimes_{\mathscr{A}} \mathscr{A}[T]$. It follows from Proposition 23.3.12 and Corollary 23.3.5 that under the canonical isomorphism of $X = \mathrm{Proj}(\mathscr{A}[T])$ and $X' = \mathrm{Spec}(\mathscr{A})$, the $\mathscr{O}_X$-module $\widetilde{\mathscr{M}}$ is identified with the $\mathscr{O}_X$-module $\widetilde{\mathscr{N}}$.

Remark 23.3.2. Let $\mathscr{S}$ be a quasi-coherent graded $\mathscr{O}_Y$-algebra and define $\mathscr{S}'$ to be the $\mathscr{O}_Y$-algebra such that $\mathscr{S}' = \mathscr{O}_Y$ and $\mathscr{S}'_n = \mathscr{S}_n$ for $n > 0$. Then the canonical isomorphism of $X = \mathrm{Proj}(\mathscr{S})$ and $\mathrm{Proj}(\mathscr{S}')$ identifies $\mathscr{O}_X(n)$ and $\mathscr{O}_{X'}(n)$ for any $n \in \mathbb{Z}$: this follows from the corresponding result in the affine case (Example 23.2.31) and the fact that this identification is compatible with restrictions. Similarly, let $X^{(d)} = \mathrm{Proj}(\mathscr{S}^{(d)})$; the canonical isomorphism of X and $X^{(d)}$ identifies $\mathscr{O}_X(nd)$ with $\mathscr{O}_{X^{(d)}}(n)$ for any $n \in \mathbb{Z}$.

Proposition 23.3.18. *Let $\mathscr{L}$ be an invertible $\mathscr{O}_Y$-module and ψ be the structural morphism from $X_{(\mathscr{L})} = \mathrm{Proj}(\mathscr{S}_{(\mathscr{L})})$ to $X = \mathrm{Proj}(\mathscr{S})$. Then for any integer $n \in \mathbb{Z}$, $\psi_*(\mathscr{O}_{X_{(\mathscr{L})}}(n))$ is canonically isomorphic to $\mathscr{O}_X(n) \otimes_Y \mathscr{L}^{\otimes n}$.*

Proof. Suppose first that Y is affine with ring A and $\mathscr{L} = \widetilde{L}$, where L is a free A-module of rank 1. With the notations of Proposition 23.3.6(c), we define for each $f \in S_d$ an isomorphism from $S(n)_{(f)} \otimes_A L^{\otimes n}$ to $S_{(L)}(n)_{(f \otimes c^d)}$ which sends $(x/f^k) \otimes c^n$, where $x \in S_{kd+n}$, to the element $(x \otimes c^{n+kd})/(f \otimes c^d)^k$. It is immedaite that this isomorphism is independent of the generator c of L, and is compatible with restrictions $D_+(f) \to D_+(fg)$. The general case then follows from glueing these isomorphisms. □

23.3.3 Graded $\mathscr{S}$-module assocaited with a sheaf

For simplicity, in the following discussion, we always assume that the quasi-coherent $\mathscr{O}_Y$-algebra $\mathscr{S}$ is generated by $\mathscr{S}_1$, which by Proposition 23.3.6 is not at all essential if we impose the finiteness conditions of Proposition 23.3.7 on Y. Let $p : X \to Y$ be the structural morphism where $X = \mathrm{Proj}(\mathscr{S})$, which is separated by Proposition 23.2.14. For any $\mathscr{O}_X$-module $\mathscr{F}$, we define

$$\Gamma_*(\mathscr{F}) = \bigoplus_{n \in \mathbb{Z}} p_*(\mathscr{F}(n))$$

and in particular

$$\Gamma_*(\mathscr{O}_X) = \bigoplus_{n \in \mathbb{Z}} p_*(\mathscr{O}_X(n)).$$

We have seen in (3.2.1) that there exists a canonical homomorphism

$$p_*(\mathscr{F}) \otimes_{\mathscr{O}_Y} p_*(\mathscr{G}) \to p_*(\mathscr{F} \otimes_{\mathscr{O}_X} \mathscr{G})$$

for any $\mathscr{O}_X$-modules $\mathscr{F}$ and $\mathscr{G}$, so we deduce from Corollary 23.3.16 that $\Gamma_*(\mathscr{O}_X)$ is endowed with a graded $\mathscr{O}_Y$-algebra structure and $\Gamma_*(\mathscr{F})$ is a graded module over $\Gamma_*(\mathscr{O}_X)$.

In view of Proposition 23.3.14 and the left-exactness of the functor f_*, $\Gamma_*(\mathscr{F})$ is an additive left-exact covariant functor from the category of $\mathscr{O}_X$-modules to the category of graded $\mathscr{O}_Y$-modules. In particular, if $\mathscr{I}$ is a sheaf of ideals of $\mathscr{O}_X$, $\Gamma_*(\mathscr{I})$ is identified with a sheaf of graded ideals of $\Gamma_*(\mathscr{O}_X)$.

Now let $\mathscr{M}$ be a quasi-coherent graded $\mathscr{S}$-module. For any affine open U of Y, we have defined a homomorphism of abelian groups

$$\alpha_{0,U} : \Gamma(U, \mathscr{M}_0) \to \Gamma(p^{-1}(U), \widetilde{\mathscr{M}}).$$

It is immediate that these homomorphisms commutes with restrictions and define (which do not use the hypothesis that $\mathscr{S}$ is generated by $\mathscr{S}_1$) a homomorphism of sheaf of abelian groups

$$\alpha_0 : \mathscr{M}_0 \to \widetilde{\mathscr{M}}.$$

Apply this result to $\mathscr{M}_n = (\mathscr{M}(n))_0$ and use Corollary 23.3.17, we define a homomorphism of abelian groups

$$\alpha_n : \mathscr{M}_n \to p_*(\widetilde{\mathscr{M}}(n)) \tag{3.3.1}$$

for each $n \in \mathbb{Z}$, whence a functorial homomorphism of graded sheaves of abelian groups

$$\alpha : \mathscr{M} \to \Gamma_*(\widetilde{\mathscr{M}}) \tag{3.3.2}$$

(we also denote it by $\alpha_{\mathscr{M}}$). In the particular case $\mathscr{M} = \mathscr{S}$, we verify that $\alpha : \mathscr{S} \to \Gamma_*(\mathscr{O}_X)$ is a homomorphism of graded $\mathscr{O}_Y$-algebra and is a bi-homomorphism of graded modules, relative to this homomorphism of graded homomorphism of algebras.

We also remark that the homomorphism α_n corresponds to a canonical homomorphism of $\mathscr{O}_X$-modules

$$\alpha_n^\sharp : p^*(\mathscr{M}_n) \to \widetilde{\mathscr{M}}(n).$$

Moreover, it is easy to verify that this homomorphism is none other than the associated homomorphism (by Proposition 23.3.13) of the canonical homomorphism $\mathscr{M}_n \otimes_{\mathscr{O}_Y} \mathscr{S} \to \mathscr{M}(n)$ of $\mathscr{O}_Y$-modules, where the $\mathscr{O}_Y$-module $\mathscr{M}_n \otimes_{\mathscr{O}_Y} \mathscr{S}$ is given the natrual graduation. To see this, we can in fact assume that $Y = \operatorname{Spec}(A)$ is affine, $\mathscr{M} = \widetilde{M}$ and $\mathscr{S} = \widetilde{S}$, where S is a graded A-algebra generated by S_1. Returning to the definition of α, we see that the restriction to $D_+(f)$ of the homomorphism $\alpha_n^\sharp$ corresponds to the homomorphism $M_n \otimes_A S_{(f)} \to M(n)_{(f)}$, where $x \otimes 1$ is maped to $x/1$.

Proposition 23.3.19. *For any section $f \in \Gamma(Y, \mathscr{S}_d)$ with $d > 0$, X_f is identified with the set of points of X on which $\alpha_d(f)$ is nonzero.*

Proof. The element $\alpha_d(f)$ is a section of $p_*(\mathscr{O}_X(d))$ over Y, and by definition is then a section of $\mathscr{O}_X(d)$ over X. The definition of X_f (Proposition 23.3.2) proves our claim in the affine case, in view of Proposition 23.2.33. □

We shall henceforth suppose, in addition to the hypothesis at the beginning of this part, that for every quasi-coherent $\mathscr{O}_X$-module $\mathscr{F}$, $p_*(\mathscr{F}(n))$ is quasi-coherent over Y, and therefore

$\Gamma_*(\mathscr{F}) = \bigoplus_{n\in\mathbb{Z}} p_*(\mathscr{F}(n))$ is also a quasi-coherent $\mathscr{O}_Y$-module; this circumstance will always occur if X is of finite type on Y (Proposition 22.6.54). We then conclude that $\widetilde{\Gamma_*(\mathscr{F})}$ is defined and is a quasi-coherent $\mathscr{O}_X$-module. For any affine open subset U of Y, we have (Corollary 22.1.6, Proposition 23.3.13, and note that U is quasi-compact)

$$\begin{aligned}\big(\Gamma(U, \bigoplus_{n\in\mathbb{Z}} p_*(\mathscr{F}(n)))\big)^\sim &= \bigoplus_{n\in\mathbb{Z}} \big(\Gamma(U, p_*(\mathscr{F}(n)))\big)^\sim = \bigoplus_{n\in\mathbb{Z}} \big(\Gamma(p^{-1}(U), \mathscr{F}(n))\big)^\sim \\ &= \Big(\bigoplus_{n\in\mathbb{Z}} \Gamma(p^{-1}(U), \mathscr{F}(n))\Big)^\sim = (\Gamma_*(\mathscr{F}|_{p^{-1}(U)}))^\sim\end{aligned}$$

and therefore a canonical homomorphism

$$\beta_U : \big(\Gamma(U, \bigoplus_{n\in\mathbb{Z}} p_*(\mathscr{F}(n)))\big)^\sim \to \mathscr{F}|_{p^{-1}(U)}.$$

Moreover, the diagram (2.5.4) shows that these homomorphisms are compatible with restrictions on Y, so we deduce a canonical homomorphism

$$\beta : \widetilde{\Gamma_*(\mathscr{F})} \to \mathscr{F}$$

(also denoted by $\beta_{\mathscr{F}}$) for the quasi-coherent $\mathscr{O}_X$-modules.

Proposition 23.3.20. *Let $\mathscr{M}$ be a quasi-coherent $\mathscr{S}$-module and $\mathscr{F}$ be a quasi-coherent $\mathscr{O}_X$-module. Then the composition homomorphisms*

$$\widetilde{\mathscr{M}} \xrightarrow{\tilde{\alpha}} (\Gamma_*(\widetilde{\mathscr{M}}))^\sim \xrightarrow{\beta} \widetilde{\mathscr{M}} \tag{3.3.3}$$

$$\Gamma_*(\mathscr{F}) \xrightarrow{\alpha} \Gamma_*(\widetilde{\Gamma_*(\mathscr{F})}) \xrightarrow{\Gamma_*(\beta)} \Gamma_*(\mathscr{F}) \tag{3.3.4}$$

Proof. The question is local over Y, so we can apply Proposition 23.2.34. □

Again, the homomorphisms α and β are in general not isomorphisms, and further finiteness conditions must be imposed. We note also that the homomorphism β is not always defined, unlike the affine case. However, we shall see that if $\mathscr{S}$ is of finite type and generated by $\mathscr{S}_1$, the homomorphisms α and β are well defined and the corresponding results of the affine cases carry over without difficulties.

Proposition 23.3.21. *Let Y be a scheme and $\mathscr{S}$ be a quasi-coherent $\mathscr{O}_Y$-algebra generated by $\mathscr{S}_1$. Suppose that $\mathscr{S}_1$ is of finite type, then $X = \mathrm{Proj}(\mathscr{S})$ is of finite type over Y.*

Proof. Again we can assume that Y is affine with ring A, so $\mathscr{S} = \widetilde{S}$ where S is a graded A-algebra generated by S_1, and S_1 is a finitely generated A-module by hypothesis. Then S is an A-algebra of finite type, and the proposition follows from Proposition 23.2.35. □

Let $\mathscr{S}$ be a quasi-coherent graded $\mathscr{O}_Y$-algebra and $\mathscr{M}$ be a quasi-coherent $\mathscr{S}$-module. We say that $\mathscr{M}$ is **eventually null** if there exists an integer n such that $\mathscr{M}_k = 0$ for $k \geq n$, and is **eventually finite** if there exists an integer n such that the $\mathscr{S}$-module $\bigoplus_{k\geq n} \mathscr{M}_k$ is of finite type. If $\mathscr{M}$ is eventually null, it is clear that $\widetilde{\mathscr{M}} = 0$, as in the affine case.

Let $\mathscr{M}$ and $\mathscr{N}$ be quasi-coherent graded $\mathscr{S}$-modules. We say a homomorphism $u : \mathscr{M} \to \mathscr{N}$ of degree 0 is eventually injective (resp. eventually sujective, eventually bijective) if there exists

an integer n such that $u_k : \mathscr{M}_k \to \mathscr{N}_k$ is injective (resp. surjective, bijective) for $k \geq n$. It is clear that in this case, $\tilde{u} : \widetilde{\mathscr{M}} \to \widetilde{\mathscr{N}}$ is injective (resp. surjective, bijective), since this can be checked locally over Y and we can apply Proposition 23.3.13. If u is eventually bijective, we also say that it is an eventual isomorphism.

Proposition 23.3.22. *Let Y be a scheme and $\mathscr{S}$ be a quasi-coherent $\mathscr{O}_Y$-algebra generated by $\mathscr{S}_1$ and such that $\mathscr{S}_1$ is of finite type. Let $\mathscr{M}$ be a quasi-coherent graded $\mathscr{S}$-module.*

(a) If $\mathscr{M}$ is eventually finite, $\widetilde{\mathscr{M}}$ is of finite type.

(b) If $\mathscr{M}$ is eventually finite, for $\widetilde{\mathscr{M}} = 0$, it is necessary and sufficient that $\mathscr{M}$ is eventually null.

Proof. The question is local over Y, so we can assume that $Y = \operatorname{Spec}(A)$, and the proposition then follows from Proposition 23.2.36. □

Theorem 23.3.23. *Let Y be a scheme and $\mathscr{S}$ be a quasi-coherent $\mathscr{O}_Y$-algebra generated by $\mathscr{S}_1$ and such that $\mathscr{S}_1$ is of finite type. Let $X = \operatorname{Proj}(\mathscr{S})$, then for any quasi-coherent $\mathscr{O}_X$-module $\mathscr{F}$, the canonical homomorphism $\beta : \widetilde{\Gamma(\mathscr{F})} \to \mathscr{F}$ is an isomorphism.*

Proof. We first note that the homomorphism β is defined because of Proposition 23.3.21. To see that β is an isomorphism, we can assume $Y = \operatorname{Spec}(A)$ is affine, and then apply Theorem 23.2.39. □

Corollary 23.3.24. *Under the hypotheses of Theorem 23.3.23, any quasi-coherent $\mathscr{O}_X$-module $\mathscr{F}$ is isomorphic to an $\mathscr{O}_X$-module of the form $\widetilde{\mathscr{M}}$, where $\mathscr{M}$ is a quasi-coherent $\mathscr{S}$-module. If moreover $\mathscr{F}$ is of finite type, and if we suppose that Y is a quasi-compact scheme, then we can choose $\mathscr{M}$ to be of finite type.*

Proof. The first assertion follows from Theorem 23.3.23 by take $\mathscr{M} = \Gamma_*(\mathscr{F})$. For the second one, it suffices to prove that $\mathscr{M}$ is the inductive limit of graded sub-$\mathscr{S}$-modules of finite type $\mathscr{N}_\lambda$: in fact, it then follows that $\widetilde{\mathscr{M}}$ is the inductive limit of the $\widetilde{\mathscr{N}_\lambda}$ (Proposition 23.3.13), hene $\mathscr{F}$ is the inductive limit of the $\beta(\mathscr{N}_\lambda)$. As X is quasi-compact (Proposition 23.3.21) and $\mathscr{F}$ is of finite type, $\mathscr{F}$ then necessarily equal to one of the $\beta(\widetilde{\mathscr{N}_\lambda})$ (Proposition 19.4.10).

To define the $\mathscr{N}_\lambda$, it suffices to consider for each $n \in \mathbb{Z}$ the quasi-coherent $\mathscr{O}_Y$-module $\mathscr{M}_n$, which is the inductive limit of its sub-$\mathscr{O}_Y$-modules $\mathscr{M}_n^{(\mu_n)}$ of finite type (by Corollary 22.6.62). It is immediate that $\mathscr{P}_{\mu_n} = \mathscr{S} \cdot \mathscr{M}_n^{(\mu_n)}$ is a graded $\mathscr{S}_n$-module of finite type, and $\mathscr{M}$ is then the inductive limit of finite direct sums of these $\mathscr{S}$-modules. □

Corollary 23.3.25. *Suppose the hypotheses of Theorem 23.3.23 and that Y is quasi-compact. Let $\mathscr{F}$ be a quasi-coherent $\mathscr{O}_X$-module of finite type. There exists an integer n_0 such that for $n \geq n_0$, the canonical homomorphism $\sigma : p^*(p_*(\mathscr{F}(n))) \to \mathscr{F}(n)$ is surjective.*

Proof. For any $y \in Y$, let U be an affine open neighborhood of y in Y. There then exists an inter $n_0(U)$ such that, for $n \geq n_0(U)$, $\mathscr{F}(n)|_{p^{-1}(U)}$ is generated by finitely many sections over $p^{-1}(U)$ (Corollary 23.2.41); but these are canonical images of sections of $p^*(p_*(\mathscr{F}(n)))$ over $p^{-1}(U)$, so $\mathscr{F}(n)|_{p^{-1}(U)}$ is equal to the canonical image of $p^*(p_*(\mathscr{F}(n)))|_{p^{-1}(U)}$. Finally, as Y is quasi-compact, there is a finite affine open cover (U_i) of Y, and we can choose n_0 to be the largest of the $n_0(U_i)$. □

Remark 23.3.3. If $p : X \to Y$ is a morphism of ringed spaces and $\mathscr{F}$ is an $\mathscr{O}_X$-module, the fact that the canonical homomorphism $\sigma : p^*(p_*(\mathscr{F})) \to \mathscr{F}$ is surjective is explained as follows: for any $x \in X$ and any sections of $\mathscr{F}$ over an open neighborhood V of x, there exists an open neighborhood U of $p(x)$ in Y, finitely many sections $(t_i)_{1\leq i\leq m}$ of $\mathscr{F}$ over $p^{-1}(U)$, a neighborhood $W \subseteq V \cap p^{-1}(U)$ of x and sections $(a_i)_{1\leq i\leq m}$ of $\mathscr{O}_X$ over W such that

$$s|_W = \sum_i a_i \cdot (t_i|_W).$$

If Y is an affine scheme and $p_*(\mathscr{F})$ is *quasi-coherent*, this condition is equivalent to the fact that $\mathscr{F}$ is generated by its sections over X: in fact, if $Y = \operatorname{Spec}(A)$, we can suppose that $U = D(f)$ with $f \in A$. Since $p_*(\mathscr{F})$ is quasi-coherent, by Theorem 22.1.20 there exists an integer $n > 0$ and sections s_i of $\mathscr{F}$ over X such that $g^n t_i$ is the restriction of s_i (where $g = \rho(f)$, and $\rho : A \to \Gamma(X, \mathscr{O}_X)$ is the homomorphism corresponding to p by Proposition 22.2.4) to $p^{-1}(U)$. As g is invertible over $p^{-1}(U)$, we then have

$$s|_W = \sum_i b_i \cdot (s_i|_W)$$

where $b_i = a_i \cdot (g|_W)^{-n}$, whence our assertion. Therefore, if Y is affine, Corollary 23.3.25 then recovers Corollary 23.2.41, in view of Corollary 19.4.11.

We finally conclude that if Y is a scheme, then the following three conditions are equivalent for a quasi-coherent $\mathscr{O}_X$-module $\mathscr{F}$ such that $p_*(\mathscr{F})$ is quasi-coherent:

(i) The canonical homomorphism $\sigma : p^*(p_*(\mathscr{F})) \to \mathscr{F}$ is surjective.

(ii) There is a quasi-coherent $\mathscr{O}_Y$-module $\mathscr{G}$ and a surjective homomorphism $p^*(\mathscr{G}) \to \mathscr{F}$.

(iii) For any affine open U of Y, $\mathscr{F}|_{p^{-1}(U)}$ is generated by its sections over $p^{-1}(U)$.

We have already established the equivalence of (i) and (iii), and (i) clearly implies (ii). conversely, any homomorphism $u : p^*(\mathscr{G}) \to \mathscr{F}$ factors into $p^*(\mathscr{G}) \to p^*(p_*(\mathscr{F})) \xrightarrow{\sigma} \mathscr{F}$ by (3.4.3), so if u is surjective, so is the canonical homomorphism $\sigma : p^*(p_*(\mathscr{F})) \to \mathscr{F}$.

Corollary 23.3.26. *Suppose the hypotheses of Theorem 23.3.23 and that Y is quasi-compact. Let $\mathscr{F}$ be a quasi-coherent $\mathscr{O}_X$-module of finite type. There then exists an integer n_0 such that for $n \geq n_0$, $\mathscr{F}$ is isomorphic to a quotient of an $\mathscr{O}_X$-module of the form $(p^*(\mathscr{G}))(-n)$, where $\mathscr{G}$ is a quasi-coherent $\mathscr{O}_Y$-module of finite type (dependent on n).*

Proof. As the structural morphism $X \to Y$ is separated and of finite type, $p_*(\mathscr{F}(n))$ is quasi-coherent by Proposition 22.6.54, and so is the inductive limits of its sub-$\mathscr{O}_Y$-modules of finite type, in view of Corollary 22.6.62. Since p^* commutes with inductive limits, we deduce from Corollary 23.3.25 and Proposition 19.4.10 that $\mathscr{F}(n)$ is the canonical image under $\sigma_{\mathscr{F}(n)}$ of an $\mathscr{O}_X$-module of the form $p^*(\mathscr{G})$, where $\mathscr{G}$ is a quasi-coherent sub-$\mathscr{O}_Y$-module of $p_*(\mathscr{F}(n))$ of finite type. The corollary then follows from Corollary 23.3.16 and Corollary 23.3.17. □

23.3.4 Functorial properties of $\operatorname{Proj}(\mathscr{S})$

Let Y be a scheme and $\mathscr{S}, \mathscr{S}'$ be two quasi-coherent graded $\mathscr{O}_Y$-algebras with positive degrees. Let $X = \operatorname{Proj}(\mathscr{S})$, $X' = \operatorname{Proj}(\mathscr{S}')$, and p, p' be the structural morphisms of X and X',

respectively. Let $\varphi : \mathcal{S}' \to \mathcal{S}$ be an $\mathcal{O}_Y$-homomorphism of graded algebras. For any affine open U of Y, let $S_U = \Gamma(U, \mathcal{S})$, $S'_U = \Gamma(U, \mathcal{S}')$; the homomorphism φ defines a homomorphism $\varphi_U : S'_U \to S_U$ of graded A_U-algebras, where $A_U = \Gamma(U, \mathcal{O}_Y)$. It then corresponds to an open subset $G(\varphi_U)$ of $p^{-1}(U)$ and a morphism $\Phi_U : G(\varphi_U) \to p'^{-1}(U)$. Moreover, if $V \subseteq U$ is another affine open subset, the diagram

$$\begin{tikzcd} S'_U \arrow[r, "\varphi_U"] \arrow[d] & S_U \arrow[d] \\ S'_V \arrow[r, "\varphi_V"] & S_V \end{tikzcd} \tag{3.4.1}$$

is commutative, and we also verify, by the definition of $G(\varphi_U)$, that

$$G(\varphi_V) = G(\varphi_U) \cap p^{-1}(V)$$

and that Φ_V is the restriction of Φ_U to $G(\varphi_V)$. We thus define an open subset $G(\varphi)$ of X such that $G(\varphi) \cap p^{-1}(U) = G(\varphi_U)$ for any affine open $U \subseteq Y$, and an affine Y-morphism $\Phi : G(\varphi) \to X'$, which is called the morphism associated with φ and denoted by $\mathrm{Proj}(\varphi)$. If for any $y \in Y$, there exists an affine open neighborhood U of Y such that $\Gamma(U, \mathcal{O}_Y)$-module $\Gamma(U, \mathcal{S}_+)$ is generated by $\varphi(\Gamma(U, \mathcal{S}'_+))$, we then have $G(\varphi_U) = p^{-1}(U)$, and thus $G(\varphi) = X$.

Proposition 23.3.27. *Let $\mathcal{M}$ (resp. $\mathcal{M}'$) be a quasi-coherent graded $\mathcal{S}$-module (resp. $\mathcal{S}'$-module). Then there exist a canonical isomorphism $\widetilde{\varphi^*(\mathcal{M})} \xrightarrow{\sim} \Phi_*(\widetilde{\mathcal{M}}|_{G(\varphi)})$ of $\mathcal{O}_{X'}$-modules and a canonical homomorphism $v : \Phi^*(\widetilde{\mathcal{M}'}) \to \widetilde{\varphi_*(\mathcal{M}')}|_{G(\varphi)}$. If $\mathcal{S}'$ is generated by $\mathcal{S}'_1$, v is an isomorphism.*

Proof. The homomorphisms considered are in fact already defined locally over Y (see Proposition 23.2.46 and Proposition 23.2.47), and the general case then follows from their compatibility with restrictions, and diagram (3.4.1). □

In particular, for any $n \in \mathbb{Z}$, we have a canonical homomorphism $\Phi^*(\mathcal{O}_{X'}(n)) \to \mathcal{O}_X(n)|_{G(\varphi)}$, and this is a homomorphism if $\mathcal{S}'$ is generated by $\mathcal{S}'_1$.

Proposition 23.3.28. *Let Y, Y' be schemes, $\psi : Y' \to Y$ be a morphism, $\mathcal{S}$ be a quasi-coherent $\mathcal{O}_Y$-algebra, and put $\mathcal{S}' = \psi^*(\mathcal{S})$. Then the Y'-scheme $X' = \mathrm{Proj}(\mathcal{S}')$ is canonically identified with $\mathrm{Proj}(\mathcal{S}) \times_Y Y'$. Moreover, if $\mathcal{M}$ is a quasi-coherent graded $\mathcal{S}$-module, the $\mathcal{O}_{X'}$-module $\widetilde{\psi^*(\mathcal{M})}$ is identified with $\widetilde{\mathcal{M}} \otimes_Y \mathcal{O}_{Y'}$.*

Proof. We first note that $\psi^*(\mathcal{S})$ and $\psi^*(\mathcal{M})$ are quasi-coherent $\mathcal{O}_{Y'}$-modules. Let U be an affine open of Y, $U' \subseteq \psi^{-1}(U)$ an affine open of Y', and A, A' the ring of U, U', respectively. We then have $\mathcal{S}|_U = \widetilde{S}$ where S is a graded A-algebra, and $\mathcal{S}'|_{U'}$ is identified with $\widetilde{S \otimes_A A'}$ by Proposition 22.1.13. The first assertion then follows from Proposition 23.2.48 and Corollary 22.3.2, since we can easily verify that the projection $\mathrm{Proj}(\mathcal{S}'|_{U'}) \to \mathrm{Proj}(\mathcal{S}|_U)$ defined by this identification is compatible with restrictions over U and U' and therefore define a morphism $\mathrm{Proj}(\mathcal{S}') \to \mathrm{Proj}(\mathcal{S})$. Now let $p : \mathrm{Proj}(\mathcal{S}) \to Y$ and $p' : \mathrm{Proj}(\mathcal{S}') \to Y'$ be the structural morphisms; $p'^{-1}(U')$ is identified with $p^{-1}(U) \times_U U'$, and the two sheaves $\widetilde{\psi^*(\mathcal{M})}|_{p'^{-1}(U')}$ and $\widetilde{\mathcal{M}} \otimes_Y \mathcal{O}_{Y'}|_{p'^{-1}(U')}$ are then canonically identified to $\widetilde{M \otimes_A A'}$, where $M = \Gamma(U, \mathcal{M})$, in view of Proposition 23.2.48 and Proposition 22.1.13; whence the second assertion, since these identifications are compatible with restrictions. □

Corollary 23.3.29. *With the notations of Proposition 23.3.28, $\mathscr{O}_{X'}(n)$ is canonically identified with $\mathscr{O}_X(n) \otimes_Y \mathscr{O}_{Y'}$ for any $n \in \mathbb{Z}$.*

Proof. With the notations of Proposition 23.3.28, it is clear that $\psi^*(\mathscr{S}(n)) = \mathscr{S}'(n)$ for any $n \in \mathbb{Z}$, whence the corollary. □

Retain the notations in Proposition 23.3.28, denote by $\Psi : X' \to X$ the canonical projection, and put $\mathscr{M}' = \psi^*(\mathscr{M})$. We suppose that $\mathscr{S}$ is generated by $\mathscr{S}_1$ and that X is of finite type over Y (for example if $\mathscr{S}_1$ is of finite type, cf. Proposition 23.3.21). Then $\mathscr{S}'$ is generated by $\mathscr{S}'_1$ (as can be checked locally on affine opens of Y) and X' is of finite type over Y by Proposition 22.6.35. Let $\mathscr{F}$ be an $\mathscr{O}_X$-module and set $\mathscr{F}' = \Psi^*(\mathscr{F})$; it then follows from Corollary 23.3.29 that we have $\mathscr{F}'(n) = \Psi^*(\mathscr{F})$ for each $n \in \mathbb{Z}$. We define a canonical Ψ-homomorphism $\theta_n : p_*(\mathscr{F}(n)) \to p'_*(\mathscr{F}'(n))$ as follows: from the commutative diagram

$$\begin{tikzcd} X' \arrow[r, "\Psi"] \arrow[d, "p'"'] & X \arrow[d, "p"] \\ Y' \arrow[r, "\psi"] & Y \end{tikzcd}$$

we see that it suffices to define a homomorphism

$$p_*(\mathscr{F}(n)) \to \psi_*(q'_*(\Psi^*(\mathscr{F}(n)))) = q_*(\Psi_*(\Psi^*(\mathscr{F}(n)))),$$

and we can take $\theta_n = p_*(\rho_n)$, where ρ_n is the canonical homomorphism $\rho_n : \mathscr{F}(n) \to \Psi_*(\Psi^*(\mathscr{F}(n)))$. It is immediate that for any affine open U of Y and any affine open U' of Y such that $U' \subseteq \psi^{-1}(U)$, the homomorphism θ_n thus defined gives a canonical homomorphism $\Gamma(p^{-1}(U), \mathscr{F}(n)) \to \Gamma(p'^{-1}(U'), \mathscr{F}'(n))$, and the commutative diagram (2.5.4) shows that if $\mathscr{F}$ is quasi-coherent, the diagram

$$\begin{tikzcd} \widetilde{\Gamma_*(\mathscr{F})} \arrow[r, "\tilde{\theta}"] \arrow[d, "\beta_{\mathscr{F}}"'] & \widetilde{\Gamma_*(\mathscr{F}')} \arrow[d, "\beta_{\mathscr{F}'}"] \\ \mathscr{F} \arrow[r, "\rho"] & \mathscr{F}' \end{tikzcd}$$

is commutative (where the send row is the canonical Ψ-morphism $\mathscr{F} \to \Phi^*(\mathscr{F})$).

Similarly, the commutative diagram (2.5.3) shows that the diagram

$$\begin{tikzcd} \mathscr{M} \arrow[r, "\rho"] \arrow[d, "\alpha_{\mathscr{M}}"] & \mathscr{M}' \arrow[d, "\alpha_{\mathscr{M}'}"] \\ \Gamma_*(\widetilde{\mathscr{M}}) \arrow[r, "\theta"] & \Gamma_*(\widetilde{\mathscr{M}'}) \end{tikzcd}$$

is commutative (where the first row is the canonical ψ-morphism $\mathscr{M} \to \psi^*(\mathscr{M})$).

Consider now a morphism $\psi : Y' \to Y$ of schemes, a quasi-coherent graded $\mathscr{O}_Y$-algebra (resp. $\mathscr{O}_{Y'}$-algebra) $\mathscr{S}$ (resp. $\mathscr{S}'$), and a ψ-morphism $u : \mathscr{S} \to \mathscr{S}'$ of graded algebras. This is equivalent to giving an $\mathscr{O}_{Y'}$-homomorphism of graded algebras $u^\sharp : \psi_*(\mathscr{S}) \to \mathscr{S}'$, and we deduce from $u^\sharp$ an Y'-morphism

$$w = \operatorname{Proj}(u^\sharp) : G(u^\sharp) \to \operatorname{Proj}(\psi^*(\mathscr{S})),$$

where $G(u^\sharp)$ is an open subset of $X' = \operatorname{Proj}(\mathscr{S}')$. On the other hand, $\operatorname{Proj}(\psi^*(\mathscr{S}))$ is canonically

identified with $X \times_Y Y'$, where $X = \mathrm{Proj}(\mathcal{S})$ (Proposition 23.3.28). By composing the morphism $\mathrm{Proj}(u^\sharp)$ with the first projection $\pi : X \times_Y Y' \to X$, we then obtain a morphism $v = \mathrm{Proj}(u) : G(u^\sharp) \to X$ such that the diagram

$$\begin{tikzcd} G(u^\sharp) \arrow[r, "v"] \arrow[d] & X \arrow[d] \\ Y' \arrow[r, "\psi"] & Y \end{tikzcd} \tag{3.4.2}$$

is commutative. Moreover, for any quasi-coherent $\mathcal{O}_Y$-module $\mathcal{M}$, we have a canonical v-morphism

$$\nu : \widetilde{\mathcal{M}} \to (\psi^*(\mathcal{M}) \otimes_{\psi^*(\mathcal{S})} \mathcal{S}')^\sim|_{G(u^\sharp)} \tag{3.4.3}$$

such that $\nu^\sharp$ is the composition

$$v^*(\widetilde{\mathcal{M}}) = w^*(\pi^*(\widetilde{\mathcal{M}})) \xrightarrow{\sim} w^*(\widetilde{\psi^*(\mathcal{M})}) \xrightarrow{\nu} (\psi^*(\mathcal{M}) \otimes_{\psi^*(\mathcal{M})} \mathcal{S}')^\sim|_{G(u^\sharp)} \tag{3.4.4}$$

where the first arrow is the isomorphism in Proposition 23.3.28 and the second one is the homomorphism ν of Proposition 23.3.27. If $\mathcal{S}$ is generated by $\mathcal{S}_1$, then it follows from Proposition 23.3.27 that $\nu^\sharp$ is an isomorphism. As a particular case, for any $n \in \mathbb{Z}$ we have a canonical v-homomorphism

$$\nu : \mathcal{O}_X(n) \to \mathcal{O}_{X'}(n)|_{G(u^\sharp)}. \tag{3.4.5}$$

23.3.5 Closed subschemes of $\mathrm{Proj}(\mathcal{S})$

Let Y be a scheme and $\varphi : \mathcal{S} \to \mathcal{S}'$ be a homomorphism of quasi-coherent graded $\mathcal{O}_Y$-algebras of degree 0. We say that φ is **eventually injective** (resp. **eventually surjective**, **eventually bijective**) if there exists an integer n such that, for $k \geq n$, $\varphi_k : \mathcal{S}_k \to \mathcal{S}'_k$ is surjective (resp. injective, bijective). If this is the case, we can then reduce the study of the morphism $\Phi : \mathrm{Proj}(\mathcal{S}') \to \mathrm{Proj}(\mathcal{S})$ to the case where φ is surjective (resp. injective, bijective) (this follows from Proposition 23.3.6). If φ is eventually bijective, we also say that φ is an **eventual isomorphism**.

Proposition 23.3.30. *Let Y be a scheme, $\mathcal{S}$ be a quasi-coherent $\mathcal{O}_Y$-algebra, and $X = \mathrm{Proj}(\mathcal{S})$.*

(a) If $\varphi : \mathcal{S} \to \mathcal{S}'$ is a eventually surjective homomorphism of graded $\mathcal{O}_Y$-algebra, the corresponding morphism $\Phi = \mathrm{Proj}(\varphi)$ is defined over $\mathrm{Proj}(\mathcal{S}')$ and is a closed immersion from $\mathrm{Proj}(\mathcal{S}')$ into X. If $\mathcal{J}$ is the kernel of φ, the closed subscheme of X associated with Φ is defined by the quasi-coherent ideal $\widetilde{\mathcal{J}}$ of $\mathcal{O}_X$.

(b) Suppose moreover that $\mathcal{S}_0 = \mathcal{O}_Y$ and $\mathcal{S}$ is generated by $\mathcal{S}_1$ where $\mathcal{S}_1$ is of finite type. Let X' be a closed subscheme of X defined by a quasi-coherent ideal $\mathcal{I}$ of $\mathcal{O}_X$. Let $\mathcal{J}$ be the inverse image of $\Gamma_*(\mathcal{I})$ under the canonical homomorphism $\alpha : \mathcal{S} \to \Gamma_*(\mathcal{O}_X)$ and put $\mathcal{S}' = \mathcal{S}/\mathcal{J}$. Then X' is the subscheme associated with the closed immersion $\mathrm{Proj}(\mathcal{S}') \to X$ corresponding to the canonical homomorphism $\mathcal{S} \to \mathcal{S}'$ of graded $\mathcal{O}_Y$-algebras.

Proof. For the assertion of (a), we can assume that φ is surjective. Then for any affine open U of Y, $\Gamma(U, \mathcal{S}) \to \Gamma(U, \mathcal{S}')$ is surjective by Corollary 22.1.6, so we have $G(\varphi) = X$. We are

immediately reduced to the case where Y is affine, and the assertion follows from Proposition 23.2.50(a).

As for case (b), we are reduced to prove that the homomorphism $\widetilde{\mathscr{J}} \to \mathscr{O}_X$ induced from the canonical injection $\mathscr{J} \to \mathscr{S}$ is an isomorphism from $\widetilde{\mathscr{J}}$ to $\mathscr{I}$. As the question is local, we can assume that Y is affine with ring A, which implies $\mathscr{S} = \widetilde{S}$, where S is a graded A-algebra generated by S_1 and S_1 is of finite type over A. It then suffices to apply Proposition 23.2.50(b). □

Corollary 23.3.31. *Under the hypotheses of Proposition 23.3.30(a), suppose that $\mathscr{S}$ is generated by $\mathscr{S}_1$. Then $\Phi^*(\mathscr{O}_X(n))$ is canonically identified with $\mathscr{O}_{X'}(n)$ for any $n \in \mathbb{Z}$.*

Proof. We have defined such an isomorphism if Y is affine; in the general case, it suffices to verify that these isomorphisms are compatible with restrictions. □

Corollary 23.3.32. *Let Y be a scheme, $\mathscr{S}$ be a quasi-coherent $\mathscr{O}_Y$-algebra generated by $\mathscr{S}_1$, $\mathscr{M}$ be a quasi-coherent $\mathscr{O}_Y$-module, and $u : \mathscr{M} \to \mathscr{S}_1$ be a surjective $\mathscr{O}_Y$-homomorphism. If $\bar{u} : \boldsymbol{S}(\mathscr{M}) \to \mathscr{S}$ is the canonical homomorphism of $\mathscr{O}_Y$-algebras extending u, then the morphism corresponding to $\bar{u}$ is a closed immersion from* $\operatorname{Proj}(\mathscr{S})$ *into* $\operatorname{Proj}(\boldsymbol{S}(\mathscr{M}))$.

Proof. In fact, $\bar{u}$ is surjective by hypothesis, so we can apply Proposition 23.3.30(a). □

23.3.6 Morphisms into $\operatorname{Proj}(\mathscr{S})$

Let $q : X \to Y$ be a morphism of schemes, $\mathscr{L}$ be an invertible $\mathscr{O}_X$-module, and $\mathscr{S}$ be a quasi-coherent $\mathscr{O}_Y$-algebra with positive degrees. Then $q^*(\mathscr{S})$ is a quasi-coherent graded $\mathscr{O}_X$-algebra with positive degrees. Suppose that we are given a graded homomorphism of $\mathscr{O}_X$-algebras

$$\psi : q^*(\mathscr{S}) \to \boldsymbol{S}(\mathscr{L}) = \bigoplus_{n \geq 0} \mathscr{L}^{\otimes n}$$

(recall that for an invertible $\mathscr{O}_X$-module $\mathscr{L}$ we have $\boldsymbol{T}(\mathscr{L}) = \boldsymbol{S}(\mathscr{L})$) or equivalently, a $\mathscr{O}_Y$-homorphism of graded algebras

$$\psi^\flat : \mathscr{S} \to q_*(\boldsymbol{S}(\mathscr{L})).$$

Since $\mathscr{L}$ is invertible and $\boldsymbol{T}(\mathscr{O}_X) = \boldsymbol{S}(\mathscr{O}_X) = \mathscr{O}_X[T]$, by Proposition 23.3.6 and Corollary 23.3.5 we know that $\operatorname{Proj}(\boldsymbol{S}(\mathscr{L}))$ is canonically identified with X. We then conclude that the homomorphism ψ induces a Y-morphism

$$r_{\mathscr{L},\psi} : G(\psi) \to \operatorname{Proj}(\mathscr{S}) = P,$$

where $G(\psi)$ is an open subset of X. Recall that this morphism is by definition obtained by composing the first projection $\pi : \operatorname{Proj}(q^*(\mathscr{S})) = P \times_Y X \to P$ with the Y-morphism $\tau = \operatorname{Proj}(\psi)$:

$G(\psi) \to \mathrm{Proj}(q^*(\mathscr{S}))$, which is shown in the following diagram:

$$\begin{tikzcd}
 & P \times_Y X \arrow[r, "\pi"] \arrow[d] & P \arrow[d, "p"] \\
G(\psi) \arrow[ur, "\tau=\mathrm{Proj}(\psi)"] \arrow[r] \arrow[uur, bend left, "r_{\mathscr{L},\psi}"] & X \arrow[r, "q"] & Y
\end{tikzcd}$$

Remark 23.3.4. Let us explain the morphism $r = r_{\mathscr{L},\psi}$ when $Y = \mathrm{Spec}(A)$ is affine, and therefore $\mathscr{S} = \widetilde{S}$, where S is a graded A-algebra with positive degrees. First suppose that $X = \mathrm{Spec}(B)$ is also affine and $\mathscr{L} = \widetilde{L}$, where L is a free B-module of rank 1. We then have $q^*(\mathscr{S}) = \widetilde{S \otimes_A B}$ by Proposition 22.1.13. If c is a generator of L, the homomorphism $\psi_n : q^*(\mathscr{S}_n) \to \mathscr{L}^{\otimes n}$ then corresponds to a B-homomorphism

$$w_n : S_n \otimes_A B \to L^{\otimes n}, \quad s \otimes b \mapsto b v_n(s) c^{\otimes n}, \tag{3.6.1}$$

where $v_n : S_n \to B$ is the n-th component of a homomorphism $v : S \to B$ of algebras. Let $f \in S_d$ with positive degree and put $g = v_d(f)$. We have $\pi^{-1}(D_+(f)) = D_+(f \otimes 1)$ in view of Proposition 23.2.48 and the identification of $D_+(f)$ with $\mathrm{Spec}(S_{(f)})$. On the other hand, the formula (2.5.1) and (3.6.1) shows that (using the canonical isomorphism of X and $\mathrm{Proj}(\boldsymbol{S}(\mathscr{L}))$)

$$\tau^{-1}(D_+(f \otimes 1)) = D(g)$$

whence $r^{-1}(D_+(f)) = D(g)$. Furthermore, the restriction of the morphism $\tau = \mathrm{Proj}(\psi)$ to $D(g)$ corresponds to the homomorphism $(S \otimes_A B)_{(f \otimes 1)} \to B_g$, which send $(s \otimes 1)/(f \otimes 1)^n$ (for $s \in S_{nd}$) to $v_{nd}(s)/g^n$, and the restriction of the projection π to $D_+(f \otimes 1)$ corresponds to the homomorphism $S_{(f)} \to (S \otimes_A B)_{(f \otimes 1)}$ given by $s/f^n \mapsto (s \otimes 1)/(f \otimes 1)^n$. We then conclude that the restriction of the morphism r to $D(g)$ corresponds to the homomorphisms $\omega : S_{(f)} \to B_g$ of A-algebras such that $\omega(s/f^n) = v_{nd}(s)/g^n$ for $s \in S_{nd}$.

Proposition 23.3.33. *Let $Y = \mathrm{Spec}(A)$ be affine and $\mathscr{S} = \widetilde{S}$, where S is a graded A-algebra. For any $f \in S_d = \Gamma(Y, \mathscr{S}_d)$, we have (where $\psi^\flat(f) \in \Gamma(X, \mathscr{L}^{\otimes d})$)*

$$r^{-1}_{\mathscr{L},\psi}(D_+(f)) = X_{\psi^\flat(f)}. \tag{3.6.2}$$

Moreover, under the canonical isomorphism of X and $\mathrm{Proj}(\boldsymbol{S}(\mathscr{L}))$, the restriction morphism $r_{\mathscr{L},\psi} : X_{\psi^\flat(f)} \to D_+(f) = \mathrm{Spec}(S_{(f)})$ corresponds to the homomorphism

$$\psi^\flat_{(f)} : S_{(f)} \to \Gamma(X_{\psi^\flat(f)}, \mathscr{O}_X)$$

such that, for any $s \in S_{nd} = \Gamma(Y, \mathscr{S}_{nd})$, we have

$$\psi^\flat_{(f)}(s/f^n) = (\psi^\flat(s)|_{X_{\psi^\flat(f)}})(\psi^\flat(f)|_{X_{\psi^\flat(f)}})^{-n}.$$

Proof. This follows from Remark 23.3.4 by passing to the general case. □

We say the morphism $r_{\mathscr{L},\psi}$ is **everywhere defined** if $G(\psi) = X$. For this to be the case, it is necessary and sufficient that $G(\psi) \cap q^{-1}(U) = q^{-1}(U)$ for any affine open $U \subseteq Y$, so this question is local over Y. If Y is affine, $G(\psi)$ is then the union of $r^{-1}(D_+(f))$ for $f \in S_+$, so by (3.6.2) the $X_{\psi^\flat(f)}$ then form a covering of X. In other words:

Corollary 23.3.34. *Under the hypotheses of Proposition 23.3.33, for the morphism $r_{\mathscr{L},\psi}$ to be everywhere defined, it is necessary and sufficient that for any $x \in X$, there exists an integer $n > 0$ and a section $s \in S_n$ such that $t = \psi^\flat(s) \in \Gamma(X, \mathscr{L}^{\otimes n})$ is nonzero at x. In particular, this is true if ψ is eventually surjective.*

Corollary 23.3.35. *Under the hypotheses of Proposition 23.3.33, for the morphism $r_{\mathscr{L},\psi}$ to be dominant, it is necessary and sufficient that for any integer $n > 0$, any section $s \in S_n$ such that $\psi^\flat(b) \in \Gamma(X, \mathscr{L}^{\otimes n})$ is locally nilpotent, is itself nilpotent.*

Proof. We must check that $r^{-1}_{\mathscr{L},\psi}(D_+(s))$ is nonempty if $D_+(s)$ is nonempty, and the corollary follows from (3.6.2) and Corollary 23.2.6. □

Proposition 23.3.36. *Let $q : X \to Y$ be a morphism, $\mathscr{L}$ be an invertible $\mathscr{O}_X$-module, and $\mathscr{S}$, $\mathscr{S}'$ be quasi-coherent graded $\mathscr{O}_Y$-algebras. Let $u : \mathscr{S}' \to \mathscr{S}$ be a homomorphism of graded algebras, $\psi : q^*(\mathscr{S}) \to \boldsymbol{S}(\mathscr{L})$ be a homomorphism of graded algebras, and $\psi' = \psi \circ q^*(u)$ be the composition.*

(i) If $r_{\mathscr{L},\psi'}$ is everywhere defined, then $r_{\mathscr{L},\psi}$ is everywhere defined;

(ii) If u is eventually surjective and $r_{\mathscr{L},\psi'}$ is dominant, then $r_{\mathscr{L},\psi}$ is dominant;

(iii) If u is eventually injective and $r_{\mathscr{L},\psi}$ is dominant, then $r_{\mathscr{L},\psi}$ is dominant.

Proof. We have $G(\psi') \subseteq G(\psi)$, whence the first assertion. If u is eventually surjective, $\mathrm{Proj}(u) : \mathrm{Proj}(S) \to \mathrm{Proj}(S')$ is everywhere defined and is a closed immersion; as $r_{\mathscr{L},\psi'}$ is the composition of $\mathrm{Proj}(u)$ and the restriction of $r_{\mathscr{L},\psi}$ to $G(\psi')$, we then conclude that if $r_{\mathscr{L},\psi'}$ is dominant, so is $r_{\mathscr{L},\psi}$. Finally, if u is eventually injective, then $\mathrm{Proj}(u)$ is a dominant morphism from $G(u)$ into $\mathrm{Proj}(\mathscr{S}')$ (Corollary 23.2.45); as $G(\psi')$ is the inverse image of $G(u)$ under $r_{\mathscr{L},\psi}$, we see that if $r_{\mathscr{L},\psi}$ is dominant, so is $r_{\mathscr{L},\psi'}$. □

Proposition 23.3.37. *Let Y be a quasi-compact scheme, $q : X \to Y$ be a quasi-compact morphism, $\mathscr{L}$ be an invertible $\mathscr{O}_X$-module, and $\mathscr{S}$ be a quasi-coherent $\mathscr{O}_Y$-algebra which is the filtered limit of a system $(\mathscr{S}^\lambda)$ of quasi-coherent $\mathscr{O}_Y$-algebras. Let $\varphi_\lambda : \mathscr{S}^\lambda \to \mathscr{S}$ be the canonical homomorphism, $\psi : q^*(\mathscr{S}) \to \boldsymbol{S}(\mathscr{L})$ be a homomorphism of graded algebras, and put $\psi_\lambda = \psi \circ q^*(\varphi_\lambda)$. Then for the morphism $r_{\mathscr{L},\psi}$ to be everywhere defined, it is necessary and sufficient that there exists an index λ such that $r_{\mathscr{L},\psi_\lambda}$ is everywhere defined; in this case, $r_{\mathscr{L},\psi_\mu}$ is everywhere defined for $\mu \geq \lambda$.*

Proof. The condition is sufficient in view of Proposition 23.3.36. Conversely, suppose that $r_{\mathscr{L},\psi}$ is everywhere defined; we can assume that Y is affine, because if for any affine open $U \subseteq Y$ there exists $\lambda(U)$ such that the restriction of $r_{\mathscr{L},\psi_{\lambda(U)}}$ to $q^{-1}(U)$ is defined everywhere, it then suffices to cover Y by finitely many affine opens U_i (recall that Y is quasi-compact) and choose $\lambda \geq \lambda(U_i)$ for all i, by Proposition 23.3.36. If Y is affine (so $\mathscr{S} = \widetilde{S}$ where $S = \Gamma(Y, \mathscr{S})$) the hypotheses implies that for any $x \in X$, there exists a section $s^{(x)} \in S_n$ for some integer n such that, if $t^{(x)} = \psi^\flat(s^{(x)})$, then $t^{(x)}(x) \neq 0$ (where $t^{(x)}$ is a section of $\mathscr{L}^{\otimes n}$ over X), which implies $t^{(x)}(z) \neq 0$ for z in a neighborhood $V(x)$ of X. As the morphism $q : X \to Y$ is quasi-compact, we see X is quasi-compact, so we can cover X by finitely many $V(x_i)$ and let $s^{(i)}$ be

the corresponding section of S. There is then an index λ such that $s^{(i)}$ is of the form $\varphi_\lambda(s_\lambda^{(i)})$, where $s_\lambda^{(i)} \in S^\lambda$ for all i, and it follows from Corollary 23.3.34 that $r_{\mathscr{L},\psi_\lambda}$ is everywhere defined. The second assertion is trival by Proposition 23.3.36. □

Corollary 23.3.38. *Under the hypotheses of Proposition 23.3.37, if the morphisms $r_{\mathscr{L},\psi_\lambda}$ are dominant, so is $r_{\mathscr{L},\psi}$. The converse is also ture if the homomorphisms φ_λ are eventually injective.*

Proof. The second assertion is a particular case of Proposition 23.3.36. To show that $r_{\mathscr{L},\psi}$ is dominant if each $r_{\mathscr{L},\psi_\lambda}$ is, we can assume that Y is affine and thus $\mathscr{S} = \widetilde{S}$ where $S = \Gamma(Y, \mathscr{S})$. If $s \in S$ is such that $\psi^\flat(s)$ is locally nilpotent, as we can write $s = \varphi_\lambda(s_\lambda)$ for some λ, from the definition of ψ_λ and by Corollary 23.3.35, we conclude that s_λ is nilpotent, so s is nilpotent, and the assertion follows by applying Corollary 23.3.35. □

Remark 23.3.5. With the hypotheses and notations of Proposition 23.3.33, for each $n \in \mathbb{Z}$ we have a homomorphism

$$\nu : r^*_{\mathscr{L},\psi}(\mathscr{O}_P(n)) \to \mathscr{L}^{\otimes n}|_{G(\psi)} \tag{3.6.3}$$

which is in fact the homomorphism ν defined in (3.4.3) on $\mathscr{O}_P(n)$. We also see that under the hypotheses of Proposition 23.3.33, the restriction of ν to $X_{\psi^\flat(f)}$ corresponds to the homomorphism sending the element s/f^k (with $s \in S_{n+kd}$) to the section

$$(\psi^\flat(s)|_{X_{\psi^\flat(f)}})(\psi^\flat(f)|_{X_{\psi^\flat(f)}})^{-k} \in \Gamma(X_{\psi^\flat(f)}, \mathscr{L}^{\otimes n}),$$

where we also use the notations of Proposition 23.3.33.

Remark 23.3.6. Let $\mathscr{F}$ be a quasi-coherent $\mathscr{O}_X$-module and suppose that q is quasi-compact and quasi-separated, so for each $n \geq 0$, $q_*(\mathscr{F} \otimes \mathscr{L}^{\otimes n})$ is a quasi-coherent $\mathscr{O}_Y$-module (Proposition 22.6.54). Let $\mathscr{M}' = \bigoplus_{n\geq 0} \mathscr{F} \otimes \mathscr{L}^{\otimes n}$, which is a quasi-coherent $\mathscr{O}_Y$-module, and consider the image $\mathscr{M} = q_*(\mathscr{M}') = \bigoplus_{n\geq 0} q_*(\mathscr{F} \otimes \mathscr{L}^{\otimes n})$ (which is a quasi-coherent $\mathscr{S}$-module via the homomorphism $\psi^\flat$). We shall see that there is a canonical homomorphism of $\mathscr{O}_X$-modules

$$\xi : r^*_{\mathscr{L},\psi}(\widetilde{\mathscr{M}}) \to \mathscr{F}|_{G(\psi)}. \tag{3.6.4}$$

For this, recall that we have defined a canonical homomorphism (3.4.3):

$$\nu : r^*_{\mathscr{L},\psi}(\widetilde{\mathscr{M}}) \to (q^*(\mathscr{M}) \otimes_{q^*(\mathscr{S})} \boldsymbol{S}(\mathscr{L}))^\sim|_{G(\psi)},$$

where the right hand side is considered as a quasi-coherent sheaf over X. On the other hand, for any quasi-coherent graded $\boldsymbol{S}(\mathscr{L})$-module $\mathscr{M}'$, we have a canonical homomorphism

$$q^*(q_*(\mathscr{M}')) \otimes_{q^*(\mathscr{S})} \boldsymbol{S}(\mathscr{L}) \to \mathscr{M}'$$

which, for any open subset U of X, any section t' of $q^*(q_*(\mathscr{M}'_h))$ over U and any section b' of $\mathscr{L}^{\otimes k}$ over U, sends the section $t' \otimes b'$ to the section $b'\sigma(t')$ of $\mathscr{M}'_{h+k}$, where σ is the canonical homomorphism $q^*(q_*(\mathscr{M}')) \to \mathscr{M}'$. We then conclude a canonical homomorphism

$$(q^*(q_*(\mathscr{M}')) \otimes_{q^*(\mathscr{S})} \boldsymbol{S}(\mathscr{L}))^\sim|_{G(\psi)} \to \widetilde{\mathscr{M}'}|_{G(\psi)}$$

and as $\widetilde{\mathscr{M}}'$ is canonically identified with $\mathscr{F}$ by Remark 23.3.1, we obtain the canonical homomorphism ξ.

Under the hypotheses and notations of Proposition 23.3.18, the restriction of this homomorphism to $X_{\psi^\flat(f)}$ is defined as follows: giving a section t_{nd} of $\mathscr{F}\otimes\mathscr{L}^{\otimes d}$ over X (which is also a section of $q_*(\mathscr{F}\otimes\mathscr{L}^{\otimes n})$ over Y), we send the element t_{nd}/f^n to the sectin $(t_{nd}|_{X_{\psi^\flat(f)}})(\psi^\flat(f)|_{X_{\psi^\flat(f)}})^{-n}$ of $\mathscr{F}$ over $X_{\psi^\flat(f)}$.

We now consider the important question that whether the induced morphism $r_{\mathscr{L},\psi}$ is an immersion (reps. an open immersion, a closed immersion). It is clear that this question is local over Y, and we shall give a criterion in this situation together with the condition that $r_{\mathscr{L},\psi}$ is defined everywhere.

Proposition 23.3.39. *Under the hypothesis and notations of Proposition 23.3.33, for the morphism $r_{\mathscr{L},\psi}$ be everywhere defined and an immersion, it is necessary and sufficient that there exists a family of sections $s_\alpha \in S_{n_\alpha}$ (with $n_\alpha > 0$) such that, if $f_\alpha = \psi^\flat(s_\alpha)$, the following conditions are satisfied:*

(i) The X_{f_α} form a covering of X.

(ii) The X_{f_α} are affine open subset of X.

(iii) For any index α and any section $t \in \Gamma(X_{f_\alpha}, \mathscr{O}_X)$, there exists an integer $n > 0$ and $s \in S_{mn_\alpha}$ such that $t = (\psi^\flat(s)|_{X_{f_\alpha}})(f_\alpha|_{X_{f_\alpha}})^{-m}$.

For the morphism $r_{\mathscr{L},\psi}$ to be everywhere defined and an open immersion, it is necessary and sufficient that the family (s_α) satisfies the following additional condition:

(iv) For any integer $m > 0$ and any $s \in S_{mn_\alpha}$ such that $\psi^\flat(s)|_{X_{f_\alpha}} = 0$, there exists an integer $n > 0$ such that $s_\alpha^n s = 0$.

Similarly, for the morphism $r_{\mathscr{L},\psi}$ to be everywhere defined and a closed immersion, it is necessary and sufficient that the family (s_α) satisfies the following additional condition:

(v) The $D_+(s_\alpha)$ form a covering of $P = \mathrm{Proj}(S)$.

Proof. By Proposition 22.4.9, for the morphism $r = r_{\mathscr{L},\psi}$ to be an immersion (resp. a closed immersion), it is necessary and sufficent that there exists a covering of $r(G(\psi))$ (resp. of P) by the sets $D_+(s_\alpha)$ such that if $V_\alpha = r^{-1}(D_+(s_\alpha))$, the restriction of r on V_α is a closed immersion of V_α into $D_+(s_\alpha)$ (cf. Corollary 22.4.10). Now condition (i) just means that r is everywhere defined and that $D_+(s_\alpha)$ cover $r(X)$, by (3.6.2). As each $D_+(s_\alpha)$ is affine, condition (ii) and (iii) express that the restriction of r to X_{f_α} is a closed immersion into $D_+(s_\alpha)$ (Example 22.4.6). Finally, as (iii) and (iv) means the ring homomorphism $\psi^\flat_{(s_\alpha)} : S_{(s_\alpha)} \to \Gamma(X_{f_\alpha}, \mathscr{O}_X)$ is an isomorphism, (ii), (iii), (iv) mean that the restriction of r to X_{f_α} is an isomorphism from X_{f_α} to $D_+(s_\alpha)$ for each α, so together with (i), they mean that r is an open immersion. □

Corollary 23.3.40. *Under the hypothesis and notations of Proposition 23.3.36, if $r_{\mathscr{L},\psi'}$ is everywhere defined and is an immersion, so is $r_{\mathscr{L},\psi}$. If we suppose that u is eventually surjective and if $r_{\mathscr{L},\psi'}$ is everywhere defined and is a closed immersion (resp. open), then so is $r_{\mathscr{L},\psi}$.*

Proof. We first suppose that $r_{\mathscr{L},\psi'}$ is everywhere defined and and is an immersion. Then by Proposition 23.3.39, there is a family $s'_\alpha \in S'_{n_\alpha}$ such that, if $f_\alpha = \psi'^\flat(s'_\alpha)$, the conditions (i), (ii), (iii) are satisfied. Set $s_\alpha = u(s'_\alpha)$, then $f_\alpha = \psi^\flat(s_\alpha)$, and we have a commutative diagram

$$\begin{tikzcd} S'_{(s'_\alpha)} \arrow[r, "\psi'^\flat_{(s'_\alpha)}"] \arrow[d, "u_{(s'_\alpha)}"'] & \Gamma(X_{f_\alpha}, \mathscr{O}_X) \\ S_{(s_\alpha)} \arrow[ur, "\psi^\flat_{(s_\alpha)}"'] & \end{tikzcd}$$

The hypothesis then implies that $\psi'^\flat_{(s'_\alpha)}$ is surjective, so the homomorphism $\psi^\flat_{(s_\alpha)}$ is also surjective. This shows that $r_{\mathscr{L},\psi}$ is everywhere defined and is an immersion, in view of Proposition 23.3.39. If $r_{\mathscr{L},\psi'}$ is moreover an open immersion, then the homomorphism $\psi'^\flat_{(s'_\alpha)}$ is also injective, and this implies the homomorphism $\psi^\flat_{(s_\alpha)}$ is injective if u is eventually surjective, since in this case the homomorphism $u_{(s'_\alpha)}$ is just surjective.

Finally, if $r_{\mathscr{L},\psi'}$ is a closed immersion, then condition (v) is satisfied for (s'_α), and hence satisfied for (s_α) if u is eventually surjective (since in this case $\mathrm{Proj}(u)$ is a closed immersion from $\mathrm{Proj}(S)$ to $\mathrm{Proj}(S')$); this implies $r_{\mathscr{L},\psi}$ is a closed immersion. □

Proposition 23.3.41. *Suppose the hypotheses of Proposition 23.3.37 and moreover that $q : X \to Y$ is a morphism of finite type. Then, for the morphism $r_{\mathscr{L},\psi}$ to be everywhere defined and an immersion, it is necessary and sufficient that there exists an index λ such that $r_{\mathscr{L},\psi_\lambda}$ is everywhere defined and is an immersion; in this case, $r_{\mathscr{L},\psi_\lambda}$ is everywhere defined and an immersion for $\mu \geq \lambda$.*

Proof. By Corollary 23.3.40, it suffices to prove that if $r_{\mathscr{L},\psi}$ is defined everywhere and is an immersion, then there exists an index λ such that $r_{\mathscr{L},\psi_\lambda}$ is defined everywhere and is an immersion. By the same reasoning of Proposition 23.3.37 and using the quasi-compactness of Y, we are reduced to the case where $Y = \mathrm{Spec}(A)$ is affine. As X is then quasi-compact, Proposition 23.3.39 shows that there exists a finite family (s_i) of elements of S ($s_i \in S_{n_i}$) satisfying the conditions (i), (ii), and (iii). The morphism $X_{f_i} \to Y$ (where $f_i = \psi^\flat(s_i)$) is of finite type since X_{f_i} is affine and the morphism $q : X \to Y$ is locally of finite type. The ring B_i of X_{f_i} is therefore an A-algebra of finite type by Corollary 22.6.39, and we choose (t_{ij}) to be a family of generators of this algebra. There are then elements $s_{ij} \in S_{m_{ij}n_i}$ such that

$$t_{ij} = (\psi^\flat(s_{ij})|_{X_{f_i}})(\psi^\flat(s_i)|_{X_{f_i}})^{-m_{ij}}$$

We can choose an index λ and elements $s_{i\lambda} \in S^\lambda_{n_i}$, $s_{ij\lambda} \in S^\lambda_{m_{ij}n_i}$ such that their images under φ_λ is s_i and s_{ij}, respectively. It is then clear that the family $(s_{i\lambda})$ satisfies the conditions (i), (ii), and (iii), so $r_{\mathscr{L},\psi}$ is everywhere defined and an immersion. □

Proposition 23.3.42. *Let Y be a quasi-compact scheme, $q : X \to Y$ be a morphism of finite type, $\mathscr{L}$ be an invertible $\mathscr{O}_X$-module, $\mathscr{S}$ be a quasi-coherent graded $\mathscr{O}_Y$-algebra, and $\psi : q^*(\mathscr{S}) \to \boldsymbol{S}(\mathscr{L})$ be a homomorphism of graded algebras. For the morphism $r_{\mathscr{L},\psi}$ to be defined everywhere and an immersion, it is necessary and sufficient that there exists an integer $n > 0$ and a quasi-coherent sub-$\mathscr{O}_Y$-module $\mathscr{E}$ of $\mathscr{S}_n$ of finite type such that:*

(a) the homomorphism $\psi_n \circ q^*(j_n) : q^*(\mathscr{E}) \to \mathscr{L}^{\otimes n}$ (where $j_n : \mathscr{E} \to \mathscr{S}_n$ is the canonical injection) is surjective.

(b) *if $\mathcal{S}'$ is the graded sub-$\mathcal{O}_Y$-algebra of $\mathcal{S}$ genrated by $\mathcal{E}$ and ψ' is the homomorphism $\psi \circ q^*(j')$, where $j' : \mathcal{S}' \to \mathcal{S}$ is the canonical injection, $r_{\mathcal{L},\psi'}$ is everywhere defined and an immersion.*

If these are true, any quasi-coherent sub-$\mathcal{O}_Y$-module $\mathcal{E}'$ of $\mathcal{S}_n$ containing $\mathcal{E}$ possesses the same properties, and so does the sub-$\mathcal{O}_Y$-module $\mathcal{S}'_{kn}$ of $\mathcal{S}_{kn}$ for any $k > 0$.

Proof. The sufficiency of these conditions is a particular case of Corollary 23.3.40 in view of the isomorphism between $\mathrm{Proj}(\mathcal{S})$ and $\mathrm{Proj}(\mathcal{S}^{(d)})$ (Proposition 23.3.6). We now prove the necessity, so let (U_i) be a finite affine open covering of Y and set $A_i = \Gamma(U_i, \mathcal{O}_Y)$. As $q^{-1}(U_i)$ is compact, the hypotheses that $r_{\mathcal{L},\psi}$ is an immersion defined on X implies by Proposition 23.3.39 the existence of a finite family (s_{ij}) of elements of $S^{(i)} = \Gamma(U_i, \mathcal{S})$ (where $s_{ij} \in S^{(i)}_{n_{ij}}$) satisfying conditions (i), (ii), and (iii). Since $q : X \to Y$ is of finite type, the restricted homomorphism $X_{f_{ij}} \to U_i$ is of finite type (where $f_{ij} = \psi^\flat(s_{ij})$), so the ring B_{ij} of $X_{f_{ij}}$ is an A_i-algebra of finite type, and we choose $(\psi^\flat(t_{ijk})|_{X_{f_{ij}}})(f_{ij}|_{X_{f_{ij}}})^{-m_{ijk}}$ to be a system of generators of B_{ij}, where $t_{ijk} \in S^{(i)}_{m_{ijk}n_{ij}}$. Let n be a common multiple of all the $m_{ijk}n_{ij}$ and put $s'_{ij} = s_{ij}^{h_{ij}} \in S^{(i)}_n$, where $h_{ij} = n/n_{ij}$. For any given piar (i, j, k), the element $t'_{ij} = s_{ij}^{h-m_{ijk}} t_{ijk}$ belongs to $S^{(i)}_n$, and it is clear that the $(\psi^\flat(t'_{ijk})|_{X_{f'_{ij}}})(f'_{ij}|_{X_{f'_{ij}}})^{-1}$ also generate B_{ij} (where $f'_{ij} = \psi^\flat(s'_{ij})$, and we note that $X_{f'_{ij}} = X_{f_{ij}}$). Let E_i be the sub-A_i-module of $S^{(i)}$ generated by these s'_{ij} and t'_{ijk}; then there exists a quasi-coherent sub-$\mathcal{O}_Y$-module $\mathcal{E}_i$ of $\mathcal{S}_n$ of finite type such that $\mathcal{E}_i|_{U_i} = \widetilde{E}_i$ (Theorem 22.6.60). It is then clear that the sub-$\mathcal{O}_Y$-module $\mathcal{E}$ of $\mathcal{E}$, which is the sum of the $\mathcal{E}_i$, satisfies the required properties. □

Remark 23.3.7. The point of Proposition 23.3.42 is that, for a scheme X of finite type over a quasi-compact scheme Y, if X can be embedded into $\mathrm{Proj}(\mathcal{S})$ via a morphism $r_{\mathcal{L},\psi}$, then we can choose $\mathcal{S}$ so that it is generated by $\mathcal{S}_1$ and $\mathcal{S}_1$ of finite type (we already know that in this case the twisted sheaves over $\mathrm{Proj}(\mathcal{S})$ have nice properties).

23.4 Projective bundles and ample sheaves

23.4.1 Projective bundles

Let Y be a scheme, $\mathcal{E}$ be a quasi-coherent $\mathcal{O}_Y$-module, and $\boldsymbol{S}(\mathcal{E})$ be the symmetric $\mathcal{O}_Y$-algebra of $\mathcal{E}$, which is quasi-coherent by Corollary 23.1.36. The **projective bundle** over Y associated with $\mathcal{E}$ is defined to be the Y-scheme $P = \mathrm{Proj}(\boldsymbol{S}(\mathcal{E}))$. The $\mathcal{O}_P$-module $\mathcal{O}_P(1)$ is called the **fundamental sheaf** of P.

If $\mathcal{E} = \mathcal{O}_Y^n$, we then denote by $\mathbb{P}_Y^{n-1}$ instead of $\mathbb{P}(\mathcal{E})$; if moreover Y is affine with ring A, we then denote this scheme by $\mathbb{P}_A^{n-1}$. As $\boldsymbol{S}(\mathcal{O}_Y)$ is canonically isomorphic to $\mathcal{O}_Y[T]$, we see $\mathbb{P}_Y^0$ is canonically identified with Y.

If $Y = \mathrm{Spec}(A)$ and $\mathcal{E} = \widetilde{E}$ where E is an A-module, we also denote by $\mathbb{P}(E)$ the projective bundle $\mathbb{P}(E)$. The simplest example is $\mathbb{P}(E)$ where E is a vector space over a field k. In this case, we see $\mathbb{P}(E)$ is isomorphic to $\mathbb{P}_k^{n-1}$, where n is the dimension of E.

Let $\mathcal{E}, \mathcal{F}$ be two qusi-coherent $\mathcal{O}_Y$-modules and $u : \mathcal{E} \to \mathcal{F}$ be an $\mathcal{O}_Y$-homomorphism. Then u corresponds canonically to a homomorphism $\boldsymbol{S}(u) : \boldsymbol{S}(\mathcal{E}) \to \boldsymbol{S}(\mathcal{F})$ of graded $\mathcal{O}_Y$-algebras. If u is surjective, so is $\boldsymbol{S}(u)$, and therefore $\mathrm{Proj}(\boldsymbol{S}(u))$ is a closed immersion $\mathbb{P}(\mathcal{F}) \to \mathbb{P}(\mathcal{E})$, which we then denoted by $\mathbb{P}(u)$. We can then say that $\mathbb{P}(\mathcal{E})$ is a contravariant functor on the category

of quasi-coherent $\mathcal{O}_Y$-modules with *surjective homomorphisms*. Suppose that u is surjective and put $P = \mathbb{P}(\mathscr{E})$, $Q = \mathbb{P}(\mathscr{F})$, and $j = \mathbb{P}(u)$. We then have an isomorphism

$$j^*(\mathcal{O}_P(n)) = \mathcal{O}_Q(n)$$

by Corollary 23.3.31.

If $\psi : Y' \to Y$ is a morphism and $\mathscr{E}' = \psi^*(\mathscr{E})$, we then have $\boldsymbol{S}_{\mathcal{O}_{Y'}}(\mathscr{E}') = \psi^*(\boldsymbol{S}_{\mathcal{O}_Y}(\mathscr{E}))$ by Proposition 23.1.34, so from Proposition 23.3.28 we deduce that

$$\mathbb{P}(\psi^*(\mathscr{E})) = \mathbb{P}(\mathscr{E}) \times_Y Y'. \tag{4.1.1}$$

Moreover, it is clear that $\psi^*((\boldsymbol{S}_{\mathcal{O}_Y}(\mathscr{E}))(n)) = (\boldsymbol{S}_{\mathcal{O}_{Y'}}(\mathscr{E}'))(n)$ for each $n \in \mathbb{Z}$, so if $P = \mathbb{P}(\mathscr{E})$ and $P' = \mathbb{P}(\mathscr{E}')$, we have a canonical isomorphism

$$\mathcal{O}_{P'}(n) = \mathcal{O}_P(n) \otimes_Y \mathcal{O}_{Y'}. \tag{4.1.2}$$

Proposition 23.4.1. *Let $\mathscr{L}$ be an invertible $\mathcal{O}_Y$-module. For any quasi-coherent $\mathcal{O}_Y$-module, there exists a canonical Y-isomorphism $i_{\mathscr{L}} : Q = \mathbb{P}(\mathscr{E} \otimes \mathscr{L}) \xrightarrow{\sim} P = \mathbb{P}(\mathscr{E})$. Moreover, $(i_{\mathscr{L}})_*(\mathcal{O}_Q(n))$ is cannically isomorphic to $\mathcal{O}_P(n) \otimes_Y \mathscr{L}^{\otimes n}$ for any $n \in \mathbb{Z}$.*

Proof. If A is a ring, E is an A-module, L is an A-module free of rank 1, we can define a canonical homomorphism

$$\boldsymbol{S}_n(E \otimes L) \to \boldsymbol{S}_n(E) \otimes L^{\otimes n}$$

which maps an element $(x_1 \otimes y_1) \cdots (x_n \otimes y_n)$ to

$$(x_1 \cdots x_n) \otimes (y_1 \otimes \cdots \otimes y_n)$$

where $x_i \in E$ and $y_i \in L$. This is easily seen to be an isomorphism, so we get an isomorphism $\boldsymbol{S}(E \otimes L) \cong \bigoplus_{n \geq 0} \boldsymbol{S}_n(E) \otimes L^{\otimes n}$. In the situation of the proposition, the preceding remark allows us to define a canonical isomorphism of graded $\mathcal{O}_Y$-algebras

$$\boldsymbol{S}(\mathscr{E} \otimes_{\mathcal{O}_Y} \mathscr{L}) \xrightarrow{\sim} \bigoplus_{n \geq 0} \boldsymbol{S}_n(\mathscr{E}) \otimes_{\mathcal{O}_Y} \mathscr{L}^{\otimes n}$$

The proposition then follows from Proposition 23.3.6 and Proposition 23.3.18. □

Let $P = \mathbb{P}(\mathscr{E})$ and denote by $p : P \to Y$ the structural morphism. As by definition $\mathscr{E} = (\boldsymbol{S}(\mathscr{E}))_1$, we have a canonical homomorphism $\alpha_1 : \mathscr{E} \to p_*(\mathcal{O}_P(1))$, and therefore a canonical homomorphism

$$\alpha_1^\sharp : p^*(\mathscr{E}) \to \mathcal{O}_P(1).$$

Proposition 23.4.2. *The canonical homomorphism $\alpha_1^\sharp$ is surjective.*

Proof. We have seen that $\alpha_1^\sharp$ corresponds to the functorial homomorphism $\mathscr{E} \otimes_{\mathcal{O}_Y} \boldsymbol{S}(\mathscr{E}) \to (\boldsymbol{S}(\mathscr{E}))(1)$ (see the remark before Proposition 23.3.19). Since $\mathscr{E}$ generates $\boldsymbol{S}(\mathscr{E})$, this homomorphism is surjective, whence our assertion in view of Proposition 23.3.13. □

23.4.2 Morphisms into $\mathbb{P}(\mathscr{E})$

With the notations of the last subsection, we now let X be an Y-scheme, $q : X \to Y$ be the structural morphism, and $r : X \to P$ be an Y-morphism, which gives a commutative diagram

$$\begin{tikzcd} X \arrow[r, "r"] \arrow[dr, "q"'] & P \arrow[d, "p"] \\ & Y \end{tikzcd}$$

As the functor r^* is right-exact, we deduce from the surjective homomorphism $\alpha_1^\sharp$ in Proposition 23.4.2 a surjective homomorphism

$$r^*(\alpha_1^\sharp) : r^*(p^*(\mathscr{E})) \to r^*(\mathscr{O}_P(1)).$$

But $r^*(p^*(\mathscr{E})) = q^*(\mathscr{E})$ and $r^*(\mathscr{O}_P(1))$ is locally isomorphic to $r^*(\mathscr{O}_P) = \mathscr{O}_X$, which is then an invertible sheaf $\mathscr{L}_r$ over X, so we obtain a canonical surjective $\mathscr{O}_X$-homomorphism

$$\varphi_r : q^*(\mathscr{E}) \to \mathscr{L}_r.$$

If $Y = \operatorname{Spec}(A)$ is affine and $\mathscr{E} = \widetilde{E}$, we can explicitly explain this homomorphism: given $f \in E$, it follows from Proposition 23.2.33 that

$$r^{-1}(D_+(f)) = X_{\varphi_r^\flat(f)}.$$

Let V be an affine open of X contained in $r^{-1}(D_+(f))$, and let B be its ring, which is an A-algebra; put $S = \boldsymbol{S}_A(E)$. The restriction of r to V then corresponds to an A-homomorphism $\omega : S_{(f)} \to B$, and we have $q^*(\mathscr{E})|_V = \widetilde{E \otimes_A B}$ and $\mathscr{L}_r|_V = \widetilde{L_r}$, where by Proposition 22.1.13, $L_r = S(1)_{(f)} \otimes_{S_{(f)}} B$. In view of the definition of α_1, the restriction of φ_r to $q^*(\mathscr{E})|_V$ therefore corresponds to the B-homomorphism

$$u : E \otimes_A B \to L_r, \quad x \otimes 1 \mapsto (x/1) \otimes 1 = (f/1) \otimes \omega(x/f)$$

The canonical extension of φ_r to a homomorphism of $\mathscr{O}_X$-algebras (recall that $(\mathscr{O}_P(1))^{\otimes n} = \mathscr{O}_P(n)$ by Corollary 23.2.29)

$$\psi_r : q^*(\boldsymbol{S}(\mathscr{E})) = \boldsymbol{S}(q^*(\mathscr{E})) \to \boldsymbol{S}(\mathscr{L}_r) = \bigoplus_{n\geq 0} \mathscr{L}_r^{\otimes n} = \bigoplus_{n\geq 0} r^*(\mathscr{O}_P(n))$$

is then such that the restriction of ψ_r to $q^*(\boldsymbol{S}_n(\mathscr{E}))|_V$ corresponds to the B-homomorphism

$$\boldsymbol{S}_n(\mathscr{E} \otimes_A B) = \boldsymbol{S}_n(E) \otimes_A B \to L_r^{\otimes n} = (S(1)_{(f)})^{\otimes n} \otimes_{S_{(f)}} B$$

which send the element $s \otimes 1$ to $(f/1)^{\otimes n} \otimes \omega(s/f^n)$.

Conversely, given an invertible $\mathscr{O}_X$-module $\mathscr{L}$ and a quasi-coherent $\mathscr{O}_Y$-module $\mathscr{E}$, then any homomorphism $\varphi : q^*(\mathscr{E}) \to \mathscr{L}$ corresponds to a canonical homomorphism of quasi-coherent $\mathscr{O}_X$-algebras

$$\psi : \boldsymbol{S}(q^*(\mathscr{E})) = q^*(\boldsymbol{S}(\mathscr{E})) \to \boldsymbol{S}(\mathscr{L}) = \bigoplus_{n\geq 0} \mathscr{L}^{\otimes n}$$

which then gives an Y-morphism $r_{\mathscr{L},\psi} : G(\psi) \to \mathrm{Proj}(\boldsymbol{S}(\mathscr{E})) \to \mathbb{P}(\mathscr{E})$, which we also denoted by $r_{\mathscr{L},\varphi}$. If φ is surjective, then so is ψ and by Corollary 23.3.34 the morphism $r_{\mathscr{L},\psi}$ is everywhere defined.

Proposition 23.4.3. *Let $q : X \to Y$ be a morphism and $\mathscr{E}$ be a quasi-coherent $\mathscr{O}_Y$-module. Then the maps $r \mapsto (\mathscr{L}_r, \varphi_r)$ and $(\mathscr{L}, \varphi) \mapsto r_{\mathscr{L},\varphi}$ form a bijective correspondence between the set of Y-morphisms $r : X \to \mathbb{P}(\mathscr{E})$ to the set of equivalence classes of couples $(\mathscr{L}, \varphi)$ formed by an invertible $\mathscr{O}_X$-module and a surjective homomorphism $\varphi : q^*(\mathscr{E}) \to \mathscr{L}$, where two couples $(\mathscr{L}, \varphi)$, $(\mathscr{L}', \varphi')$ are equivalent if there exists an $\mathscr{O}_X$-isomorphism $\tau : \mathscr{L} \to \mathscr{L}'$ such that $\varphi' = \tau \circ \varphi$.*

Proof. Let us start with an Y-morphism $r : X \to \mathbb{P}(\mathscr{E})$, form $\mathscr{L}_r$ and φ_r, and put $r' = r_{\mathscr{L}_r,\varphi_r}$. To see the morphisms r and r' coincide, we may assume that $Y = \mathrm{Spec}(A)$ is affine, so $\mathscr{E} = \widetilde{E}$, and let $S = \boldsymbol{S}_A(E)$. Let $V = \mathrm{Spec}(B)$ be an affine open of X contained in $r^{-1}(D_+(f))$, where $f \in E$. Then as we have already seen, the restriction of r to V corresponds to an A-homomorphism $\omega : S_{(f)} \to B$, and the restriction of ψ_r to $q^*(\boldsymbol{S}_n(\mathscr{E}))|_V$ corresponds to the B-homomorphism $\boldsymbol{S}_n(E) \otimes_A B \to L_r^{\otimes n}$ which sends $s \otimes 1$ to $(f/1)^{\otimes n} \otimes \omega(s/f^n)$. The restriction of $\psi_r^\flat$ to $\boldsymbol{S}(\mathscr{E})|_V$ then corresponds to the homomorphism $\boldsymbol{S}_n(E) \to L_r^{\otimes n}$ which sends $s \in \boldsymbol{S}_n(E)$ to $(f/1)^{\otimes n} \otimes \omega(s/f^n)$, and by Proposition 23.3.33, the restriction of $r_{\mathscr{L}_r,\psi_r}$ to V corresponds to the homomorphism $(\psi_r^\flat)_{(f)}$, which send $s \in S_n$ to

$$(\psi_r^\flat(s))(\psi_r^\flat(f))^{-n} = [(f/1)^{\otimes n} \otimes \omega(s/f^n)][(f/1) \otimes 1]^{-n} = 1 \otimes \omega(s/f^n).$$

Therefore, under the identification of X with $\mathrm{Proj}(\boldsymbol{S}(\mathscr{L}))$, $r_{\mathscr{L},\psi_r}$ coincides with r over V, so they coincide on X.

Conversely. let $(\mathscr{L}, \varphi)$ be a couple and form $r = r_{\mathscr{L},\varphi}$, $\mathscr{L}_r$, and φ_r. We show that there is a canonical isomorphism $\tau : \mathscr{L}_r \to \mathscr{L}$ such that $\varphi = \tau \circ \varphi_r$. For this, we can assume that $Y = \mathrm{Spec}(A)$ and $X = \mathrm{Spec}(B)$ are affine, and (with the notations of Remark 23.3.4) define τ be sending an element $(x/1) \otimes 1$ of L_r (where $x \in E$) to the element $v_1(x)c$ of L. It is easy to verify that τ is independent of the choice of the generator c of L. As v_1 is surjective, to show that τ is an isomorphism, it suffices to prove that if $x/1 = 0$ in $S(1)_{(f)}$, then $v_1(x)/1 = 0$ in B_g. But the first condition means that $f^n x = 0$ in S_{n+1} for some n, and we then deduce that $v_{n+1}(f^n x) = g^n v_1(x) = 0$ in B, whence the conclusion. Finally, it is immediate that for two equivalent couples $(\mathscr{L}, \varphi)$, $(\mathscr{L}', \varphi')$, we have $r_{\mathscr{L},\varphi} = r_{\mathscr{L}',\varphi'}$. □

Theorem 23.4.4. *The set of Y-sections of $\mathbb{P}(\mathscr{E})$ is in bijective correspondence to the set of quasi-coherent sub-$\mathscr{O}_Y$-modules $\mathscr{F}$ of $\mathscr{E}$ such that $\mathscr{E}/\mathscr{F}$ is invertible.*

Proof. This is a particular case of Proposition 23.4.3 by taking $X = Y$ and note that if two pairs $(\varphi, \mathscr{L})$ and $(\varphi', \mathscr{L}')$ are equivalent, then $\ker \varphi$ and $\ker \varphi'$ are identical. □

Note that this property corresponds to the classical definition of the "projective space" as the set of hyperplanes of a vector space (the classical case corresponding to $Y = \mathrm{Spec}(k)$, where k is a field, and $\mathscr{E} = \widetilde{E}$, E being a finite dimensional k-vector. The sheaves $\mathscr{F}$ having the property stated in Theorem 23.4.4 corresponds then to the hyperplanes of E.

Remark 23.4.1. As there is a canonical correspondence between Y-morphisms from X to P and their graph morphisms, which are X-sections of $P \times_Y X$, we see conversely that Proposition 23.4.3 can be deduced from Theorem 23.4.4. Let $\mathrm{Hyp}_Y(X, \mathscr{E})$ be the set of quasi-coherent

sub-$\mathscr{O}_X$-modules $\mathscr{F}$ of $\mathscr{E} \otimes_Y \mathscr{O}_X = q^*(\mathscr{E})$ such that $q^*(\mathscr{E})/\mathscr{F}$ is an invertible $\mathscr{O}_X$-module. If $g : X' \to X$ is an Y-morphism, then $g^*(q^*(\mathscr{E})/\mathscr{F}) = g^*(q^*(\mathscr{E}))/g^*(\mathscr{F})$ by the right exactness of g^*, so the second sheaf is invertible, and therefore $\mathrm{Hyp}_Y(X, \mathscr{E})$ is a covariant functor over the category of Y-schemes. We can then interprete Theorem 23.4.4 by saying that the Y-scheme $\mathbb{P}(\mathscr{E})$ representes the functor $\mathrm{Hyp}_Y(-, \mathscr{E})$. This also provides a characterization of the projective bundle $P = \mathbb{P}(\mathscr{E})$ by the following universal property, more close to the geometric intuition that the constructions of $r_{\mathscr{L},\psi}$: for any morphism $q : X \to Y$ and any invertible $\mathscr{O}_X$-module $\mathscr{L}$ which is a quotient of $q^*(\mathscr{E})$, there exists a unique Y-morphism $r : X \to P$ such that $\mathscr{L}$ is isomorphic to $r^*(\mathscr{O}_P(1))$.

Corollary 23.4.5. *Suppose that any invertible $\mathscr{O}_Y$-module is trivial. Let $E = \mathrm{Hom}_{\mathscr{O}_Y}(\mathscr{E}, \mathscr{O}_Y)$ considered as a module over the ring $A = \Gamma(Y, \mathscr{O}_Y)$, and let $E^\times$ be the subset of E formed by surjective homomorphisms. Then the set of Y-sections of $\mathbb{P}(\mathscr{E})$ is canonically identified with $E^\times/A^\times$, where $A^\times$ is the group of units of A.*

Example 23.4.6. Let Y be a scheme, y be a point of Y, and $Y' = \mathrm{Spec}(\kappa(y))$. The fiber $p^{-1}(y)$ of $\mathbb{P}(\mathscr{E})$ is, in view of (4.1.1), identified with $\mathbb{P}(\mathscr{E}^y)$, where $\mathscr{E}^y = \mathscr{E}_y \otimes_{\mathscr{O}_{Y,y}} \kappa(y) = \mathscr{E}_y/\mathfrak{m}_y\mathscr{E}_y$ is considered as a vector space over $\kappa(y)$. More generally, if K is an extension of $\kappa(y)$, $p^{-1}(y) \otimes_{\kappa(y)} K$ is identified with $\mathbb{P}(\mathscr{E}^y \otimes_{\kappa(y)} K)$. Since any invertible sheaves over a local scheme is trivial, Corollary 23.4.5 shows that the points of $\mathbb{P}(\mathscr{E})$ lying over y with values in K, which are called the **rational geometric fibers** of $\mathbb{P}(\mathscr{E})$ over K lying over y, is identified with the projective space of the dual of the vector K-space $\mathscr{E}^y \otimes_{\kappa(y)} K$.

Example 23.4.7. Suppose now that Y is affine with ring A, and any invertible sheaf on Y is trivial; we put $\mathscr{E} = \mathscr{O}_Y^n$. Then with the notations of Corollary 23.4.5, E is identified with A^n by Corollary 22.1.3 and $E^\times$ is identified with the set of systems $(f_i)_{1\leq i\leq n}$ of elements of A which generate the unit ideal of A. By Corollary 23.4.5, two such systems determine the same Y-section of $\mathbb{P}_Y^{n-1} = \mathbb{P}_A^{n-1}$, which means the same point of $\mathbb{P}_A^{n-1}$ with values in A, if and only if one is deduced from the other by multiplication by an invertible element of A.

Remark 23.4.2. Let $u : X' \to X$ be a morphism. If the Y-morphism $r : X \to P$ corresponds to the homomorphism $\varphi : q^*(\mathscr{E}) \to \mathscr{L}$, then by definition, the morphism $r \circ u$ corresponds to $u^*(\varphi) : u^*(q^*(\mathscr{E})) \to u^*(\mathscr{L})$. On the other hand, let $\mathscr{E}, \mathscr{F}$ be two quasi-coherent $\mathscr{O}_Y$-modules and $j = \mathbb{P}(v)$ be the closed immersion $\mathbb{P}(\mathscr{F}) \to \mathbb{P}(\mathscr{E})$ corresponding to a surjective homomorphism $v : \mathscr{E} \to \mathscr{F}$. If the Y-morphism $r : X \to \mathbb{P}(\mathscr{E})$ corresponds to the homomorphism $\varphi : q^*(\mathscr{E}) \to \mathscr{L}$, then $j \circ r$ corresponds to the composition

$$q^*(\mathscr{E}) \xrightarrow{q^*(v)} q^*(\mathscr{F}) \xrightarrow{\varphi} \mathscr{L}$$

Let $\psi : Y' \to Y$ be a morphism and put $\mathscr{E}' = \psi^*(\mathscr{E})$. If the Y-morphism $r : X \to P$ corresponds to the homomorphism $\varphi : q^*(\mathscr{E}) \to \mathscr{L}$, the Y'-morphism

$$r_{(Y')} : X_{(Y')} \to P' = \mathbb{P}(\mathscr{E}')$$

correspond to $\varphi_{(Y')} : q^*_{(Y')}(\mathscr{E}') = q^*(\mathscr{E}) \otimes_Y \mathscr{O}_{Y'} \to \mathscr{L} \otimes_Y \mathscr{O}_{Y'}$. In fact, by (4.1.1), we have the

following commutative diagram

$$\begin{tikzcd} X_{(Y')} \arrow[r, "r_{(Y')}"] \arrow[d, "v"] & P' = P_{(Y')} \arrow[r, "p_{(Y')}"] \arrow[d, "u"] & Y' \arrow[d, "\psi"] \\ X \arrow[r, "r"] & P \arrow[r, "p"] & Y \end{tikzcd}$$

In view of (4.1.2), we have

$$(r_{(Y')})^*(\mathscr{O}_{P'}(1)) = (r_{(Y')})^*(u^*(\mathscr{O}_P(1))) = v^*(r^*(\mathscr{O}_P(1))) = v^*(\mathscr{L}) = \mathscr{L} \otimes_Y \mathscr{O}_{Y'}.$$

Also, $u^*(\alpha_1^\sharp)$ is equal to the canonical homomorphism $\alpha_1^\sharp : (p_{(Y')})^*(\mathscr{E}') \to \mathscr{O}_{P'}(1)$, in view of the definition of α_1, whence our assertion.

23.4.3 The Segre morphism

Let Y be a scheme and $\mathscr{E}, \mathscr{F}$ be two quasi-coherent $\mathscr{O}_Y$-modules. Put $P_1 = \mathbb{P}(\mathscr{E})$, $P_2 = \mathbb{P}(\mathscr{F})$, and denote by p_1, p_2 their morphisms; let $Q = P_1 \times_Y P_2$ and q_1, q_2 be the canonical projections. The $\mathscr{O}_Q$-module

$$\mathscr{L} = \mathscr{O}_{P_1}(1) \times_Y \mathscr{O}_{P_2}(1) = q_1^*(\mathscr{O}_{P_1}(1)) \times_{\mathscr{O}_Q} q_2^*(\mathscr{O}_{P_2}(1))$$

is invertible as a tensor product of invertible modules. On the other hand, if $r = p_1 \circ q_1 = p_2 \circ q_2$ is the structural morphism of Q, we have $r^*(\mathscr{E} \otimes_{\mathscr{O}_Y} \mathscr{F}) \otimes_{\mathscr{O}_Q} q_2^*(p_2^*(\mathscr{F}))$; the canonical surjective homomorphism $p_1^1(\mathscr{E}) \to \mathscr{O}_{P_1}(1)$ and $p_2^*(\mathscr{F}) \to \mathscr{O}_{P_2}(1)$ then give a canonical surjective homomorphism

$$s : r^*(\mathscr{E} \otimes_{\mathscr{O}_Y} \mathscr{F}) \to \mathscr{L} \tag{4.3.1}$$

we then deduce a canonical homomorphism, called the Segre morphism:

$$\zeta : \mathbb{P}(\mathscr{E}) \times_Y \mathbb{P}(\mathscr{F}) \to \mathbb{P}(\mathscr{E} \otimes_{\mathscr{O}_Y} \mathscr{F}). \tag{4.3.2}$$

To explain this morphism ζ, let us consider the case where $Y = \operatorname{Spec}(A)$ is affine, $\mathscr{E} = \widetilde{E}$, $\mathscr{F} = \widetilde{F}$, where E and F are two A-module; whence $\mathscr{E} \otimes_{\mathscr{O}_Y} \mathscr{F} = \widetilde{E \otimes_A F}$. Put $R = \boldsymbol{S}(E)$, $S = \boldsymbol{S}(F)$, and $T = \boldsymbol{S}(E \otimes_A F)$. Let $f \in E$, $g \in F$, and consider the affine open

$$D_+(f) \times_Y D_+(g) = \operatorname{Spec}(B)$$

of Q, where $B = R_{(f)} \otimes_A S_{(g)}$. The restriction of $\mathscr{L}$ on this affine open is $\widetilde{L}$, where

$$L = (R(1)_{(f)}) \otimes_A (S(1)_{(g)})$$

and the element $c = (f/1) \otimes (g/1)$ is a generator of L as a free B-module (Proposition 23.2.24). The homomorphism (4.3.1) then corresponds to the homomorphism

$$(x \otimes y) \otimes b \mapsto b((x/1) \otimes (y/1))$$

from $(E \otimes_A F) \otimes_A B$ to L. With the notations of Remark 23.3.4, we then have $v_1(x \otimes y) = (x/f) \otimes (y/g)$, so the restriction of the morphism ζ to $D_+(f) \times_Y D_+(g)$ is a morphism from this

affine scheme to $D_+(f \otimes g)$, which corresponds to the ring homomorphism

$$\omega((x \otimes y)/(f \otimes g)) = (x/f) \otimes (y/g) \tag{4.3.3}$$

for $x \in E$ and $y \in F$.

From Proposition 23.4.3, there is a canonical isomorphism

$$\tau : \zeta^*(\mathscr{O}_P(1)) \xrightarrow{\sim} \mathscr{O}_{P_1}(1) \otimes_Y \mathscr{O}_{P_2}(1)$$

where we put $P = \mathbb{P}(\mathscr{E} \otimes_{\mathscr{O}_Y} \mathscr{F})$. Moreover, for $x \in \Gamma(Y, \mathscr{E})$ and $y \in \Gamma(Y, \mathscr{F})$, we have

$$\tau(\alpha_1(x \otimes y)) = \alpha_1(x) \otimes \alpha_1(y) \tag{4.3.4}$$

To see this, we can assume that Y is affine, so with the notations above and the definition of α_1, we have $\alpha_1^{f\otimes g}(x \otimes y) = (x \otimes y)/1$, $\alpha_1^f(x) = x/1$, and $\alpha_1^g(y) = y/1$. The definition of τ given in the proof of Proposition 23.4.3 says τ maps $(x/1) \otimes 1$ to $v_1(x)c$. Since we have seen that $v_1(x \otimes y) = (x/f) \otimes (y/g)$, this implies the assertion by a simple computation. From this, we then deduce the formula

$$\zeta^{-1}(P_{x\otimes y}) = (P_1)_x \times_Y (P_2)_y \tag{4.3.5}$$

where we need to use the following lemma:

Lemma 23.4.8. *Let B, B' be two A-algebras, and let $Y = \mathrm{Spec}(A)$, $Z = \mathrm{Spec}(B)$, $Z' = \mathrm{Spec}(B')$. Then for $t \in B$, $t' \in B'$, we have $D(t \otimes t') = D(t) \times_Y D(t')$.*

Proof. Let p, p' be the canonical projections of $Z \times_Y Z'$. Then it follows from Proposition 10.4.18 that $p^{-1}(D(t)) = D(t \otimes 1)$ and $p'^{-1}(D(t')) = D(1 \otimes t')$. Corollary 22.3.2 then implies the lemma, since $(t \otimes 1)(1 \otimes t') = t \otimes t'$. □

Proposition 23.4.9. *The Segre morphism is a closed immersion.*

Proof. Since the question is local on Y, we can assume that Y is affine. With the previous notations, the $D_+(f \otimes g)$ form a basis for P, since the elements $f \otimes g$ generate T for $f \in E$, $g \in F$. On the other hand, we have $\zeta^{-1}(D_+(f \otimes g)) = D_+(f) \times_Y D_+(g)$ in view of (4.3.5). It then suffices to use Corollary 22.4.10 to prove that the restriction of ζ to $D_+(f) \times_Y D_+(g)$ is a closed immersion into $D_+(f \otimes g)$. But this is a morphism between affine schemes whose corresponding ring homomorphism ω is surjective in view of the formula (4.3.3), so our assertion follows. □

The Segre morphism is functorial on $\mathscr{E}$ and $\mathscr{F}$ if we restrict ourselves to quasi-coherent $\mathscr{O}_Y$-modules with *surjective* homomorphisms. To see this, it suffices to consider a surjective $\mathscr{O}_Y$-homomorphism $\mathscr{E} \to \mathscr{E}'$ and prove that the following diagram is commutative

$$\begin{tikzcd}
\mathbb{P}(\mathscr{E}') \times \mathbb{P}(\mathscr{F}) \arrow[r, "j\times 1"] \arrow[d, "\zeta"'] & \mathbb{P}(\mathscr{E}') \times \mathbb{P}(\mathscr{F}) \arrow[d, "\zeta"] \\
\mathbb{P}(\mathscr{E}' \otimes \mathscr{F}) \arrow[r] & \mathbb{P}(\mathscr{E} \otimes \mathscr{F})
\end{tikzcd}$$

where j is the canonical closed immersion $\mathbb{P}(\mathscr{E}') \to \mathbb{P}(\mathscr{E})$. Put $P'_1 = \mathbb{P}(\mathscr{E}')$ and retain the previous notations; $j \times 1$ is a closed immersion by Proposition 23.3.30 and we have

$$(j \times 1)^*(\mathscr{O}_{P_1}(1) \otimes \mathscr{O}_{P_2}(1)) = j^*(\mathscr{O}_{P_1}(1)) \otimes \mathscr{O}_{P_2}(1) = \mathscr{O}_{P'_1}(1) \otimes \mathscr{O}_{P_2}(1)$$

in view of (4.1.2) and Corollary 22.3.14. The assertion then follows from Remark 23.4.2.

Proposition 23.4.10. *Let $\psi : Y \to Y'$ be a morphism and put $\mathscr{E}' = \psi^*(\mathscr{E})$, $\mathscr{F}' = \psi^*(\mathscr{F})$. Then the Segre morphism $\mathbb{P}(\mathscr{E}') \times \mathbb{P}(\mathscr{F}') \to \mathbb{P}(\mathscr{E}' \otimes \mathscr{F}')$ is identified with $\zeta_{(Y')}$.*

Proof. Put $P'_1 = \mathbb{P}(\mathscr{E}')$ and $P'_2 = \mathbb{P}(\mathscr{F}')$. Then by Remark 23.4.2, P'_i is identified with $(P_i)_{(Y')}$ for $i = 1, 2$, so the structural morphism $P'_1 \times_{Y'} P'_2 \to Y'$ is identified with $r_{(Y')}$, where r is the structural morphism of $P_1 \times_Y P_2$. On the other hand, $\mathscr{E}' \otimes \mathscr{F}'$ is identified with $\psi^*(\mathscr{E} \otimes \mathscr{F})$, so $\mathbb{P}(\mathscr{E}' \otimes \mathscr{F}')$ is identified with $\mathbb{P}(\mathscr{E} \otimes \mathscr{F})_{(Y')}$ by Proposition 23.3.28. Finally, $\mathscr{O}_{P'_1}(1) \otimes_{Y'} \mathscr{O}_{P'_2}(1) = \mathscr{L}$ is identified with $\mathscr{L} \otimes_Y \mathscr{O}_{Y'}$ in view of (4.1.2) and Proposition 22.3.13. The canonical homomorphism $(r_{(Y')})^*(\mathscr{E}' \otimes \mathscr{F}') \to \mathscr{L}'$ is then identified with $s_{(Y')}$, and our assertion follows from Proposition 23.4.3. □

Remark 23.4.3. The coproduct of $\mathbb{P}(\mathscr{E})$ and $\mathbb{P}(\mathscr{F})$ is similarly canonical isomorphic to a closed subscheme of $\mathbb{P}(\mathscr{E} \oplus \mathscr{F})$. In fact, the surjective homomorphisms $\mathscr{E} \oplus \mathscr{F} \to \mathscr{E}$, $\mathscr{E} \oplus \mathscr{F} \to \mathscr{F}$ correspond to closed immersions $\mathbb{P}(\mathscr{E}) \to \mathbb{P}(\mathscr{E} \oplus \mathscr{F})$, $\mathbb{P}(\mathscr{E}) \to \mathbb{P}(\mathscr{E} \oplus \mathscr{F})$; it then boils down to showing that the underlying spaces of these closed subschemes of $\mathbb{P}(\mathscr{E} \oplus \mathscr{F})$ thus obtained have no common point. The question being local on Y, we can assume that Y is affine adapt our previous notations. Now $\boldsymbol{S}_n(E)$ and $\boldsymbol{S}_n(F)$ are identified with submodules of $S_n(E \oplus F)$ with intersection reduced to 0, and if $\mathfrak{p}$ is a graded prime ideal of $\boldsymbol{S}(E)$ such that $\mathfrak{p} \cap S_n(E) \neq S_n(E)$ for all $n \geq 0$, then it corresponds to a unique graded prime ideal in $\boldsymbol{S}(E \oplus F)$ whose trace on $\boldsymbol{S}_n(E)$ is $\mathfrak{p} \cap S_n(E)$, but which contains $S_+(F)$. Therefore, two distinct points of $\operatorname{Proj}(\boldsymbol{S}(E))$ and $\operatorname{Proj}(\boldsymbol{S}(F))$ can not have same image in $\operatorname{Proj}(\boldsymbol{S}(E \oplus F))$.

23.4.4 Very ample sheaves

Proposition 23.4.11. *Let Y be a quasi-compact scheme, $q : X \to Y$ a morphism of finite type, and $\mathscr{L}$ be an invertible $\mathscr{O}_X$-module.*

(a) Let $\mathscr{S}$ be a quasi-coherent graded $\mathscr{O}_Y$-algebra and $\psi : q^*(\mathscr{S}) \to \boldsymbol{S}(\mathscr{L})$ be a graded homomorphism of algebras. For the morphism $r_{\mathscr{L},\psi}$ to be everywhere defined and an immersion, it is necessary and sufficent that there exists an integer $n \geq 0$ and a quasi-coherent sub-$\mathscr{O}_Y$-module of finite type $\mathscr{E}$ of $\mathscr{S}_n$ such that the homomorphism $\varphi' = \psi_n \circ q^*(j) : q^*(\mathscr{E}) \to \boldsymbol{S}(\mathscr{L}) = \mathscr{L}'$ ($j : \mathscr{E} \to \mathscr{S}_n$ being the canonical injection) is surjective and the morphism $r_{\mathscr{L}',\varphi'} : X \to \mathbb{P}(\mathscr{E})$ is an immersion.

(b) Let $\mathscr{F}$ be a quasi-coherent $\mathscr{O}_Y$-module and $\varphi : q^*(\mathscr{F}) \to \mathscr{L}$ be a surjective homomorphism. For the morphism $r_{\mathscr{L},\varphi} : X \to \mathbb{P}(\mathscr{F})$ to be an immersion, it is necessary and sufficent that there exists a quasi-coherent sub-$\mathscr{O}_Y$-module of finite type $\mathscr{E}$ of $\mathscr{F}$ such that the homomorphism $\varphi' = \varphi \circ q(j) : q^*(\mathscr{E}) \to \mathscr{L}$ (where $j : \mathscr{E} \to \mathscr{F}$ is the canonical injection) is surjective and such that $r_{\mathscr{L},\varphi'} : X \to \mathbb{P}(\mathscr{E})$ is an immersion.

Proof. We first consider case (a). The fact that $r_{\mathscr{L},\psi}$ is everywhere defined and an immersion is equivalent by Proposition 23.3.42 to the existence of an integer $n > 0$ and $\mathscr{E}$ such that, if $\mathscr{S}'$ is

the subalgebra of $\mathscr{S}$ generated by $\mathscr{E}$, the homomorphism $q^*(\mathscr{E}) \to \mathscr{L}^{\otimes n}$ is surjective and $r_{\mathscr{L},\psi'} : X \to \mathrm{Proj}(\mathscr{S}')$ is everywhere defined and an immersion. We also have a closed immersion corresponding to the surjective homomorphism $\boldsymbol{S}(\mathscr{E}) \to \mathscr{S}'$, so these the morphism $X \to \mathbb{P}(\mathscr{E})$ is an immersion.

Now consider the situation of (b). As $\mathscr{F}$ is the inductive limit of its quasi-coherent submodules of finite type $\mathscr{E}_\lambda$ (Corollary 22.6.62), $\boldsymbol{S}(\mathscr{F})$ is the inductive limit of the $\boldsymbol{S}(\mathscr{E}_\lambda)$, so by Proposition 23.3.41 there exists λ such that $r_{\mathscr{L},\varphi_\mu}$ is everywhere defined and an immersion for $\mu \geq \lambda$. Also, since the functor f^* is left-adjoint, it commutes with inductive limits and therefore $q^*(\mathscr{F})$ is the inductive limits of the $q^*(\mathscr{E}_\lambda)$. Since $\mathscr{L}$ is an $\mathscr{O}_X$-module of finite type and $q^*(\mathscr{F}) \to \mathscr{L}$ is surjective, it follows from Proposition 19.4.10 that there exists λ' such that $q^*(\mathscr{E}_\mu) \to \mathscr{L}$ is surjective for $\mu \geq \lambda'$. It then suffices to choose $\mathscr{E} = \mathscr{E}_\mu$ for $\mu \geq \lambda$ and $\mu \geq \lambda'$. □

Let Y be a scheme and $q : X \to Y$ be a morphism. We say an invertible $\mathscr{O}_X$-module $\mathscr{L}$ is **very ample for q** (or **very ample relative to q**, or simple **very ample**) if there exists a quasi-coherent $\mathscr{O}_Y$-module $\mathscr{E}$ and a Y-immersion $r : X \to \mathbb{P}(\mathscr{E})$ such that $\mathscr{L}$ is isomorphic to $r^*(\mathscr{O}_P(1))$. In view of Proposition 23.4.3, this is equivalent to the existence of a quasi-coherent $\mathscr{O}_Y$-module $\mathscr{E}$ and a surjective homomorphism $\varphi : q^*(\mathscr{E}) \to \mathscr{L}$ such that the associated morphism $r_{\mathscr{L},\varphi} : X \to \mathbb{P}(\mathscr{E})$ is an immersion. We also note that the existence of a very ample $\mathscr{O}_X$-module relative to Y implies that q is separated (Proposition 23.2.14 and Proposition 22.5.25).

Corollary 23.4.12. *Suppose that there exists a quasi-coherent $\mathscr{O}_Y$-algebra $\mathscr{S}$ genrated by $\mathscr{S}_1$ and a Y-immersion $r : X \to P = \mathrm{Proj}(\mathscr{S})$ such that $\mathscr{L} \cong r^*(\mathscr{O}_P(1))$. Then $\mathscr{L}$ is very ample relative to q.*

Proof. If $\mathscr{F} = \mathscr{S}_1$, the canonical homomorphism $\boldsymbol{S}(\mathscr{F}) \to \mathscr{S}$ is surjective, so by composing r with the corresponding closed immersion $\mathrm{Proj}(\mathscr{S}) \to \mathbb{P}(\mathscr{F})$, we obtain an immersion $r' : X \to \mathbb{P}(\mathscr{F}) = P'$ such that $\mathscr{L}$ is isomorphic to $r'^*(\mathscr{O}_{P'}(1))$. □

Proposition 23.4.13. *Let $q : X \to Y$ be a quasi-compact morphism and $\mathscr{L}$ be an invertible $\mathscr{O}_X$-module. Then $\mathscr{L}$ is very ample relative to q if and only if $q_*(\mathscr{L})$ is quasi-coherent, the cannical homomorphism $\sigma : q^*(q_*(\mathscr{L})) \to \mathscr{L}$ is surjective, and the morphism $r_{\mathscr{L},\sigma} : X \to \mathbb{P}(q_*(\mathscr{L}))$ is an immersion.*

Proof. As q is quasi-compact, $q_*(\mathscr{L})$ is quasi-coherent if q is separated (Proposition 22.6.54). By Remark 23.3.3, the existence of a surjective homomorphism $\varphi : q^*(\mathscr{E}) \to \mathscr{L}$ ($\mathscr{E}$ being a quasi-coherent $\mathscr{O}_Y$-module) implies that σ is surjective. Moreover, the factorization $\varphi : q^*(\mathscr{E}) \to q^*(q_*(\mathscr{L})) \xrightarrow{\sigma} \mathscr{L}$ of (3.4.3) corresponds to a canonical factorization (recall that q^* commutes with $\boldsymbol{S}$)

$$q^*(\boldsymbol{S}(\mathscr{E})) \longrightarrow q^*(\boldsymbol{S}(q_*(\mathscr{L}))) \longrightarrow \boldsymbol{S}(\mathscr{L})$$

so by Corollary 23.3.40 the hypothesis that $r_{\mathscr{L},\varphi}$ is an immersion implies that $j = r_{\mathscr{L},\sigma}$ is an immersion. Moreover, by Proposition 23.4.3, $\mathscr{L}$ is isomorphic to $j^*(\mathscr{O}_{P'}(1))$ where $P' = \mathbb{P}(q_*(\mathscr{L}))$. The converse of this is clear by the definition of very ampleness. □

Corollary 23.4.14. *Let $q : X \to Y$ be a quasi-compact morphism and $\mathscr{L}$ be an invertible $\mathscr{O}_X$-module. For $\mathscr{L}$ to be very ample relative to Y, it is necessary and sufficent that there exists an open covering (U_α) of Y such that $\mathscr{L}|_{q^{-1}(U_\alpha)}$ is very ample relative to U_α for each α.*

Proof. This follows from the fact that the criterion of Proposition 23.4.13 is local over Y. □

Proposition 23.4.15. *Let Y be a quasi-compact scheme, $q : X \to Y$ a morphism of finite type, and $\mathscr{L}$ be an invertible $\mathscr{O}_X$-module. Then the following conditions are equivalent:*

(i) $\mathscr{L}$ is very ample relative to Y.

(ii) There exists a quasi-coherent $\mathscr{O}_Y$-module $\mathscr{E}$ of finite type and a surjective homomorphism $\varphi : q^*(\mathscr{E}) \to \mathscr{L}$ such that $r_{\mathscr{L},\varphi}$ is an immersion.

(iii) There exists a coherent sub-$\mathscr{O}_Y$-module of finite type $\mathscr{E}$ of $q_*(\mathscr{L})$ and a surjective homomorphism $\varphi : q^*(\mathscr{E}) \to \mathscr{L}$ such that $r_{\mathscr{L},\varphi}$ is an immersion.

Proof. It is clear that (ii) or (iii) implies (i); but (i) implies (ii) by Proposition 23.4.11, and similarly (i) implies (iii) in view of Proposition 23.4.13. □

Corollary 23.4.16. *Suppose that Y is a quasi-compact scheme. If $\mathscr{L}$ is very ample relative to Y, there exists a quasi-coherent graded $\mathscr{O}_Y$-algebra $\mathscr{S}$ generated by $\mathscr{S}_1$ and such that $\mathscr{S}_1$ is of finite type, and a dominant open Y-immersion $i : X \to P = \mathrm{Proj}(\mathscr{S})$ such that $\mathscr{L}$ is isomorphic to $i^*(\mathscr{O}_P(1))$.*

Proof. Since $\mathscr{L}$ is very ample, by Proposition 23.4.15 there exists a coherent sub-$\mathscr{O}_Y$-module of finite type $\mathscr{E}$ of $q_*(\mathscr{L})$ and a surjective homomorphism $\varphi : q^*(\mathscr{E}) \to \mathscr{L}$ such that $r_{\mathscr{L},\varphi}$ is an immersion. The structural morphism $p : P' = \mathbb{P}(\mathscr{E}) \to Y$ is then separated and of finite type (Proposition 23.3.21), so P' is a quasi-compact scheme if Y is quasi-compact. Let Z be scheme theoretic image of X in P', with underlying space $\overline{j(X)}$, where $j = r_{\mathscr{L},\varphi}$; then j factors through Z into a dominant open immersion $i : X \to Z$. But Z is identified with the scheme $\mathrm{Proj}(\mathscr{S})$, where $\mathscr{S}$ is the quotient graded $\mathscr{O}_Y$-algebra of $\boldsymbol{S}(\mathscr{E})$ by a quasi-coherent graded ideal (Proposition 23.3.30), and it is clear that $\mathscr{S}_1$ is generated by $\mathscr{S}$ (since $\boldsymbol{S}(\mathscr{E})$ satisfies this condition). Moreover, by Corollary 23.3.31, $\mathscr{O}_Z(1)$ is the inverse image of $\mathscr{O}_{P'}(1)$ under the canonical injection, so $\mathscr{L} = i^*(\mathscr{O}_Z(1))$. □

Proposition 23.4.17. *Let $q : X \to Y$ be a morphism, $\mathscr{L}$ be a very ample $\mathscr{O}_X$-module relative to q, and $\mathscr{L}'$ be an invertible $\mathscr{O}_X$-module such that there exists a quasi-coherent $\mathscr{O}_Y$-module $\mathscr{E}'$ and a surjective homomorphism $q^*(\mathscr{E}') \to \mathscr{L}'$. Then $\mathscr{L} \otimes_{\mathscr{O}_X} \mathscr{L}'$ is very ample relative to q.*

Proof. The hypothesis on $\mathscr{L}'$ implies the existence of an Y-morphism $r' : X \to P' = \mathbb{P}(\mathscr{E}')$ such that $\mathscr{L}'$ is isomorphic to $r'^*(\mathscr{O}_{P'}(1))$ (Proposition 23.4.3). There is by hypothesis a quasi-coherent $\mathscr{O}_Y$-module $\mathscr{E}$ and a Y-immersion $r : X \to P = \mathbb{P}(\mathscr{E})$ such that $\mathscr{L}$ is isomorphic to $r^*(\mathscr{O}_P(1))$. Consider the Segre morphism $\zeta : P \times_Y P' \to Q$ where $Q = \mathbb{P}(\mathscr{E} \otimes \mathscr{E}')$. As r is an immersions, so is the morphism $(r, r')_Y : X \to P \times_Y P'$ by Corollary 22.5.16, and therefore we get an immersion

$$r'' : X \overset{(r,r')_Y}{\to} P \times_Y P' \overset{\zeta}{\to} Q.$$

Since $\zeta^*(\mathscr{O}_Q(1))$ is isomorphic to $\mathscr{O}_P(1) \otimes_Y \mathscr{O}_{P'}(1)$, we conclude from Corollary 22.3.14 that $r''^*(\mathscr{O}_Q(1))$ is isomorphic to $\mathscr{L} \otimes \mathscr{L}'$, this proves the assertion. □

Remark 23.4.4. Note that $q^*(\mathscr{O}_Y^{\oplus I}) = \mathscr{O}_X^{\oplus I}$ and there exists a surjection $\mathscr{O}_X^{\oplus I} \to \mathscr{L}'$ if and only if $\mathscr{L}'$ is generated by global sections, so Proposition 23.4.17 is applicable if $\mathscr{L}'$ is generated by global sections.

Corollary 23.4.18. *Let $q : X \to Y$ be a morphism.*

(a) *Let $\mathscr{L}$ be an invertible $\mathscr{O}_X$-module and $\mathscr{K}$ be an invertible $\mathscr{O}_Y$-module. For $\mathscr{L}$ to be very ample relative to q, it is necessary and sufficent that $\mathscr{L} \otimes q^*(\mathscr{K})$ is very ample relative to q.*

(b) *If $\mathscr{L}$ and $\mathscr{L}'$ are two invertible $\mathscr{O}_X$-modules that are very ample relative to q, then so is $\mathscr{L} \otimes \mathscr{L}'$. In particular, $\mathscr{L}^{\otimes n}$ is very ample relative to q for any $n > 0$.*

Proof. The assertions in (b) is an immediate concequence of Proposition 23.4.17, so is the half implication of (a). Now assume that $\mathscr{L} \otimes q^*(\mathscr{K})$ is very ample; then so is $(\mathscr{L} \otimes q^*(\mathscr{K})) \otimes q^*(\mathscr{K}^{-1})$ by Proposition 23.4.17, which is isomorphic to $\mathscr{L}$. □

Proposition 23.4.19. *Let $f : X \to Y$ be a quasi-compact morphism where Y is quasi-compact, and $\mathscr{L}$ be a very ample $\mathscr{O}_X$-module relative to f. Let $\mathscr{F}$ be a quasi-coherent $\mathscr{O}_X$-module of finite type and for each $n \in \mathbb{Z}$, set $\mathscr{F}(n) = \mathscr{F} \otimes \mathscr{L}^{\otimes n}$. Then there exists an integer n_0 such that for $n \geq n_0$, the canonical homomorphism $\sigma : f^*(f_*(\mathscr{F}(n))) \to \mathscr{F}(n)$ is surjective.*

Proof. □

Proposition 23.4.20. *Let $f : X \to Y$ be a quasi-compact morphism where Y is quasi-compact, and $\mathscr{L}$ be a very ample $\mathscr{O}_X$-module relative to f. Let $\mathscr{F}$ be a quasi-coherent $\mathscr{O}_X$-module of finite type. Then there exists an integer n_0 such that, for $n \geq n_0$, $\mathscr{F}$ is isomorphic to a quotient of an $\mathscr{O}_X$-module $f^*(\mathscr{G}) \otimes_{\mathscr{O}_X} \mathscr{L}^{\otimes(-n)}$, where $\mathscr{G}$ is a quasi-coherent $\mathscr{O}_Y$-module of finite type (dependent on n).*

Proof. Since $\mathscr{L}$ is very ample, f is separated and by Proposition 23.4.19 the canonical homomorphism $\sigma : f^*(f_*(\mathscr{F}(n))) \to \mathscr{F}(n)$ is surjective for n sufficiently large. The proposition is then a generalization of Corollary 23.3.26, and can be proved similarly. □

Proposition 23.4.21 (Properties of Very Ample Sheaves).

(i) *For any scheme Y, any invertible $\mathscr{O}_Y$-module $\mathscr{L}$ is very ample relative to the identify morphism 1_Y.*

(ii) *Let $f : X \to Y$ be a morphism and $j : X' \to X$ be an immersion. If $\mathscr{L}$ is a very ample $\mathscr{O}_X$-module relative to f, then $j^*(\mathscr{L})$ is very ample relative to $f \circ j$.*

(iii) *Let $f : X \to Y$ be a morphism of finite type and $g : Y \to Z$ be a quasi-compact morphism where Z is quasi-compact. Let $\mathscr{L}$ a very ample $\mathscr{O}_X$-module relative to f and $\mathscr{K}$ be a very ample $\mathscr{O}_Y$-module relative to g. Then there exists an integer $n_0 > 0$ such that for any $n \geq n_0$, $\mathscr{L} \otimes f^*(\mathscr{K}^{\otimes n})$ is very ample relative to $g \circ f$.*

(iv) *Let $f : X \to Y$, $g : Y' \to Y$ be two morphisms, and put $X' = X_{(Y')}$. If $\mathscr{L}$ is a very ample $\mathscr{O}_X$-module relative to f, $\mathscr{L}' = \mathscr{L} \otimes_Y \mathscr{O}_{Y'}$ is very ample relative to $f_{(Y')}$.*

(v) *Let $f_i : X_i \to Y_i$ $(i = 1, 2)$ be two S-morphisms. If $\mathscr{L}_i$ is a very ample $\mathscr{O}_{X_i}$-module relative to f_i, then $\mathscr{L}_1 \otimes_S \mathscr{L}_2$ is very ample relative to $f_1 \times_S f_2$.*

(vi) *Let $f : X \to Y$, $g : Y \to Z$ be two morphisms. If an $\mathscr{O}_X$-module $\mathscr{L}$ is very ample relative to $g \circ f$, then $\mathscr{L}$ is very ample relative to f.*

(vii) *Let $f : X \to Y$ be a morphism and $j : X_{\mathrm{red}} \to X$ be the canonical injection. If $\mathscr{L}$ is a very ample $\mathscr{O}_X$-module relative to f, then $j^*(\mathscr{L})$ is very ample relative to f_{red}.*

Proof. The property (ii) follows from the definition and it is immedaite that (vii) is deduced from (ii) and (vi). To prove (vi), consider the factorization

$$X \xrightarrow{\Gamma_f} X \times_Z Y \xrightarrow{p_2} Y$$

and note that $p_2 = (g \circ f) \times 1_Y$. It follows from the hypothesis and from (i) and (v) that $\mathscr{L} \otimes_{\mathscr{O}_Z} \mathscr{O}_Y$ is very ample relative to p_2. On the other hand, we have $\mathscr{L} = \Gamma_f^*(\mathscr{L} \otimes_{\mathscr{O}_Z} \mathscr{O}_Y)$ by Corollary 22.3.14, and Γ_f is an immersion (Corollary 22.5.8), so we can apply (ii). As for (i), we can apply the definition with $\mathscr{E} = \mathscr{L}$, and note that $\mathbb{P}(\mathscr{L})$ is identified with Y (Proposition 23.3.6).

We now prove (iv). Under the hypothesis of (iv), there exists a quasi-coherent $\mathscr{O}_Y$-module $\mathscr{E}$ and a Y-immersion $i : X \to P = \mathbb{P}(\mathscr{E})$ such that $\mathscr{L} = i^*(\mathscr{O}_P(1))$. Then, if $\mathscr{E}' = g^*(\mathscr{E})$, $\mathscr{E}'$ is a quasi-coherent $\mathscr{O}_Y$-module and we have $P' = \mathbb{P}(\mathscr{E}') = P_{(Y')}$, $i_{(Y')}$ is an immersion from $X_{(Y')}$ to P', and $\mathscr{L}'$ is isomorphic to $(i_{(Y')})^*(\mathscr{O}_{P'}(1))$ (Remark 23.4.2).

To prove (v), remark that there exists by hypothesis a Y_i-immersion $r_i : X_i \to P_i = \mathbb{P}(\mathscr{E}_i)$, where $\mathscr{E}_i$ is a quasi-coherent $\mathscr{O}_{Y_i}$-module, and $\mathscr{L}_i = r_i^*(\mathscr{O}_{P_i}(1))$. Then $r_1 \times_S r_2$ is an S-immersion of $X_1 \times_S X_2$ to $P_1 \times_S P_2$ (Proposition 22.4.11) and the inverse image of $\mathscr{O}_{P_1}(1) \otimes_S \mathscr{O}_{P_2}(1)$ by this immersion is $\mathscr{L}_1 \otimes_S \mathscr{L}_2$. On the other hand, put $T = Y_1 \times_S Y_2$, and let p_1, p_2 be the projection of T, respectively. If $P'_i = \mathbb{P}(p_i^*(\mathscr{E}_i))$, we have $P'_i = P_i \times_{Y_i} T$, whence

$$P'_1 \times_T P'_2 = (P_1 \times_{Y_1} T) \times_T (P_2 \times_{Y_2} T) = P_1 \times_{Y_1} (T \times_{Y_2} P_2) = P_1 \times_{Y_1} (Y_1 \times_S P_2) = P_1 \times_S P_2.$$

Similarly, we have $\mathscr{O}_{P'_i}(1) = \mathscr{O}_{P'_i}(1) \otimes_{Y_i} \mathscr{O}_T$, and $\mathscr{O}_{P'_1}(1) \otimes_T \mathscr{O}_{P'_2}(1)$ is identified with $\mathscr{O}_{P_1}(1) \otimes_S \mathscr{O}_{P_2}(1)$. We can then consider $r_1 \times_S r_2$ as an T-immersion from $X_1 \times_S X_2$ to $P'_1 \times_T P'_2$, the inverse image of $\mathscr{O}_{P'_1}(1) \otimes_T \mathscr{O}_{P'_2}(1)$ by this immersion being $\mathscr{L}_1 \otimes_S \mathscr{L}_2$. We can then conclude as in Proposition 23.4.17 that $\mathscr{L}_1 \otimes_S \mathscr{L}_2$ is very ample.

It remains to prove (iii). We can first restrict to the case where Z is an affine scheme, since there exists a finite covering (U_i) of Z by affine opens; if the property is proved for $\mathscr{K}|_{g^{-1}(U_i)}$, $\mathscr{L}|_{f^{-1}(g^{-1}(U_i))}$ and an integer n_i, it suffices to choose n_0 to be the largest n_i to prove the property for $\mathscr{K}$ and $\mathscr{L}$ (Corollary 23.4.14). The hypotheses imply that f, g are spearated morphisms, so X and Y are quasi-compact schemes. Since $\mathscr{L}$ is very ample relative to f, there exists an immersion $r : X \to P = \mathbb{P}(\mathscr{E})$, where $\mathscr{E}$ is a quasi-coherent $\mathscr{O}_Y$-module of finite type and $\mathscr{L} = r^*(\mathscr{O}_P(1))$, in view of Proposition 23.4.15. We claim that there exists an integer m_0 such that for any $m \geq m_0$, there is a very ample $\mathscr{O}_P$-module $\mathscr{M}$ relative to the composition morphism $j : P \to Y \xrightarrow{g} Z$ such that $\mathscr{O}_P(1)$ is isomorphic to $\mathscr{M} \otimes_Y \mathscr{K}^{\otimes(-m)}$. For $n \geq m+1$, $\mathscr{O}_P(1) \otimes_Y \mathscr{K}^{\otimes n}$ will then be very ample relative to Z in view of the hypothesis and applying (v) to the morphism $j : P \to Z$ and 1_Z; as r is an immersion and $\mathscr{L} \otimes f^*(\mathscr{K}^{\otimes n}) = r^*(\mathscr{O}_P(1) \otimes_Y \mathscr{K}^{\otimes n})$, the conclusion then follows from (ii).

To estabilsh the claim, we can use Proposition 23.4.20 to obtain a closed immersion j_1 of P to $P_1 = \mathbb{P}(g^*(\mathscr{F}) \otimes \mathscr{K}^{\otimes(-m)})$ such that $\mathscr{O}_P(1)$ is isomorphic to $j_1^*(\mathscr{O}_{P_1}(1))$ (Proposition 23.3.30). On the other hand, there is an isomorphism from P_1 to $P_2 = \mathbb{P}(g^*(\mathscr{F}))$, identifying $\mathscr{O}_{P_1}(1)$ with $\mathscr{O}_{P_2}(1) \otimes_Y \mathscr{K}^{\otimes(-m)}$ (Proposition 23.4.1); we then have a closed immersion $j_2 : P \to P_2$ such that $\mathscr{O}_P(1)$ is isomorphic to $j_2^*(\mathscr{O}_{P_2}(1)) \otimes_Y \mathscr{K}^{\otimes(-m)}$. Finally, P_2 is identified with $P_3 \times_Z Y$ where $P_3 = \mathbb{P}(\mathscr{F})$, and $\mathscr{O}_{P_2}(1)$ is identified with $\mathscr{O}_{P_3}(1) \otimes_Z \mathscr{O}_Y$ (4.1.2). By definition, $\mathscr{O}_{P_3}(1)$ is very ample for Z, and so is $\mathscr{K}$, so it follows from (v) that the $\mathscr{O}_{P_2}$-module $\mathscr{O}_{P_3}(1) \otimes_Y \mathscr{K}$ is very ample for Z. In view of (ii), $\mathscr{M} = j_2^*(\mathscr{O}_{P_3}(1) \otimes_Y \mathscr{K})$ is then very ample for Z, and $\mathscr{O}_P(1)$ is isomorphic to

$\mathscr{M} \otimes_Y \mathscr{K}^{\otimes(-m-1)}$, whence the demonstration. □

Proposition 23.4.22. *Let $f : X \to Y$, $f' : X' \to Y$ be two morphisms, $X'' = X \amalg X'$, and $f'' = f \amalg f'$. Let $\mathscr{L}$ (resp. $\mathscr{L}'$) be an invertible $\mathscr{O}_X$-module (resp. $\mathscr{O}_{X'}$-module), and let $\mathscr{L}''$ be the invertible $\mathscr{O}_{X''}$-module which coincides with $\mathscr{L}$ over X and with $\mathscr{L}'$ over X'. For $\mathscr{L}''$ to be very ample relative to f'', it is necessary and sufficent that $\mathscr{L}$ is very ample relative to f and $\mathscr{L}'$ is very ample relative to f'.*

Proof. We can assume that Y is affine. If $\mathscr{L}''$ is very ample then so is $\mathscr{L}$ and $\mathscr{L}'$ in view of Proposition 23.4.21(ii). Conversely, if $\mathscr{L}$ and $\mathscr{L}'$ are very ample, it follows from Remark 23.4.3 that $\mathscr{L}''$ is very ample. □

23.4.5 Ample sheaves

Let X be a scheme, $\mathscr{L}$ be an invertible $\mathscr{O}_X$-module, and $\mathscr{F}$ be an $\mathscr{O}_X$-module. For any $n \in \mathbb{Z}$, we set $\mathscr{F}(n) = \mathscr{F} \otimes_{\mathscr{O}_X} \mathscr{L}^{\otimes n}$ (if there is no confusion), and $S = \bigoplus_{n\geq 0} \Gamma(X, \mathscr{L}^{\otimes n})$. If we consider X as a $\mathbb{Z}$-scheme and let $p : X \to Y = \operatorname{Spec}(\mathbb{Z})$ be the structural morphism, there are bijections

$$\operatorname{Hom}_{\mathsf{Qcoh}(X)}(p^*(\widetilde{S}), \boldsymbol{S}(\mathscr{L})) \xrightarrow{\sim} \operatorname{Hom}_{\mathsf{Qcoh}(Y)}(\widetilde{S}, p_*(\boldsymbol{S}(\mathscr{L}))) \xrightarrow{\sim} \operatorname{Hom}_{\mathbb{Z}}(S, \Gamma(X, \boldsymbol{S}(\mathscr{L})))$$

where we use Proposition 22.2.5. The homomorphism $\varepsilon : p^*(\widetilde{S}) \to \boldsymbol{S}(\mathscr{L})$ corresponding to the canonical injection of S into $\Gamma(X, \boldsymbol{S}(\mathscr{L}))$ is called the **canonical homomorphism associated with** $\mathscr{L}$. It then corresponds to a canonical morphism

$$r_{\mathscr{L},\varepsilon} : G(\varepsilon) \to \operatorname{Proj}(S). \tag{4.5.1}$$

Theorem 23.4.23. *Let X be a quasi-compact and quasi-separated scheme, $\mathscr{L}$ be an invertible $\mathscr{O}_X$-module and $S = \bigoplus_{n\geq 0} \Gamma(X, \mathscr{L}^{\otimes n})$. The following conditions are equivalent:*

(i) The subsets X_f, as f runs through the set of homogeneous elements of S_+, form a basis for X.

(i′) The subsets X_f which are affine, as f runs through the set of homogeneous elements of S_+, form a basis for X.

(ii) The canonical morphism $r_{\mathscr{L},\varepsilon} : G(\varepsilon) \to \operatorname{Proj}(S)$ is everywhere defined and a dominant open immersin.

(ii′) The canonical morphism $r_{\mathscr{L},\varepsilon} : G(\varepsilon) \to \operatorname{Proj}(S)$ is everywhere defined and a homeomorphism from X onto a subspace of $\operatorname{Proj}(S)$.

(iii) For any quasi-coherent $\mathscr{O}_X$-module $\mathscr{F}$, if $\mathscr{F}_n$ is the sub-$\mathscr{O}_X$-module of $\mathscr{F}(n)$ generated by the sections of $\mathscr{F}(n)$ over X, then $\mathscr{F}$ is the direct sum of the sub-$\mathscr{O}_X$-modules $\mathscr{F}_n(-n)$ for $n > 0$.

(iii′) Property (iii) holds for any quasi-coherent ideal of $\mathscr{O}_X$.

Moreover, in this case, if (f_α) is a family of homogeneous elements of S_+ such that X_{f_α} is affine, then the restriction to $\bigcup_\alpha X_{f_\alpha}$ of the canonical morphism $r_{\mathscr{L},\varepsilon} : X \to \operatorname{Proj}(S)$ is an isomorphism from $\bigcup_\alpha X_{f_\alpha}$ to $\bigcup_\alpha (\operatorname{Proj}(S))_{f_\alpha}$.

Proof. It is clear that (ii) implies (ii′), and (ii′) implies (i) in view of the formula (3.6.2). Condition (i) implies (i′), because any $x \in X$ admits an affine neighborhood U such that $\mathscr{L}|_U$ is

isomorphic to $\mathscr{O}_X|_U$; if $f \in \Gamma(X, \mathscr{L}^{\otimes n})$ is such that $x \in X_f \subseteq U$, X_f is also the set of $x' \in U$ such that $(f|_U)(x') \neq 0$, and this is an affine open subset of U (hence of X). To prove that (i′) implies (ii), it suffices to show the last assertion of the statement, hence to check that if $X = \bigcup_\alpha X_{f_\alpha}$, the condition (iv) of Proposition 23.3.39 is satisfied; this follows immediately from Theorem 22.6.14(a). To see that $r_{\mathscr{L},\varepsilon}$ is dominant, we note that for $f \in S_+$ homogeneous, X_f is the inverse image of $D_+(f)$ by $r_{\mathscr{L},\varepsilon}$ and by Corollary 22.6.15 we have $\Gamma(X_f, \mathscr{O}_X) = S_{(f)}$ is nonzero if f is not nilpotent, so X_f is nonempty if $D_+(f)$ is not empty.

To prove that (i′) implies (iii), note that if X_f is affine (where $f \in S_d$), $\mathscr{F}|_{X_f}$ is generated by its sections over X_f (Theorem 22.1.20); on the other hand, by Theorem 22.6.14 such a section s is of the form $(t|_{X_f}) \otimes (f|_{X_f})^{-m}$ where $t \in \Gamma(X, \mathscr{F}(md))$. By definition, t is also a section of $\mathscr{F}_{md}$, so s is a section of $\mathscr{F}_{md}(-md)$ over X_f, which proves (iii). It is clear that (iii) implies (iii′), and it rests to show that (iii′) implies (i). Now let U be an open neighborhood of $x \in X$, and let $\mathscr{I}$ be a quasi-coherent ideal of $\mathscr{O}_X$ defining a closed subscheme of X with underlying subspace $X - U$. The hypothesis of (iii′) implies that there exists an integer $n > 0$ and a section $\mathscr{I}(n)$ over X such that $f(x) \neq 0$. Then we have evidently $f \in S_n$ and $x \in X_f \subseteq U$, this proves (i). □

If X is a quasi-compact and quasi-separated scheme, the equivalent conditions of Theorem 23.4.23 implies that X is separated, since it is isomorphic to a subscheme of $\mathrm{Proj}(S)$. We say an invertible $\mathscr{O}_X$-module $\mathscr{L}$ is **ample** if X is a qausi-compact and quasi-separated scheme and the equivalent conditions of Theorem 23.4.23 are satisfied. It follows from Theorem 23.4.23(i) that if $\mathscr{L}$ is an ample $\mathscr{O}_X$-module, then for any open subset U of X, $\mathscr{L}|_U$ is an ample $(\mathscr{O}_X|_U)$-module.

Corollary 23.4.24. *Let $\mathscr{L}$ be an ample $\mathscr{O}_X$-module. For any finite subspace Z of X and any open neighborhood U of Z, there exists an integer $n > 0$ and a section $f \in \Gamma(X, \mathscr{L}^{\otimes n})$ such that X_f is an affine neighborhood of Z contained in U.*

Proof. In view of Theorem 23.4.23(ii), we can view X as a subscheme of $\mathrm{Proj}(S)$ and we only need to prove that for any finite subset Z' of $\mathrm{Proj}(S)$ and any open neighborhood U of Z', there exists a homogeneous element $f \in S_+$ such that $Z \subseteq D_+(f) \subseteq U$. Now by definition the closed set Y, which is the complement of U in $\mathrm{Proj}(S)$, is of the form $V_+(\mathfrak{I})$ where $\mathfrak{I}$ is a graded ideal of S, not containing S_+; on the other hand, the points of Z' are by definition graded prime ideals $\mathfrak{p}_i$ of S_+ not containing $\mathfrak{I}$. There then exists an element $f \in \mathfrak{I}$ not contained in each $\mathfrak{p}_i$ (Proposition 10.4.15), and as the $\mathfrak{p}_i$ are graded, we can assume that f is homogeneous. This element f then satisfies the required. □

Proposition 23.4.25. *Suppose that X is a quasi-compact and quasi-separated scheme. Then the conditions of Theorem 23.4.23 are equivalent to the following conditions:*

(iv) For any quasi-coherent $\mathscr{O}_X$-module $\mathscr{F}$ of finite type, there exists an integer $n_0 > 0$ such that, for any $n \geq n_0$, $\mathscr{F}(n)$ is generated by its sections over X.

(iv′) For any quasi-coherent $\mathscr{O}_X$-module $\mathscr{F}$ of finite type, there exists integers $n > 0, k > 0$ such that $\mathscr{F}$ is isomorphic to a quotient of the $\mathscr{O}_X$-module $\mathscr{L}^{\otimes(-n)} \otimes \mathscr{O}_X^k$.

(iv″) Property (iv′) holds for any quasi-coherent ideal of $\mathscr{O}_X$ of finite type.

Proof. As X is quasi-compact, if a quasi-coherent $\mathscr{O}_X$-module $\mathscr{F}$ of finite type is such that $\mathscr{F}(n)$ is generated by global sections, $\mathscr{F}(n)$ is then generated by finitely many global sections (Corollary 19.4.11), so (iv) impliess (iv′) and it is clear that (iv′) implies (iv″). As any quasi-coherent $\mathscr{O}_X$-module $\mathscr{G}$ is the inductive limit of its sub-$\mathscr{O}_X$-modules of finte type (Corollary 22.6.62), to verify conditin (iii′) of Theorem 23.4.23, it suffices to verify that for a quasi-coherent ideal of $\mathscr{O}_X$ that is of finite type, and this is clear if condition (iv″) holds. It remains to prove that if $\mathscr{L}$ is an ample $\mathscr{O}_X$-module, then condition (iv) holds. Consider a finite affine open covering (X_{f_i}) of X with $f_i \in S_{n_i}$; by changing f_i by its power, we can assume that the integers n_i equal to the same integer m. The sheaf $\mathscr{F}|_{X_{f_i}}$, being of finite type by hypotheses, is generated by a finitely number of sections h_{ij} over X_{f_i} (Corollary 22.1.23). By Theorem 22.6.14, there then exists an integer k_0 such that the section $h_{ij} \otimes f_i^{k_0}$ extend to a section of $\mathscr{F}(k_0 m)$ over X for any couple (i, j). A fortiori the $h_{ij} \otimes f_i^k$ extend to sections of $\mathscr{F}(km)$ over X for $k \geq k_0$, and for such values of k, $\mathscr{F}(km)$ is then generated by global sections. For any integer p such that $0 < p < m$, $\mathscr{F}(p)$ is also of finite type, so there exist an integer k_p such that $\mathscr{F}(p)(km) = \mathscr{F}(p + km)$ is generated by global sections for $k \geq k_p$. Let n_0 be the largest of the $k_p m$ for $0 < p < m$; we then conclude that $\mathscr{F}(n)$ is generated by global sections for $n \geq n_0$. □

Proposition 23.4.26. *Let X be a quasi-compact and quasi-separated scheme and $\mathscr{L}$ be an invertible $\mathscr{O}_X$-module.*

(a) Let $n > 0$ be an integer. For $\mathscr{L}$ to be ample, it is necessary and sufficent that $\mathscr{L}^{\otimes n}$ is ample.

(b) Let $\mathscr{L}'$ be an inveritble $\mathscr{O}_X$-module such that, for any $x \in X$, there exists a section s' of $\mathscr{L}'^{\otimes n}$ over X such that $s'(x) \neq 0$. Then, if $\mathscr{L}$ is ample, so is $\mathscr{L} \otimes \mathscr{L}'$.

Proof. Property (a) is a concequence of (i) of Theorem 23.4.23 since $X_{f^{\otimes n}} = X_f$. On the other hand, if $\mathscr{L}$ is ample, for any $x \in X$ and any neighborhood U of x, there exists $m > 0$ and $f \in \Gamma(X, f^{\otimes m})$ such that $x \in X_f \subseteq U$; if $f' \in \Gamma(X, \mathscr{L}'^{\otimes n})$ is such that $f'(x) \neq 0$, then $s(x) \neq 0$ for $s = f^{\otimes n} \otimes f'^{\otimes m} \in \Gamma(X, (\mathscr{L} \otimes \mathscr{L}')^{\otimes mn})$, so $x \in X_s \subseteq X_f \subseteq U$, and therefore $\mathscr{L} \otimes \mathscr{L}'$ is ample. □

Corollary 23.4.27. *The tensor product of two ample $\mathscr{O}_X$-modules is ample.*

Proof. An ample $\mathscr{O}_X$-module satisfies the condition of Proposition 23.4.26(b). □

Corollary 23.4.28. *Let $\mathscr{L}$ be an ample $\mathscr{O}_X$-module and $\mathscr{L}'$ be an invertible $\mathscr{O}_X$-module. There then exists an integer $n_0 > 0$ such that $\mathscr{L}^{\otimes n} \otimes \mathscr{L}'$ is ample and generated by global sections for $n \geq n_0$.*

Proof. It follows from Proposition 23.4.25 that there exists an integer m_0 such that for $m \geq m_0$, $\mathscr{L}^{\otimes m} \otimes \mathscr{L}'$ is generated by global sections, and therefore satisfies the condition of Proposition 23.4.26(b); we can then choose $n_0 = m_0 + 1$. □

Remark 23.4.5. Let $P = \mathrm{Pic}(X) = H^1(X, \mathscr{O}_X^\times)$ be the picard group of $\mathscr{O}_X$-modules, and let P^+ be the subset of P formed by ample sheaves. Suppose that P^+ is nonempty. Then it follows from Corollary 23.4.27 and Corollary 23.4.28 that we have

$$P^+ + P^+ \subseteq P^+, \quad P^+ - P^+ = P.$$

which means $P^+ \cup \{0\}$ is the set of positive elements of P for an order structure over P compatible with the group structure, which is archimedean in view of Corollary 23.4.28.

Proposition 23.4.29. *Let $q : X \to Y$ be a quasi-compact and quasi-separated morphism where Y is affine, and $\mathscr{L}$ be an inveritble $\mathscr{O}_X$-module.*

(a) If $\mathscr{L}$ is very ample relative to q then $\mathscr{L}$ is ample.

(b) Suppose that q is of finite type. Then for $\mathscr{L}$ to be ample, it is necessary and sufficent that it satisfies the following equivalent conditions:

(v) There exists $n_0 > 0$ such that for any integer $n \geq n_0$, $\mathscr{L}^{\otimes n}$ is very ample relative to q.

(v′) There exists $n > 0$ such that $\mathscr{L}^{\otimes n}$ is very ample relative to q.

Proof. The first assertion follows from the definition of very ample: if A is the ring of Y, there exists an A-module E and a surjective homomorphism

$$\psi : q^*(\widetilde{\boldsymbol{S}(E)}) \to \boldsymbol{S}(\mathscr{L})$$

such that $i = r_{\mathscr{L},\psi}$ is an immersion from X to $P = \mathbb{P}(\widetilde{E})$ such that $\mathscr{L} \cong i^*(\mathscr{O}_P(1))$. As the $D_+(f)$ for $f \in \boldsymbol{S}(E)_+$ homogeneous form a basis for P and $i^{-1}(D_+(f)) = X_{\psi^\flat(f)}$, we see that condition (i) of Theorem 23.4.23 holds, so $\mathscr{L}$ is ample.

Now assume that q is of finite type and $\mathscr{L}$ is ample. It follows from Theorem 23.4.23(ii) and Proposition 23.4.11(a) that there exists an integer $k_0 > 0$ such that $\mathscr{L}^{\otimes k_0}$ is very ample relative to q. On the other hand, in view of Proposition 23.4.25, there exists an integer m_0 such that, for $m \geq m_0$, $\mathscr{L}^{\otimes m}$ is generated by global sections. Put $n_0 = k_0 + m_0$; if $n \geq n_0$, we can write $n = k_0 + m$ where $m \geq m_0$, whence $\mathscr{L}^{\otimes n} = \mathscr{L}^{\otimes k_0} \otimes \mathscr{L}^{\otimes m}$. As $\mathscr{L}^{\otimes m}$ is generated by global sections, it follow from Proposition 23.4.17 and Remark 23.3.3 that $\mathscr{L}^{\otimes n}$ is very ample relative to q. Finally, it is clear that (v) implies (v′), and (v′) implies that $\mathscr{L}$ is ample in view of (a) and Proposition 23.4.26. □

Corollary 23.4.30. *Let $q : X \to Y$ be a quasi-compact and quasi-separated morphism of finite type where Y is affine, $\mathscr{L}$ be an ample $\mathscr{O}_X$-module, and $\mathscr{L}'$ be an invertible $\mathscr{O}_X$-module. Then there exists an integer $n_0 > 0$ such that for $n \geq n_0$, $\mathscr{L}^{\otimes n} \otimes \mathscr{L}'$ is very ample relative to q.*

Proof. In fact, there exists integer m_0 such that for $m \geq m_0$, $\mathscr{L}^{\otimes m} \otimes \mathscr{L}'$ is generated by global section (Corollary 23.4.28); on the other hand, there exists k_0 such that $\mathscr{L}^{\otimes k}$ is very ample relative to q for $k \geq k_0$. Thus $\mathscr{L}^{\otimes(k+m_0)} \otimes \mathscr{L}'$ is very ample for $k \geq k_0$ (Corollary 23.4.16). □

Proposition 23.4.31. *Let X be a quasi-compact scheme, Z be a closed subscheme of X defined by a qausi-coherent nilpotent ideal $\mathscr{I}$ of $\mathscr{O}_X$, and $j : Z \to X$ be the canonical injectin. For an inveritble $\mathscr{O}_X$-module $\mathscr{L}$ to be ample, it is necessary and sufficient that $\mathscr{L}' = j^*(\mathscr{L})$ is an ample $\mathscr{O}_Z$-module.*

Proof. This conditions is necessary. In fact, for any section f of $\mathscr{L}^{\otimes n}$ over X, let f' be the image $f \otimes 1$, which is a section of $\mathscr{L}'^{\otimes n} = \mathscr{L}^{\otimes n} \otimes_{\mathscr{O}_X} (\mathscr{O}_X/\mathscr{I})$ over the subspace Z (identified with X); it is clear that $Z_{f'} = X_f$, hence condition (i) of Theorem 23.4.23 shows that $\mathscr{L}'$ is ample.

To prove the sufficiency, note first that we can reduce to the case $\mathscr{I}^2 = 0$ by considering the finite sequence of schemes $X_k = (X, \mathscr{O}_X/\mathscr{I}^{k+1})$, which is a closed subscheme of the previous one and is defined by a square zero ideal. Now X is quasi-separated if X_{red} is quasi-separated (Proposition 22.6.7(vi)). Criterion (i) of Theorem 23.4.23 shows that it will suffice to prove that,

if g is a section of $\mathscr{L}'^{\otimes n}$ over Z such that Z_g is affine, then there exists $m > 0$ such that $g^{\otimes m}$ is the canonical image of a section f of $\mathscr{L}^{\otimes nm}$ over X. For this, we consider the exact sequence

$$0 \longrightarrow \mathscr{I}(n) \longrightarrow \mathscr{O}_X(n) = \mathscr{L}^{\otimes n} \longrightarrow \mathscr{O}_Z(n) = \mathscr{L}'^{\otimes n} \longrightarrow 0$$

since $\mathscr{F}(n)$ is an exact functor on $\mathscr{F}$; whence an exact sequence on cohomology:

$$0 \longrightarrow \Gamma(X, \mathscr{I}(n)) \longrightarrow \Gamma(X, \mathscr{L}^{\otimes n}) \longrightarrow \Gamma(X, \mathscr{L}'^{\otimes n}) \xrightarrow{\delta} H^1(X, \mathscr{I}(n))$$

which associates in particular g to an element $\delta g \in H^1(X, \mathscr{I}(n))$.

Note that since $\mathscr{I}^2 = 0$, $\mathscr{I}$ can be considered as a quasi-coherent $\mathscr{O}_Z$-module and we have, for any k, $\mathscr{L}'^{\otimes k} \otimes_{\mathscr{O}_Z} \mathscr{I}(n) = \mathscr{I}(n+k)$. For any section $s \in \Gamma(X, \mathscr{L}'^{\otimes k})$, tensoring by s is then a homomorphism $\mathscr{I}(n) \to \mathscr{I}(n+k)$ of $\mathscr{O}_Z$-modules, which gives a homomorphism $H^i(X, \mathscr{I}(n)) \to H^i(X, \mathscr{I}(n+k))$ of cohomology groups. We claim that

$$g^{\otimes m} \otimes \delta g = 0 \tag{4.5.2}$$

for $m > 0$ sufficiently large. In fact, Z_g is an affine open of Z and we have $H^1(Z_g, \mathscr{I}(n)) = 0$ where $\mathscr{I}(n)$ is considered as an $\mathscr{O}_Z$-module. In particular, if we put $g' = g|_{Z_g}$, and if we consider its image under $\delta : \Gamma(Z_g, \mathscr{L}'^{\otimes n}) \to H^1(Z_g, \mathscr{I}(n))$, we have $\delta g' = 0$. To explain this relation, observe that the first cohomology group of a sheaf coincides with the Cech cohomology; to form δg, it is necessary to consider an open covering (U_α) of X, which we can assume that is finite and formed by affine opens, and choose for each α a section $g_\alpha \in \Gamma(U_\alpha, \mathscr{L}^{\otimes n})$ whose image in $\Gamma(U_\alpha, \mathscr{L}'^{\otimes n})$ is $g|_{U_\alpha}$, and consider the class of cocycle $(g_{\alpha\beta} - g_{\beta\alpha})$, where $g_{\alpha\beta}$ is the restriction of g_α to $U_\alpha \cap U_\beta$ (a cocycle with values in $\mathscr{I}(n)$). We can moreover suppose that $\delta g'$ is in the same manner using the covering formed by $U_\alpha \cap Z_g$ and the restrictions $g_\alpha|_{U_\alpha \cap Z_g}$; the relation $\delta g' = 0$ signifies then that there exists for each α a section $h_\alpha \in \Gamma(U_\alpha \cap Z_g, \mathscr{I}(n))$ such that $(g_{\alpha\beta} - g_{\beta\alpha})|_{U_\cap \cap U_\beta \cap Z_g} = h_{\alpha\beta} - h_{\eta\alpha}$, where $h_{\alpha\beta}$ denotes the restriction of h_α to $U_\alpha \cap U_\beta \cap Z_g$. Now by Theorem 22.6.14 there exists an integer $m > 0$ such that $g^{\otimes m} \otimes h_\alpha$ is the restriction to $U_\alpha \cap Z_g$ of a section $t_\alpha \in \Gamma(U_\alpha, \mathscr{I}(n+nm))$ for each α; we then have $g^{\otimes m} \otimes (g_{\alpha\beta} - g_{\beta\alpha}) = t_{\alpha\beta} - t_{\beta\alpha}$ for any couple of indices, which proves $g^{\otimes m} \otimes \delta g = 0$.

We remark on the other hand that if $s \in \Gamma(X, \mathscr{O}_Z(p))$, $t \in \Gamma(X, \mathscr{O}_Z(q))$, we have, in the group $H^1(X, \mathscr{I}(p+q))$, that

$$\delta(s \otimes t) = (\delta s) \otimes t + s \otimes (\delta t). \tag{4.5.3}$$

For this, we can still consider an open cover (U_α) of X, and for each α a section $s_\alpha \in \Gamma(U_\alpha, \mathscr{O}_X(p))$ (resp. a section $t_\alpha \in \Gamma(U_\alpha, \mathscr{O}_X(q))$) whose canonical image in $\Gamma(U_\alpha, \mathscr{O}_Z(p))$ (resp. in $\Gamma(U_\alpha, \mathscr{O}_Z(q))$) is $s|_{U_\alpha}$; the relation (4.5.3) then follows from

$$(s_{\alpha\beta} \otimes t_{\alpha\beta}) - (s_{\beta\alpha} \otimes t_{\beta\alpha}) = (s_{\alpha\beta} - s_{\beta\alpha}) \otimes t_{\alpha\beta} + s_{\beta\alpha} \otimes (t_{\alpha\beta} - t_{\beta\alpha})$$

with the same notations before. By recurrence on k, we then have

$$\delta(g^{\otimes k}) = (k g^{\otimes (k-1)}) \otimes (\delta g) \tag{4.5.4}$$

and in view of (4.5.2) and (4.5.4), we have $\delta(g^{\otimes (m+1)}) = 0$, so $g^{\otimes (m+1)}$ is the canonical image of a

section f of $\mathscr{L}^{\otimes n(m+1)}$ over X, whence our demonstration. □

Corollary 23.4.32. *Let X be a Noetherian scheme and $j : X_{\mathrm{red}} \to X$ be the canonical injection. For an inveritble $\mathscr{O}_X$-module $\mathscr{L}$ to be ample, it is necessary and sufficient that $j^*(\mathscr{L})$ is an ample $\mathscr{O}_{X_{\mathrm{red}}}$-module.*

Proof. The nilradical $\mathscr{N}_X$ is nilpotent and we can apply Proposition 23.4.31. □

23.4.6 Relatively ample sheaves

Let $f : X \to Y$ be a quasi-compact morphism and $\mathscr{L}$ be an invertible $\mathscr{O}_X$-module. We say that $\mathscr{L}$ is **ample relative to f**, or relative to Y, or **f-ample**, or **Y-ample**, if there exists an affine open covering (U_α) of Y such that if $X_\alpha = f^{-1}(U_\alpha)$, $\mathscr{L}|_{X_\alpha}$ is an ample $\mathscr{O}_{X_\alpha}$-module for each α. Again, the existence of an f-ample $\mathscr{O}_X$-module implies that X is separated, so f is necessarily separated by Proposition 22.5.25.

Proposition 23.4.33. *Let $f : X \to Y$ be a quasi-compact morphism and $\mathscr{L}$ be an invertible $\mathscr{O}_X$-module. If $\mathscr{L}$ is very ample relative to f, then it is ample relative to f.*

Proof. If $\mathscr{L}$ is very ample relative to f then the morphism f is separated, so by Proposition 23.4.29(a) the restriction $\mathscr{L}|_{f^{-1}(U)}$ for any affine open U of Y is very ample, hence ample. □

Let $f : X \to Y$ be a quasi-compact morphism and $\mathscr{L}$ be an invertible $\mathscr{O}_X$-module. We consider the graded $\mathscr{O}_Y$-algebra $\mathscr{S} = \bigoplus_{n\geq 0} f_*(\mathscr{L}^{\otimes n})$. Then the canonical homomorphisms $\sigma_n : f^*(f_*(\mathscr{L}^{\otimes n})) \to \mathscr{L}^{\otimes n}$ induce a canonical homomorphism

$$\sigma : f^*(\mathscr{S}) \to \bigoplus_{n\geq 0} \mathscr{L}^{\otimes n} = \boldsymbol{S}(\mathscr{L}).$$

On the other hand, it is easy to see that $\sigma^\flat$ is the canonical injection from $\mathscr{S}$ into $f_*(\boldsymbol{S}(\mathscr{L}))$. The homomorphism σ gives an Y-morphism

$$r_{\mathscr{L},\sigma} : G(\sigma) \to \mathrm{Proj}(\mathscr{S}) = P.$$

Proposition 23.4.34. *Let $f : X \to Y$ be a quasi-compact morphism and $\mathscr{L}$ be an invertible $\mathscr{O}_X$-module. Then the following conditions are equivalent:*

(i) $\mathscr{L}$ is f-ample.

(ii) $\mathscr{S}$ is quasi-coherent and the Y-morphism $r_{\mathscr{L},\sigma}$ is everywhere defined and a dominant open immersion.

(ii′) The morphism f is separated, the Y-morphism $r_{\mathscr{L},\sigma}$ is everywhere defined and is a homeomorphism from X onto a subspace of $\mathrm{Proj}(\mathscr{S})$.

Moreover, if these are satisfied, for any $n \in \mathbb{Z}$ the canonical homomorphism of (3.6.3)

$$\nu : r^*_{\mathscr{L},\sigma}(\mathscr{O}_P(n)) \to \mathscr{L}^{\otimes n} \tag{4.6.1}$$

is an isomorphism. Finally, for any quasi-coherent $\mathscr{O}_X$-module $\mathscr{F}$, if we put $\mathscr{M} = \bigoplus_{n\geq 0} f_*(\mathscr{F}\otimes\mathscr{L}^{\otimes n})$, the canonical homomorphism of (3.6.4)

$$\xi : r^*_{\mathscr{L},\sigma}(\widetilde{\mathscr{M}}) \to \mathscr{F} \tag{4.6.2}$$

is an isomorphism.

Proof. We have remarked that (i) implies that f is separated, so $\mathscr{S}$ is quasi-coherent by Proposition 22.6.54. As the fact that $r_{\mathscr{L},\sigma}$ is an open immersion everywhere defined is local over Y, to shows that (i) implies (ii), we can assume that Y is affine and $\mathscr{L}$ is ample; the assertion then follows from Theorem 23.4.23. It is clear that (ii) implies (ii′); finally, to show that (ii′) implies (i), it suffices to consider an affine open cover (U_α) of Y and use Theorem 23.4.23(ii′) to $\mathscr{L}|_{X_\alpha}$.

To prove the last two assertions, we use the fact that $\sigma^\flat$ is the canonical injection of $\mathscr{S}$ to $f_*(\boldsymbol{S}(\mathscr{L}))$ and the expression of the morphisms ν and ξ in Remark 23.3.5 and Remark 23.3.6. It then follows that ν and ξ are injective. As for the surjectivity, we can assume that Y is affine, so $\mathscr{L}$ is ample; the criterion of Theorem 23.4.23(iii) then shows that ν and ξ are surjective, whence the assertion. □

Remark 23.4.6. From Proposition 23.4.34 and its proof, we conclude that if $\mathscr{L}$ is f-ample then $f_*(\boldsymbol{S}(\mathscr{L}))$ is equal to $\mathscr{S}$, so the homomorphism $\sigma^\flat$ is the identity on $\mathscr{S}$. This can also be seen from Proposition 22.6.55 since in this case f is separated.

Corollary 23.4.35. *Let (U_α) be an open covering of Y. For $\mathscr{L}$ to be Y-ample, it is necessary and sufficient that $\mathscr{L}|_{f^{-1}(U_\alpha)}$ is U_α-ample for each α.*

Proof. This is ture since the condition (ii) of Proposition 23.4.34 is local over Y. □

Corollary 23.4.36. *Let $\mathscr{K}$ be an invertible $\mathscr{O}_Y$-module. For $\mathscr{L}$ to be Y-ample, it is necessary and sufficient that $\mathscr{L}\otimes f^*(\mathscr{K})$ is Y-ample.*

Proof. This is a concequence of Corollary 23.4.35 by taking U_α to be such that $\mathscr{K}|_{U_\alpha}$ is isomorphic to $\mathscr{O}_Y|_{U_\alpha}$ for each α. □

Corollary 23.4.37. *Suppose that Y is affine. For $\mathscr{L}$ to be Y-ample, it is necessary and sufficient that $\mathscr{L}$ is ample.*

Proof. This is immediate from the definition of Y-ample, and Proposition 23.4.34(ii) and Theorem 23.4.23(ii), since

$$\operatorname{Proj}(\mathscr{S}) = \operatorname{Proj}(\Gamma(Y,\mathscr{S})) = \operatorname{Proj}(\bigoplus_{n\geq 0}\Gamma(Y, f_*(\mathscr{L}^{\otimes n}))) = \operatorname{Proj}(S)$$

in this case (note that Y is quasi-compact). □

Corollary 23.4.38. *Let $f : X \to Y$ be a quasi-compact morphism. Suppose that there exists a quasi-coherent $\mathscr{O}_Y$-module $\mathscr{E}$ and a Y-morphism $i : X \to P = \mathbb{P}(\mathscr{E})$ which is a homeomorphism from X onto a subspace of P. Then $\mathscr{L} = i^*(\mathscr{O}_P(1))$ is Y-ample.*

Proof. We can assume that Y is affine, and the corollary then follows from the criterion (i) of Theorem 23.4.23 and the formula (3.6.2). □

Proposition 23.4.39. *Let X be a quasi-compact and quasi-separated scheme and $f : X \to Y$ be a quasi-compact and quasi-separated morphism. For an invertible $\mathscr{O}_X$-module $\mathscr{L}$ to be f-ample, it is necessary and sufficient that following equivalent conditions are satisfied:*

(iii) For any quasi-coherent $\mathscr{O}_X$-module $\mathscr{F}$ of finite type, there exists an integer $n_0 > 0$ such that, for any $n \geq n_0$, the canonical homomorphism $\sigma : f^*(f_*(\mathscr{F} \otimes \mathscr{L}^{\otimes n})) \to \mathscr{F} \otimes \mathscr{L}^{\otimes n}$ is surjective.

(iii′) For any ideal $\mathscr{I}$ of $\mathscr{O}_X$ of finite type, there exist an integer $n > 0$ such that the canonical homomorphism $\sigma : f^*(f_*(\mathscr{I} \otimes \mathscr{L}^{\otimes n})) \to \mathscr{I} \otimes \mathscr{L}^{\otimes n}$ is surjective.

Proof. □

Proposition 23.4.40. *Let $f : X \to Y$ be a quasi-compact morphism and $\mathscr{L}$ be an invertible $\mathscr{O}_X$-module.*

(a) Let $n > 0$ be an integer. For $\mathscr{L}$ to be f-ample, it is necessary and necessary that $\mathscr{L}^{\otimes n}$ is f-ample.

(b) Let $\mathscr{L}'$ be an invertible $\mathscr{O}_X$-module, and suppose that there exists an integer $n > 0$ such that the canonical homomorphism $\sigma : f^*(f_*(\mathscr{L}'^{\otimes n})) \to \mathscr{L}'^{\otimes n}$ is surjective. Then, if $\mathscr{L}$ is f-ample, so is $\mathscr{L} \otimes \mathscr{L}'$.

Corollary 23.4.41. *The tensor product of two f-ample $\mathscr{O}_X$-modules is f-ample.*

Proposition 23.4.42. *Let $f : X \to Y$ be a morphism of finite type where Y is quasi-compact, and $\mathscr{L}$ be an invertible $\mathscr{O}_X$-module. For $\mathscr{L}$ to be f-ample, it is necessary and sufficient that the following equivalent conditions are satisfied:*

(iv) There exists $n_0 > 0$ such that, for any integer $n \geq n_0$, $\mathscr{L}^{\otimes n}$ is very ample relative to f.

(iv′) There exist $n > 0$ such that $\mathscr{L}^{\otimes n}$ is very ample relative to f.

Lemma 23.4.43. *Let $u : Z \to S$ be a morphism, $\mathscr{L}$ be an invertible $\mathscr{O}_S$-module, s a section of $\mathscr{L}$ over S, and t be the inverse image of s under u. Then $Z_t = u^{-1}(S_s)$.*

Proof. □

Lemma 23.4.44. *Let Z, Z' be two S-schemes, p, p' be the projections of $T = Z \times_S Z'$, $\mathscr{L}$ (resp. $\mathscr{L}'$) be an invertible $\mathscr{O}_Z$-module (resp. $\mathscr{O}_{Z'}$-module), t (resp. t') be a section of $\mathscr{L}$ (resp. $\mathscr{L}'$) over Z (resp. Z'), s (resp. s') be the inverse image of t (resp. t') under p (resp. p'). Then we have $T_{s \otimes s'} = Z_t \times_S Z'_{t'}$.*

Proof. □

Proposition 23.4.45 (Properties of Relative Ample Sheaves).

(i) For any scheme Y, any invertible $\mathscr{O}_Y$-module $\mathscr{L}$ is relative ample relative to the identify morphism 1_Y.

(ii) Let $f : X \to Y$ be a quasi-compact morphism and $j : X' \to X$ be a quasi-compact morphism that is a homeomorphism from X' onto a subspace of X. If $\mathscr{L}$ is an $\mathscr{O}_X$-module relative to f, then $j^*(\mathscr{L})$ is relative relative to $f \circ j$.

(iii) Let $f : X \to Y$ and $g : Y \to Z$ be quasi-compact morphisms where Z is quasi-compact. Let $\mathscr{L}$ an ample $\mathscr{O}_X$-module relative to f and $\mathscr{K}$ be an ample $\mathscr{O}_Y$-module relative to g. Then there exists an integer $n_0 > 0$ such that for any $n \geq n_0$, $\mathscr{L} \otimes f^*(\mathscr{K}^{\otimes n})$ is ample relative to $g \circ f$.

(iv) *Let $f : X \to Y$ be a quasi-compact morphism, $g : Y' \to Y$ be a morphism, and put $X' = X_{(Y')}$. If $\mathscr{L}$ is an ample $\mathscr{O}_X$-module relative to f, $\mathscr{L}' = \mathscr{L} \otimes_Y \mathscr{O}_{Y'}$ is ample relative to $f_{(Y')}$.*

(v) *Let $f_i : X_i \to Y_i$ $(i = 1, 2)$ be two quasi-compact S-morphisms. If $\mathscr{L}_i$ is an ample $\mathscr{O}_{X_i}$-module relative to f_i, then $\mathscr{L}_1 \otimes_S \mathscr{L}_2$ is ample relative to $f_1 \times_S f_2$.*

(vi) *Let $f : X \to Y$, $g : Y \to Z$ be two morphisms such that $g \circ f$ is quasi-compact. If an $\mathscr{O}_X$-module $\mathscr{L}$ is ample relative to $g \circ f$ and if g is separated or X is locally Noetherian, then $\mathscr{L}$ is ample relative to f.*

(vii) *Let $f : X \to Y$ be a quasi-compact morphism and $j : X_{\mathrm{red}} \to X$ be the canonical injection. If $\mathscr{L}$ is an ample $\mathscr{O}_X$-module relative to f, then $j^*(\mathscr{L})$ is ample relative to f_{red}.*

Proof. □

Proposition 23.4.46. *Let $f : X \to Y$ be a quasi-compact morphism, $\mathscr{I}$ be a locally nilpotent ideal of $\mathscr{O}_X$, Z the closed subscheme of X defined by $\mathscr{I}$, and $j : Z \to X$ be the cannical injection. For an invertible $\mathscr{O}_X$-module to be ample relative to f, it is necessary and sufficient that $j^*(\mathscr{L})$ is ample relative to $f \circ j$.*

Corollary 23.4.47. *Let X be a locally Noetherian scheme and $f : X \to Y$ be a quasi-compact morphism. For an invertible $\mathscr{O}_X$-module $\mathscr{L}$ to be ample relative to f, it is necessary and sufficient that its inverse image $\mathscr{L}'$ under the canonical injection $X_{\mathrm{red}} \to X$ is ample relative to f_{red}.*

Proposition 23.4.48. *Let $f : X \to Y$, $f' : X' \to Y$ be two morphisms, $X'' = X \amalg X'$, and $f'' = f \amalg f'$. Let $\mathscr{L}$ (resp. $\mathscr{L}'$) be an invertible $\mathscr{O}_X$-module (resp. $\mathscr{O}_{X'}$-module), and let $\mathscr{L}''$ be the invertible $\mathscr{O}_{X''}$-module which coincides with $\mathscr{L}$ over X and with $\mathscr{L}'$ over X'. For $\mathscr{L}''$ to be ample relative to f'', it is necessary and sufficent that $\mathscr{L}$ is ample relative to f and $\mathscr{L}'$ is ample relative to f'.*

Proposition 23.4.49. *Let Y be a quasi-compact scheme, $\mathscr{S}$ be a quasi-coherent graded $\mathscr{O}_Y$-algebra of finite type, $X = \mathrm{Proj}(\mathscr{S})$, and $f : X \to Y$ be the structural morphism. Then f is of finite type and there exists an integer $n > 0$ such that $\mathscr{O}_X(d)$ is invertible and f-ample.*

23.5 Quasi-affine, proper, and projective morphisms

23.5.1 Quasi-affine morphisms

We say a scheme is **quasi-affine** if it is isomorphic to the subscheme induced over a quasi-compact open subset of an affine scheme. We say a morphism $f : X \to Y$ is quasi-affine, or that X is a quasi-affine Y-scheme, if there exists an affine open cover (U_α) of Y such that $f^{-1}(U_\alpha)$ is a quasi-affine scheme. Since any quasi-compact open subscheme of an affine scheme is separated, it is clear that quasi-affine morphisms are separated and quasi-compact, and any affine morphism is quasi-affine.

Recall that for any scheme X, if $A = \Gamma(X, \mathscr{O}_X)$, the identify homomorphism $A \to A$ induces a canonical morphism $q : X \to \mathrm{Spec}(A)$ by Proposition 22.2.4. This is also the morphism $r_{\mathscr{L},\varepsilon} : X \to \mathrm{Proj}(S)$ in (4.5.1) defined for $\mathscr{L} = \mathscr{O}_X$, since $\Gamma(X, -)$ commutes with taking tensor product with $\mathscr{O}_X$ (cf. **??**) and we have $S = \bigoplus_{n \geq 0} \Gamma(X, \mathscr{O}_X)^{\otimes n} = A[T]$, and $\mathrm{Proj}(A[T])$ is canonically identified with $\mathrm{Spec}(A)$.

Proposition 23.5.1. *Let X be a quasi-compact scheme and $A = \Gamma(X, \mathcal{O}_X)$. The following conditions are equivalent:*

(i) X is a quasi-affine scheme.

(ii) The canonical morphism $q : X \to \mathrm{Spec}(A)$ is an open immersion.

(ii′) The canonical morphism $q : X \to \mathrm{Spec}(A)$ is a homeomorphism from X onto a subspace of $\mathrm{Spec}(A)$.

(iii) The $\mathcal{O}_X$-module $\mathcal{O}_X$ is very ample relative to q.

(iii′) The $\mathcal{O}_X$-module $\mathcal{O}_X$ is ample.

(iv) The subsets X_f, as f runs through A, form a basis for X.

(iv′) The subsets X_f which are affine, as f runs through A, form a basis for X.

(v) Any quasi-coherent $\mathcal{O}_X$-module is generated by its global sections.

(v′) Any quasi-coherent ideal of finite type of $\mathcal{O}_X$ is generated by its global sections.

Proof. It is clear that (ii)⇒(i) by definition, and (iii)⇒(iii′) by Proposition 23.4.29. Since the canonical morphisms $q : X \to \mathrm{Spec}(A)$ and $r_{\mathcal{O}_X,\varepsilon} : X \to \mathrm{Proj}(S)$ are identified, we see that (iii′)⇔(ii)⇔(ii′)⇔(iv)⇔(iv′) by Theorem 23.4.23. Also, (iii′)⇔(v)⇔(v′) in view of Proposition 23.4.25.

We also note that if X is quasi-affine, then it can be identified as an open subscheme of an affine scheme $Y = \mathrm{Spec}(B)$. Let $\varphi : B \to A$ be the correspond homomorphism (Proposition 22.2.4). Since the affine opens $D(g)$, with $g \in B$, form a basis of Y, and we have $X_f = D(g) \cap X$ where $f = \varphi(g)$, it follows that the subsets X_f which are affine, with $f \in A$, form a basis for X, which proves (i)⇒(iv′).

Finally, it remains to show that (i)⇒(iii). For this we first note that if X is quasi-affine then it is quasi-compact and separated, so by Corollary 22.6.15, for $f \in A$ we have $\Gamma(X_f, \mathcal{O}_X) = A_f$. Since we have $q^{-1}(D_+(f)) = X_f$, we conclude that the canonical morphism $q : X \to \mathrm{Spec}(A)$ is of finite type, and by Proposition 23.4.29, since $\mathcal{O}_X^{\otimes n}$ is isomorphic to $\mathcal{O}_X$ for any integer $n > 0$, $\mathcal{O}_X$ is very ample relative to q. This completes the proof. □

Remark 23.5.1. Let X be a quasi-affine scheme and $A = \Gamma(X, \mathcal{O}_X)$. By Proposition 23.5.1 we know that $\mathcal{O}_X$ is very ample relative to $q : X \to \mathrm{Spec}(A)$. Since X is separated and quasi-compact, by Proposition 22.6.54 we know that $q_*(\mathcal{O}_X)$ is quasi-coherent, and from $\Gamma(\mathrm{Spec}(A), q_*(\mathcal{O}_X)) = A$ we conclude that $q_*(\mathcal{O}_X) = \widetilde{A}$, so $q^*(q_*(\mathcal{O}_X)) = \mathcal{O}_X$ and the canonical homomorphism $\sigma : q^*(q_*(\mathcal{O}_X)) \to \mathcal{O}_X$ is identified with the identity on $\mathcal{O}_X$. This being so, the canonical morphism $r_{\mathcal{O}_X,\sigma} : X \to \mathbb{P}(q_*(\mathcal{O}_X))$ is then identified with $q : X \to \mathrm{Spec}(A)$, because we have

$$\mathbb{P}(q_*(\mathcal{O}_X)) = \mathrm{Proj}(\boldsymbol{S}(q_*(\mathcal{O}_X))) = \mathrm{Proj}(\boldsymbol{S}(A)) = \mathrm{Proj}(A[T]) = \mathrm{Spec}(A);$$

and we conclude from Proposition 23.5.1 that this is an open immersion, which justifies Proposition 23.4.13.

Corollary 23.5.2. *Let X be a quasi-compact scheme. If there exists a morphism $r : X \to Y$ from X into an affine scheme Y which is a homeomorphism onto an open subspace of Y, then X is quasi-affine.*

Proof. In fact, there then exists a family (g_α) of sections of $\mathscr{O}_Y$ over Y such that the $D(g_\alpha)$ form a basis for the topology of $r(X)$. If we put $f_\alpha = \theta(g_\alpha)$ where $\theta : \Gamma(Y, \mathscr{O}_Y) \to \Gamma(X, \mathscr{O}_X)$ is the corresponding ring homomorphism, then we have $X_{f_\alpha} = r^{-1}(D(g_\alpha))$, so the X_{f_α} form a basis for X, and by Proposition 23.5.1 X is then quasi-affine. □

Corollary 23.5.3. *If X is a quasi-affine scheme, any invertible $\mathscr{O}_X$-module is very ample (relative to the canonical morphism $q : X \to \operatorname{Spec}(A)$) and a fortiori ample.*

Proof. In fact any such module $\mathscr{L}$ is generated by its global sections (Proposition 23.5.1(v)), so $\mathscr{L} \otimes \mathscr{O}_X$ is very ample by Proposition 23.4.17. We also note that the morphism q is of finite type. □

Corollary 23.5.4. *Let X be a quasi-compact scheme. If there exists an invertible $\mathscr{O}_X$-module $\mathscr{L}$ such that $\mathscr{L}$ and $\mathscr{L}^{-1}$ are ample, then X is quasi-affine.*

Proof. In fact, $\mathscr{O}_X = \mathscr{L} \otimes \mathscr{L}^{-1}$ is then ample by Corollary 23.4.27. □

Proposition 23.5.5. *Let $f : x \to Y$ be a quasi-compact morphism. The following conditions are equivalent:*

(i) f is quasi-affine.

(ii) The $\mathscr{O}_Y$-algebra $f_*(\mathscr{O}_X) = \mathscr{A}(X)$ is quasi-coherent and the canonical morphism $X \to \operatorname{Spec}(\mathscr{A}(X))$ corresponding to the identity homomorphism of $\mathscr{A}(X)$ is an open immersion.

(ii′) The $\mathscr{O}_Y$-algebra $\mathscr{A}(X)$ is quasi-coherent and the canonical morphism $X \to \operatorname{Spec}(\mathscr{A}(X))$ is a homeomorphism from X onto a subspace of $\operatorname{Spec}(\mathscr{A}(X))$.

(iii) The $\mathscr{O}_X$-module $\mathscr{O}_X$ is very ample relative to f.

(iii′) The $\mathscr{O}_X$-module $\mathscr{O}_X$ is ample relative to f.

(iv) The morphism f is separated and for any quasi-coherent $\mathscr{O}_X$-modle $\mathscr{F}$, the canonical homomorphism $\sigma : f^*(f_*(\mathscr{F})) \to \mathscr{F}$ is surjective.

Morever, if f is quasi-affine, any invertible $\mathscr{O}_X$-module $\mathscr{L}$ is very ample relative to f.

Proof. The equivalence of these properties follows from the fact that they are all local over Y and the criteria of Proposition 23.5.1. Also, we note that $f_*(\mathscr{F})$ is quasi-coherent if f is separated (Proposition 22.6.54). The last assertion follows from Corollary 23.5.3. □

Corollary 23.5.6. *Let Y be an affine scheme and $f : X \to Y$ be a quasi-compact morphism. For f to be quasi-affine, it is necessary and sufficient that X is quasi-affine scheme.*

Proof. This is an immediate concequence of Proposition 23.5.5 and Corollary 23.4.37. □

Corollary 23.5.7. *Let Y be a quasi-compact and quasi-separated scheme, $f : X \to Y$ be a morphism of finite type. If f is quasi-affine, there exists a quasi-coherent sub-$\mathscr{O}_Y$-algebra $\mathscr{B}$ of $\mathscr{A}(X)$ of finite type such that the morphism $X \to \operatorname{Spec}(\mathscr{B})$ corresponding to the canonical injection $\mathscr{B} \to \mathscr{A}(X)$ is an immersion. Moreover, any quasi-coherent sub-$\mathscr{O}_Y$-algebra of finite type $\mathscr{B}'$ of $\mathscr{A}(X)$, containing $\mathscr{B}$, has the same property.*

Proof. In fact, $\mathscr{A}(X)$ is the inductive limit of its quasi-coherent sub-$\mathscr{O}_Y$-algebras of finite type (Corollary 22.6.62); the assertion is then a particular case of Proposition 23.3.41, in view of the identification of $\operatorname{Spec}(\mathscr{A}(X))$ and $\operatorname{Proj}(\mathscr{A}(X)[T])$ (Corollary 23.3.5) and the canonical morphisms from X into them (cf. Remark 23.5.1). □

Proposition 23.5.8 (Properties of Quasi-affine Morphisms).

(i) A quasi-compact morphism $f : X \to Y$ that is a homeomorphism from X onto a subspace of Y (and in particular a quasi-compact immersion) is quasi-affine.

(ii) The composition of two quasi-affine morphisms is quasi-affine.

(iii) If $f : x \to Y$ is a quasi-affine S-morphism, $f_{(S')} : X_{(S')} \to Y_{(S')}$ is a quasi-affine morphism for any base change $S' \to S$.

(iv) If $f : X \to Y$ and $g : X' \to Y'$ are two quasi-affine S-morphisms, so is $f \times_S g$.

(v) If $f : X \to Y$, $g : Y \to Z$ are two morphisms such that $g \circ f$ is quasi-affine and if g is separated or X is locally Noetherian, then f is quasi-affine.

(vi) Let $f : X \to Y$ be a quasi-compact morphism and $j : X_{\mathrm{red}} \to X$ the canonical injection. If an $\mathscr{O}_X$-module $\mathscr{L}$ is ample relative to f, then $j^*(\mathscr{L})$ is ample relative to f_{red}.

Proof. In view of the criterion (iii') of Proposition 23.5.5, (i), (iii), (iv), (v) and (vi) are concequences of Proposition 23.4.45. To prove (ii), we can assume that Z is affine, and the assertion then follows from Proposition 23.4.45(iii), applied to $\mathscr{L} = \mathscr{O}_X$ and $\mathscr{K} = \mathscr{O}_Y$. □

Remark 23.5.2. Let $f : X \to Y$, $g : Y \to Z$ be two morphisms such that $X \times_Z Y$ is locally Noetherian. Then the graph morphism $\Gamma_f : X \to X \times_Z Y$ is a quasi-compact immersion, hence quasi-affine, and the reasoning of Proposition 22.5.14 shows that the conclusion of (v) remains valid if we remove the hypothesis that g is separated.

Proposition 23.5.9. *Let $f : X \to Y$ be a quasi-compact morphism and $g : X' \to X$ be a quasi-affine morphism. If $\mathscr{L}$ is an f-ample $\mathscr{O}_X$-module, then $g^*(\mathscr{L})$ is ample relative to $f \circ g$.*

Proof. By hypothesis $\mathscr{O}_{X'}$ is very ample relative to f, and since the question is local over Y, it follows from Proposition 23.4.45(iii) that there exists (for Y affine) an integer n such that $g^*(\mathscr{L}^{\otimes n}) = (g^*(\mathscr{L}))^{\otimes n}$ is ample relative to $f \circ g$, whence $g^*(\mathscr{L})$ is ample relative to $f \circ g$. □

23.5.2 Serre's criterion on affineness

Theorem 23.5.10 (Serre's criterion). *For a quasi-compact and quasi-separated scheme X, then the following conditions are equivalent:*

(i) X is an affine scheme.

(ii) There exists a family (f_α) of elements of $A = \Gamma(X, \mathscr{O}_X)$ such that X_{f_α} are affine and the ideal generated by the f_α equals to A.

(iii) The functor $\Gamma(X, -)$ is exact on the category of quasi-coherent $\mathscr{O}_X$-modules.

(iii′) For any exact sequence of quasi-coherent $\mathscr{O}_X$-modules

$$0 \longrightarrow \mathscr{F}' \longrightarrow \mathscr{F} \longrightarrow \mathscr{F}'' \longrightarrow 0$$

where $\mathscr{F}$ is isomorphic to a sub-$\mathscr{O}_X$-module of a finite product $\mathscr{O}_X^n$, the induced sequence

$$0 \longrightarrow \Gamma(X, \mathscr{F}') \longrightarrow \Gamma(X, \mathscr{F}) \longrightarrow \Gamma(X, \mathscr{F}'') \longrightarrow 0$$

is exact.

(iv) $H^1(X, \mathscr{F}) = 0$ for any quasi-coherent $\mathscr{O}_X$-module $\mathscr{F}$.

(iv′) $H^1(X, \mathscr{I}) = 0$ for any quasi-coherent ideal $\mathscr{I}$ of $\mathscr{O}_X$.

Proof. It is clear that (i) implies (ii); (ii) implies on the oter hand that the X_{f_α} cover X, since by hypothesis the unit section 1 is a linear combination of f_α, and that the $D(f_\alpha)$ cover $\operatorname{Spec}(A)$. The last assertion of Theorem 23.4.23 then implies that $X \to \operatorname{Spec}(A)$ is an isomorphism.

We have seen that (i) implies (iii), and it is trivial that (iii) implies (iii′). On the other hand, (iii′) implies that, for any closed point $x \in X$ and any open neighborhood U of x, there exists $f \in A$ such that $x \in X_f \subseteq X - U$. To see this, let $\mathscr{I}$ (resp. $\mathscr{I}'$) be the quasi-coherent ideal of $\mathscr{O}_X$ defining the reduced closed subscheme of X with underlying space $X - U$ (resp. $(X - U) \cup \{x\}$). It is clear that $\mathscr{I}' \subseteq \mathscr{I}$, and the quotient $\mathscr{I}'' = \mathscr{I}/\mathscr{I}'$ is a quasi-coherent $\mathscr{O}_X$-module. By hypothesis, the stalk of $\mathscr{O}_X/\mathscr{I}$ and $\mathscr{O}_X/\mathscr{I}'$ are zero at any point $x \in U - \{x\}$. Moreover, since $\{x\}$ is closed in X, the subscheme $X - U$ is *open and closed* in $(X - U) \cup \{x\}$, so we conclude that $(\mathscr{O}_X/\mathscr{I})_z = (\mathscr{O}_X/\mathscr{I}')_z$ for $z \in X - U$, and therefore $\mathscr{I}''_z = 0$. At the point x, we have $\mathscr{I}_x = \mathscr{O}_X$, while $\mathscr{I}'_x = \mathfrak{m}_x$ (cf. Example 22.4.42), so $\mathscr{I}''$ is supported at $\{x\}$ and $\mathscr{I}''_x = \kappa(x)$. The hypothesis of (iii′) applied to the exact sequence $0 \to \mathscr{I}' \to \mathscr{I} \to \mathscr{I}'' \to 0$ shows that $\Gamma(X, \mathscr{I}) \to \Gamma(X, \mathscr{I}'')$ is surjective, so the section of $\mathscr{I}''$ whose germ at x equals to 1_x is the image of a section $f \in \Gamma(X, \mathscr{I}) \subseteq \Gamma(X, \mathscr{O}_X)$, and we have by definition $f(x) = 1_x$ and $f(y) = 0$ over $X - U$, which proves the assertion. Moreover, if U is affine, so is X_f, and the union X' of these affine opens X_f (with $f \in A$) is then an open subset of X containing any closed point of X. As X is a quasi-compact Kolmogoroff space, we then have $X' = X$ (**??**). Since X is quasi-compact, there are finitely many elements $f_i \in A$ $(1 \leq i \leq n)$ such that (X_{f_i}) is an affine open cover of X. Consider the homomorphism $\mathscr{O}_X^n \to \mathscr{O}_X$ defined by the sections f_i; since for any $x \in X$ at least one of the $(f_i)_x$ is invertible, this homomorphism is surjective, and we then get an exact sequence

$$0 \longrightarrow \mathscr{R} \longrightarrow \mathscr{O}_X^n \longrightarrow \mathscr{O}_X \longrightarrow 0$$

where $\mathscr{R}$ is a quasi-coherent sub-$\mathscr{O}_X$-module of $\mathscr{O}_X$. It then follows from (iii′) that the corresponding homomorphism $\Gamma(X, \mathscr{O}_X^n) \to \Gamma(X, \mathscr{O}_X)$ is surjective, which proves (ii).

Finally, (i) implies (iv) and (iv) implies (iv′). We show that (iv′) implies (iii′). Now, if $\mathscr{F}'$ is a quasi-coherent sub-$\mathscr{O}_X$-module of $\mathscr{O}_X^n$, the filtration $0 \subseteq \mathscr{O}_X \subseteq \mathscr{O}_X^2 \cdots \subseteq \mathscr{O}_X^n$ defines over $\mathscr{F}'$ a filtration of the form $\mathscr{F}'_k = \mathscr{F} \cap \mathscr{O}_X^k$ $(0 \leq k \leq n)$, which are quasi-coherent $\mathscr{O}_X$-modules (Corollary 22.2.20(ii)), and $\mathscr{F}'_{k+1}/\mathscr{F}'_k$ is isomorphic to a quasi-coherent sub-$\mathscr{O}_X$-module of $\mathscr{O}_X^{k+1}/\mathscr{O}_X^k = \mathscr{O}_X$, which is thus a quasi-coherent ideal of $\mathscr{O}_X$. In the exact sequence

$$H^1(X, \mathscr{F}'_k) \longrightarrow H^1(X, \mathscr{F}'_{k+1}) \longrightarrow H^1(\mathscr{F}'_{k+1}/\mathscr{F}'_k) = 0$$

by hypothesis of (iv′) we have $H^1(\mathscr{F}'_{k+1}/\mathscr{F}'_k) = 0$; since $H^0(X, \mathscr{F}'_0) = 0$, we conclude by recurrence on k that $H^1(X, \mathscr{F}'_k) = 0$ for each k, whence the claim. □

Remark 23.5.3. Note that if X is a covering of (X_{f_i}) with X_{f_i} being affine, then X is automatically quasi-separated, since for any couple (i, j) of indices we have $X_{f_i} \cap X_{f_j} = D_{X_{f_i}}(f_j|_{X_{f_i}})$, which is an affine open of X_{f_i} and hence quasi-compact (Proposition 22.6.10).

Remark 23.5.4. If X is a Noetherian scheme, then in conditions (iii′) and (iv′) we can replace "quasi-coherent" by "coherent". In fact, in the demonstration that (iii′) implies (ii), $\mathscr{I}$ and $\mathscr{I}'$ are then coherent ideals, and moreover, any quasi-coherent submodule of a coherent module is coherent (Theorem 22.1.29), whence the assertion.

Corollary 23.5.11. *Let $f : X \to Y$ be a quasi-compact and quasi-separated morphism. Then the following conditions are equivalent:*

(i) f is an affine morphism.

(ii) The functor f_* is exact on the cateogry of quasi-coherent $\mathscr{O}_X$-modules.

(iii) For any quasi-coherent $\mathscr{O}_X$-module $\mathscr{F}$, we have $R^1 f_*(\mathscr{F}) = 0$.

(iii′) For any quasi-coherent ideal $\mathscr{I}$ of $\mathscr{O}_X$, we have $R^1 f_*(\mathscr{I}) = 0$.

Proof. Any of these conditions are local over Y, by the definition of $R^1 f_*(\mathscr{F})$ (that is, the sheaf associated with the presheaf $U \mapsto H^1(f^{-1}(U), \mathscr{F})$), so we may assume that Y is affine. If f is affine, X is then affine and (ii) follows from Corollary 22.1.12. Conversely, we prove that (ii) implies (i): for any quasi-coherent $\mathscr{O}_X$-module $\mathscr{F}$, $f_*(\mathscr{F})$ is a quasi-coherent $\mathscr{O}_Y$-module by Proposition 22.6.54. By hypothesis the fonctor f_* is exact; $\Gamma(Y, -)$ is exact since Y is affine, so we conclude that $\Gamma(Y, f_*(-)) = \Gamma(X, -)$ is exact, which proves that X is affine in view of Theorem 23.5.10.

If f is affine, $f^{-1}(U)$ is affine for any affine open U of Y, so $H^1(f^{-1}(U), \mathscr{F}) = 0$ by Theorem 23.5.10, which means $R^1 f_*(\mathscr{F}) = 0$. Finally, suppose that (iii′) is satisfied; the exact sequence of low-degree terms in the Leray spectral sequence gives

$$0 \longrightarrow H^1(Y, f_*(\mathscr{I})) \longrightarrow H^1(X, \mathscr{I}) \longrightarrow H^0(Y, R^1 f_*(\mathscr{I}))$$

As Y is affine and $f_*(\mathscr{I})$ is quasi-coherent (Proposition 22.6.54), we have $H^1(Y, f_*(\mathscr{I})) = 0$, so the hypothesis of (iii′) imlies that $H^1(X, \mathscr{I}) = 0$, and we conclude from Theorem 23.5.10 that X is an affine scheme. □

Corollary 23.5.12. *If $f : X \to Y$ is an affine morphism then for any quasi-coherent $\mathscr{O}_X$-module $\mathscr{F}$, the canonical homomorphism $H^1(Y, f_*(\mathscr{F})) \to H^1(X, \mathscr{F})$ is bijective.*

Proof. In fact, we have an exact sequence

$$0 \longrightarrow H^1(Y, f_*(\mathscr{F})) \longrightarrow H^1(X, \mathscr{F}) \longrightarrow H^0(Y, R^1 f_*(\mathscr{F}))$$

which comes from the lower terms of the Leray spectral sequence, and the conclusion follows from Corollary 23.5.11. □

23.5.3 Quasi-projective morphisms

We say a morphism $f : X \to Y$ is **quasi-projective**, of that X is **quasi-projective over Y**, or that X is a **quasi-projective Y-scheme**, if f is of finite type and there exists an invertible $\mathcal{O}_X$-module that is f-ample. It is clear that a quasi-projective morphism is necessarily separated. If Y is quasi-compact, it is also equivalent to say that f is of finite type and there exists a very ample $\mathcal{O}_X$-module relative to f (Proposition 23.4.33).

Remark 23.5.5. It should be noted that this definition is not local over Y. There exist examples where X and Y are nonsingular algebraic schemes over an algebraically closed field such that any point of Y admits an affine neighborhood U such that $f^{-1}(U)$ is quasi-projective over U, but f is not quasi-projective.

Proposition 23.5.13. *Let Y be a quasi-compact and quasi-separated scheme and X be a Y-scheme. Then the following conditions are equivalent:*

(i) X is a quasi-projective Y-scheme.

(ii) X is of finite type over Y and there exists a quasi-coherent $\mathcal{O}_Y$-module $\mathcal{E}$ of finite type such that X is Y-isomorphic to a subscheme of $\mathbb{P}(\mathcal{E})$.

(iii) X is of finite type over Y and there exists a quasi-coherent graded $\mathcal{O}_Y$-algebra $\mathcal{S}$ that is generated by $\mathcal{S}_1$ and $\mathcal{S}_1$ is of finite type such that X is isomorphic to a dense open subscheme of $\mathrm{Proj}(\mathcal{S})$.

Proof. This follows from Corollary 23.4.12, Proposition 23.4.15 and Corollary 23.4.16. □

Corollary 23.5.14. *Let Y be a quasi-compact and quasi-separated scheme such that there exists an ample $\mathcal{O}_Y$-module $\mathcal{L}$. For a Y-scheme X to be quasi-projective, it is necessary and sufficient that X is of finite type over Y and is isomorphic to a sub-Y-scheme of a projective bundle of the form $\mathbb{P}^r_Y$.*

Proof. By the hypothesis on Y, if $\mathcal{E}$ is a quasi-coherent $\mathcal{O}_Y$-module of finite type, $\mathcal{E}$ is isomorphic to a quotient of an $\mathcal{O}_Y$-module $\mathcal{L}^{\otimes(-n)} \otimes_{\mathcal{O}_Y} \mathcal{O}_Y^k$ (Proposition 23.4.25), so $\mathbb{P}(\mathcal{E})$ is isomorphic to a closed subscheme of $\mathbb{P}^{k-1}_Y$ (Proposition 23.4.1). □

Proposition 23.5.15 (Properties of Quasi-projective Morphisms).

(i) A quasi-affine morphism of finite type (in particular a quasi-compact immersion or an affine morphism of finite type) is quasi-projective.

(ii) If $f : X \to Y$ and $g : Y \to Z$ are quasi-projective and if Z is quasi-compact, $g \circ f$ is quasi-projective.

(iii) If $f : X \to Y$ is a quasi-projective S-morphism, $f_{(S')} : X_{(S')} \to Y_{(S')}$ is quasi-projective for any base change $S' \to S$.

(iv) If $f : X \to Y$ and $g : X' \to Y'$ are two quasi-projective S-morphisms, $f \times_S g$ is quasi-projective.

(v) If $f : X \to Y$, $g : y \to Z$ are two morphisms such that $g \circ f$ is quasi-projective and if g is separated or X is locally Noetherian, then f is quasi-projective.

(vi) If f is quasi-projective, so is f_{red}.

Proof. Property (i) follows from Proposition 23.5.5 and Proposition 23.4.45(i). The other parts follows from the definition of quasi-projective morphism and Proposition 23.4.45, with the corresponding properties of morphisms of finite type (Proposition 22.6.35). □

Remark 23.5.6. Note that it may happen that f_{red} is quasi-projective without f being so, even we assume that Y is the spectrum of a finite dimensional algebra over C and f is proper.

Corollary 23.5.16. *If X and X' are two quasi-projective Y-schemes, $X \amalg X'$ is quasi-projective over Y.*

Proof. This follows from Proposition 23.4.48. □

23.5.4 Universally closed and proper morphisms

As the terminology indicates, we say a morphism $f : X \to Y$ is **universally closed** if the projection $f \times_Y 1_{Y'} : X \times_Y Y' \to Y'$ is closed for any base change $Y' \to Y$. By Corollary 22.4.12, we know that a closed immersion is universally closed. We say a morphism $f : X \to Y$ is **proper** if it is separated, of finite type, and universally closed, and in this case X is said to be **proper over Y**, or a **proper Y-scheme**. It is clear that all these notations are local over Y. We also note that, to verify that the image of a closed subset Z of $X \times_Y Y'$ under the projection $q : X \times_Y Y' \to Y'$ is closed in Y', it suffices to shows that $q(Z) \cap U'$ is closed in U' for any affine open subset U' of Y'. As $q(Z) \cap U' = q(Z \cap q^{-1}(U'))$ and $q^{-1}(U')$ is identified with $X \times_Y U'$ (Corollary 22.3.2), we see that to verify the universally closedness of f, it suffices to limit the case where Y' is affine. We will see later that if Y is locally Noetherian, we can even assume that Y' is of finite type over Y.

Proposition 23.5.17 (Properties of Proper Morphisms).

(i) A closed immersion is proper.

(ii) The composition of two proper morphisms is proper.

(iii) If $f : X \to Y$ is a proper S-morphism, then $f_{(S')} : X_{(S')} \to Y_{(S')}$ is proper for any base change $S' \to S$.

(iv) If $f : X \to Y$ and $g : X' \to Y'$ are two proper S-morphisms, then $f \times_S g$ is proper.

Proof. It suffices to prove the first three properties. In view of Proposition 22.5.25 and Proposition 22.6.35, it suffices to verify the universally closedness in each cases. This is trivial in (i) since closed immersions are universal. For (ii), consider two proper morphisms $X \to Y$, $Y \to Z$, and a morphism $Z' \to Z$. We have $X \times_Z Z' = X \times_Y (Y \times_Z Z')$ and therefore the projection $X \times_Z Z' \to Z'$ factors into $X \times_Y (Y \times_Z Z') \to Y \times_Z Z' \to Z'$. By hypothesis, this is a composition of two closed morphisms, hence closed. Finally, in (iii), for any morphism $S' \to S$, $X_{(S')}$ is identified with $X \times_Y Y_{(S')}$; for any morphism $Z \to Y_{(S')}$, we have

$$X_{(S')} \times_{Y_{(S')}} Z = (X \times_Y Y_{(S')}) \times_{Y_{(S')}} Z = X \times_Y Z$$

and $X \times_Y Z \to Z$ is closed by hypothesis, so (iii) follows. □

Corollary 23.5.18. *Let $f : X \to Y$, $g : Y \to Z$ be two morphisms such that $g \circ f$ is proper.*

(a) If g is separated, f is proper.

(b) If g is separated and of finite type and f is surjective, then g is proper.

Proof. The first claim follows from Proposition 22.5.22. To prove (b), we only need to verify that g is universally closed. For any morphism $Z' \to Z$, the diagram

$$\begin{tikzcd} X \times_Z Z' \arrow[r, "f \times 1_{Z'}"] \arrow[dr, "p"'] & Y \times_Z Z' \arrow[d, "p'"] \\ & Z' \end{tikzcd}$$

(where p and p' are projections) is commutative. Moreover, $f \times 1_{Z'}$ is surjective if f is (Proposition 22.3.26), and p is a closed immersion by hypothesis. Any closed subset F of $Y \times_Z Z'$ is then the image under $f \times 1_{Z'}$ of a closed subset E of $X \times_Z Z'$, so $p'(F) = p(E)$ is closed in Z' by hypothesis, whence the corollary. □

Corollary 23.5.19. *If X is a proper scheme over Y and $\mathcal{S}$ is a quasi-coherent $\mathcal{O}_Y$-algebra, any Y-morphism $f : X \to \operatorname{Proj}(\mathcal{S})$ is proper (and a fortiori closed).*

Proof. In fact, the structural morphism $p : \operatorname{Proj}(\mathcal{S}) \to Y$ is separated, and $p \circ f$ is proper by hypothesis. □

Corollary 23.5.20. *Let $f : X \to Y$ be a separated morphism of finite type. Let $(X_i)_{1 \leq i \leq n}$ (resp. $(Y_i)_{1 \leq i \leq n}$) be a family of closed subscheme of X (Resp. Y), $j_i : X_i \to X$ (resp. $h_i : Y_i \to Y$) be the canonical injection. Suppose that (X_i) forms a covering of X and for each i, let $f_i : X_i \to Y_i$ be a morphism such that the diagram*

$$\begin{tikzcd} X_i \arrow[r, "f_i"] \arrow[d, "j_i"'] & Y_i \arrow[d, "h_i"] \\ X \arrow[r, "f"] & Y \end{tikzcd}$$

is commutative. Then, for f to be proper, it is necessary and sufficient that each f_i is proper.

Proof. If f is proper, so is each $f \circ j_i$, since j_i is a closed immersion; as each h_i is a closed immersion, hence separated, f_i is proper by Corollary 23.5.18. Suppose conversely that each f_i is proper, and consider the sum Z of X_i; let $u : Z \to X$ be the morphism that induces j_i on X_i. The restriction of $f \circ u$ to each X_i is equal to $f \circ j_i = h_i \circ f_i$, hence proper; it then follows that $f \circ u$ is proper. Since u is surjective by hypothesis, we conclude from Corollary 23.5.18 that f is proper. □

Corollary 23.5.21. *Let $f : X \to Y$ be a separated morphism of finite type. For f to be proper, it is necessary and sufficient that $f_{\mathrm{red}} : X_{\mathrm{red}} \to Y_{\mathrm{red}}$ is proper.*

Proof. This is a particular case where $n = 1$, $X_1 = X_{\mathrm{red}}$ and $Y_1 = Y_{\mathrm{red}}$. □

If X and Y and Noetherian schemes and $f : X \to Y$ is a separated morphism of finite type, to verify that f is proper, we can reduce to dominant morphisms of integral schemes. In fact, let X_i $(1 \leq i \leq n)$ be the irreducible components of X and consider for each i the unique reduced closed subscheme structure on X_i. Let Y_i be the reduced closed subscheme with underlying space $\overline{f(X_i)}$. If $j_i : X_i \to X$ (resp. $h_i : Y_i \to Y$) are the canonical injections, we then have $f \circ j_i = h_i \circ f_i$, where f_i is a dominant morphism $f_i : X_i \to Y_i$. We then see that the conditions

of Corollary 23.5.20 are satisfied, and for f to be proper, it is necessary and sufficient that each f_i is.

Corollary 23.5.22. *Let X and Y be separated S-schemes of finite type and $f : X \to Y$ be an S-morphism. For f to be proper, it is necessary and sufficient that for any S-scheme S', the morphism $f_{(S')} : X_{(S')} \to Y_{(S')}$ is closed.*

Proof. We note that if $\varphi : X \to S$ and $\psi : Y \to S$ are the structural morphisms, we have $\varphi = \psi \circ f$, so f is separated and of finite type (Proposition 22.5.25 and Proposition 22.6.35). If f is proper, so is $f_{(S')}$, and is a fortiori closed. Conversely, assume this condition and let Y' be a Y-scheme; Y' can be considered as an S-scheme, and the morphism $Y \to S$ is separated. In the commutative diagram

$$\begin{tikzcd} X \times_Y Y' \arrow[r, "f \times_Y 1_{Y'}"] \arrow[d] & Y \times_Y Y' = Y' \arrow[d] \\ X \times_S Y' \arrow[r, "f_{(Y')}"] & Y \times_S Y' \end{tikzcd}$$

the vertical morphisms are a closed immersion by Proposition 22.5.18. It follows from the assumption that $f_{(Y')}$ is closed, and so is $f \times_Y 1_{Y'}$. □

Let $f : X \to Y$ be a morphism of finit type. We say that a closed subset Z of X is **proper over** Y (or **Y-proper**, or **f-proper**) if the restriction of f to a closed subscheme of X with underlying space Z is proper. As this restriction is then separated, it follows from Corollary 23.5.21 and Proposition 22.5.25(vi) the property that Z is proper over Y is independent of the closed subscheme structural chosen for Z.

Let Z be a proper subset of X for f and let $g : X' \to X$ be a proper morphism. Then $g^{-1}(Z)$ is then a proper subset of X': if T is a subscheme of X with underlying space Z, it suffices to note that the restriction of g to the closed subscheme $g^{-1}(T)$ of X' is a proper morphism $g^{-1}(T) \to T$ by Proposition 23.5.17(iii), and we can apply Proposition 23.5.17(ii) to conclude that $g^{-1}(T)$ is proper.

On the other hand, if X'' is a Y-scheme of finite type and $h : X \to X''$ is a Y-morphism, $h(Z)$ is also a proper subset of X'': in fact, for any reduced closed subscheme T of X with underlying space Z. The restriction of f to T is proper, and so is the restriction of h to T (Corollary 23.5.18(a)), so $h(Z)$ is closed in X''. Let T'' be a closed subscheme of X'' with underlying space $h(Z)$ so that the morphism $h|_T$ factors into (cf. Proposition 22.4.44)

$$T \xrightarrow{h|_T} T'' \xrightarrow{j} X''$$

where j is the canonical injection. Then $h|_T$ is proper by Corollary 23.5.20 and surjective. If $\psi : X'' \to Y$ is the structural morphism, $\psi|_{T''}$ is then separated of finite type (Proposition 22.5.25 and Proposition 22.6.35), and we have $f|_T = (\psi|_{T''}) \circ (h|_T)$; it then follows from Proposition 23.5.17(ii) that $\psi|_{T''}$ is proper, whence the assertion.

In particular, for a Y-proper subset of X, we have the following:

(a) For any closed subset X' of X, $Z \cap X'$ is a Y-proper subset of X'.

(b) If X is a subscheme of a Y-scheme of finite type X'', Z is also a Y-proper subset of X'' (and in particular is closed in X'').

23.5.5 Projective morphisms

Proposition 23.5.23. *Let X be a Y-scheme. The following conditins are equivalent:*

(a) X is Y-isomorphic to a closed subscheme of a projective bundle $\mathbb{P}(\mathscr{E})$, where $\mathscr{E}$ is a quasi-coherent $\mathscr{O}_Y$-module of finite type.

(b) There exists a quasi-coherent graded $\mathscr{O}_Y$-algebra such that $\mathscr{S}_1$ is of finite type and generates $\mathscr{S}$, and that X is Y-isomorphic to a $\operatorname{Proj}(\mathscr{S})$.

Proof. Condition (a) implies (b) by Proposition 23.3.30(b): if $\mathscr{I}$ is the quasi-coherent graded ideal of $\boldsymbol{S}(\mathscr{E})$, the quasi-coherent graded $\mathscr{O}_Y$-algebra $\mathscr{S} = \boldsymbol{S}(\mathscr{E})/\mathscr{I}$ is generateed by $\mathscr{S}_1$ and the later, which is the canonical image of $\mathscr{E}$, is an $\mathscr{O}_X$-module of finite type. Condition (b) implies (a) in view of Corollary 23.3.32 applied to the case where $\mathscr{M} \to \mathscr{S}_1$ is the identify homomorphism. □

We say a Y-scheme X is **projective over $\boldsymbol{Y}$** or a projective **$\boldsymbol{Y}$-scheme** if it satisfies the equivalent conditions of Proposition 23.5.23. We say a morphism $f : X \to Y$ is **projective** if X is a projective Y-scheme via this morphism. It is clear that if $f : X \to Y$ is projective, then there exists a very ample $\mathscr{O}_X$-module relative to f (Corollary 23.4.12).

Theorem 23.5.24. *Any projective morphism is quasi-projective and proper. Conversely, if Y is a quasi-compact and quasi-separated scheme, any quasi-projective and proper morphism $f : X \to Y$ is projective.*

Proof. It is clear that any projective morphism is of finite type and quasi-projective. On the other hand, it follows from Proposition 23.5.23(b) and Proposition 23.3.28 that if f is projective, so is $f \times_Y 1_{Y'} : X \times_Y Y' \to Y'$ for any morphism $Y' \to Y$. The proof that f is universally closed then boils down to show that a projective morphism f is closed. The question is local over Y, so we can suppose that $Y = \operatorname{Spec}(A)$ is affine, so by Proposition 23.5.23 $X = \operatorname{Proj}(S)$ where S is a graded A-algebra generated by finitely many elements of S_1. For any $y \in Y$, the fiber $f^{-1}(y)$ is identified with $\operatorname{Proj}(S) \times_Y \operatorname{Spec}(\kappa(y))$, hence to $\operatorname{Proj}(S \otimes_A \kappa(y))$ (Proposition 23.2.48). Therefore, $f^{-1}(y)$ is empty if and only if $S \otimes_A \kappa(y)$ is eventually zero, which meaens $S_n \otimes_A \kappa(y) = 0$ for n sufficiently large. Now as $(S_n)_y$ is an $\mathscr{O}_{Y,y}$-module of finite type, the preceding condition signifies that $(S_n)_y = 0$ for n sufficiently large, in view of Nakayama's lemma. If $\mathfrak{a}_n$ is the annihilator in A of the A-module S_n, the preceding condition is then equivalent to that $\mathfrak{a}_n \subseteq \mathfrak{p}_y$ for n sufficiently large. Now as $S_n S_1 = S_{n+1}$ by hypothesis, we have $\mathfrak{a}_n \subseteq \mathfrak{a}_{n+1}$, and if $\mathfrak{a}$ is the sum of $\mathfrak{a}_n$, we then have $f(X) = V(\mathfrak{a})$, so $f(X)$ is closed in Y. If now X' is a closed subset of X, there exists a closed subscheme of X with underlying space X' and it is clear (by Proposition 23.5.23(a)) that the composition morphism $X' \to X \to Y$ is projective, so $f(X')$ is closed in Y.

Now conversely, assume that Y is quasi-compact and quasi-separated. The hypothesis that f is quasi-projective implies the existence of a quasi-coherent $\mathscr{O}_Y$-module of finite type $\mathscr{E}$ and a Y-immersion $j : X \to \mathbb{P}(\mathscr{E})$ (Proposition 23.5.13). Since f is proper and the structural morphism $\mathbb{P}(\mathscr{E}) \to Y$ is separated, j is proper (hence closed) by Corollary 23.5.18(a), so f is projective. □

Remark 23.5.7. Let $f : X \to Y$ be a morphism such that

(i) f is proper

(ii) there exists a very ample $\mathscr{O}_X$-module $\mathscr{L}$ relative to f

(iii) the quasi-coherent $\mathscr{O}_Y$-module $\mathscr{E} = f_*(\mathscr{L})$ is of finite type

Then f is projective: there then exists a Y-immersion $j : X \to \mathbb{P}(\mathscr{E})$, and since f is proper, j is a closed immersion by Corollary 23.5.18(a). We will see that if Y is locally Noetherian, the last condition (iii) is a concequence of the others, and conditions (i) and (ii) characterize projective morphisms. If Y is Noetherian, we can further repalce in (ii) that there exists a *ample* $\mathscr{O}_X$-module relative to f (Proposition 23.4.42). We also note that there are proper morphisms that is not projective.

Remark 23.5.8. Let Y be a quasi-compact scheme such that there exists an ample $\mathscr{O}_Y$-module. For a Y-scheme X to be projective, it is necessary and sufficient that it is isomorphic to a closed subscheme of a projective bundle of the form $\mathbb{P}^r_Y$. This conditions is clearly sufficient. Conversely, if X is projective over Y, it is quasi-projective, so there exists a Y-immersion $j : X \to \mathbb{P}^r_Y$ by Corollary 23.5.14, which is closed by Corollary 23.5.18(a) and Theorem 23.5.24.

Remark 23.5.9. The reasoning of Theorem 23.5.24 shows that for any scheme Y, and any integer $r \geq 0$, the structural morphism $\mathbb{P}^r_Y \to Y$ is surjective, because if we put $\mathscr{S}_{\mathscr{O}_Y} = \boldsymbol{S}(\mathscr{O}_Y^{r+1})$, we have evidently $\mathscr{S}_y = \boldsymbol{S}_{\kappa(y)}(\kappa(y)^{r+1})$, so $(\mathscr{S}_n)_y \neq 0$ for any $y \in Y$ and $n \geq 0$.

Proposition 23.5.25 (Properties of Projective Morphisms).

(i) A closed immersion is projective.

(ii) If $f : X \to Y$ and $g : Y \to Z$ are projective morphisms and if Z is quasi-compact and quasi-separated, then $g \circ f$ is projective.

(iii) If $f : X \to Y$ is a projective morphism, $f_{(S')} : X_{(S')} \to Y_{(S')}$ is projective for any base change $S' \to S$.

(iv) If $f : X \to Y$ and $g : X' \to Y'$ are projective S-morphisms, so is $f \times_S g$.

(v) If $g \circ f$ is a projective morphism and if g is separated, f is projective.

(vi) If f is projective, so is f_{red}.

Proof. Property (i) follows from Corollary 23.3.5. It is necessary here to prove (iii) and (iv) separately, because of the restriction introduced on Z in (ii). To prove (iii), we can reduce to the case where $S = Y$ (Corollary 22.3.8) and the assertion then follows immediately from Proposition 23.5.23(b) and from Proposition 23.3.28. To prove (iv), we can assume that $X = \mathbb{P}(\mathscr{E})$, $X' = \mathbb{P}(\mathscr{E}')$, where $\mathscr{E}$ (resp. $\mathscr{E}'$) is a quasi-coherent $\mathscr{O}_Y$-module of finite type. Let p, p' be the projection of $T = Y \times_S Y'$ to Y and Y' respectively; by (4.1.1), we have $\mathbb{P}(p^*(\mathscr{E})) = \mathbb{P}(\mathscr{E}) \times_Y T$ and $\mathbb{P}(p'^*(\mathscr{E})) = \mathbb{P}(\mathscr{E}') \times_{Y'} T$, whence

$$\begin{aligned}\mathbb{P}(p^*(\mathscr{E})) \times_T \mathbb{P}(p'^*(\mathscr{E}')) &= (\mathbb{P}(\mathscr{E}) \times_Y T) \times_T (T \times_{Y'} \mathbb{P}(\mathscr{E}')) = \mathbb{P}(\mathscr{E}) \times_Y (T \times_{Y'} \mathbb{P}(\mathscr{E}')) \\ &= \mathbb{P}(\mathscr{E}) \times_Y ((Y \times_S Y') \times_{Y'} \mathbb{P}(\mathscr{E}')) = \mathbb{P}(\mathscr{E}) \times_S \mathbb{P}(\mathscr{E}').\end{aligned}$$

Now $p^*(\mathscr{E})$ and $p'^*(\mathscr{E}')$ are of finite type over T (Proposition 19.4.5), and so is $p^*(\mathscr{E}) \otimes_{\mathscr{O}_T} p'^*(\mathscr{E}')$; as $\mathbb{P}(p^*(\mathscr{E})) \times_T \mathbb{P}(p'^*(\mathscr{E}'))$ is identified with a closed subscheme of $\mathbb{P}(p^*(\mathscr{E}) \otimes_{\mathscr{O}_T} p'^*(\mathscr{E}'))$ (Proposition 23.4.10), this proves (iv). For (v) and (vi), we can apply Proposition 22.5.22, since any closed subscheme of a projective Y-scheme is projective by Proposition 23.5.23(a). □

Proposition 23.5.26. *If X and X' are two projective Y-schemes, so is $X \amalg X'$.*

Proof. This is evident from Remark 23.4.3. □

Proposition 23.5.27. *Let X be a projective Y-scheme, $\mathscr{L}$ be a Y-ample $\mathscr{O}_Y$-module. For any section f of $\mathscr{L}$ over X, X_f is affine over Y.*

Proof. Since the question is local over Y, we can assume that $Y = \operatorname{Spec}(A)$ is affine; since $X_{f^{\otimes n}} = X_f$, by replacing $\mathscr{L}$ by $\mathscr{L}^{\otimes n}$ we can assume that $\mathscr{L}$ is very ample for the structural morphism $q : X \to Y$ (Proposition 23.4.29). The canonical homomorphism $\sigma : q^*(q_*(\mathscr{L})) \to \mathscr{L}$ is then surjective and the corresponding morphism

$$r = r_{\mathscr{L},\sigma} : X \to P = \mathbb{P}(q_*(\mathscr{L}))$$

is an immersion such that $\mathscr{L} \cong r^*(\mathscr{O}_P(1))$ (Proposition 23.4.13). Moreover, as X is proper over Y, the immersion r is closed by Corollary 23.5.18. By definition $f \in \Gamma(Y, q_*(\mathscr{L}))$ and $\sigma^\flat$ is the identity of $q_*(\mathscr{L})$; it then follows from the formula (3.6.2) that we have $X_f = r^{-1}(D_+(f))$. Then X_f is a closed subscheme of the affine scheme $D_+(f)$, and therefore is affine. □

If we take $Y = X$ in Proposition 23.5.27, we obtain that, for any scheme X and any invertible $\mathscr{O}_X$-module $\mathscr{L}$, the open subset X_f is affine over X.

23.5.6 Chow's lemma

Theorem 23.5.28 (Chow's lemma). *Let X be a separated S-scheme of finite type and suppose that one of the following conditions is satisfied:*

(a) S is Noetherian.

(b) S is quasi-compact and X has finitely many irreducible components.

Then there exists a quasi-projective S-scheme X' and a surjective projective S-morphism $f : X' \to X$ that induces an isomorphism an isomorphism $f^{-1}(U) \cong U$ for some open dense subset of X. If X is reduced (resp. irreducible), we can also choose X' to be reduced (resp. irreducible).

Proof. The proof is divided into several steps. First of all, we can assume that X is irreducible. To see this, we note that in both cases the scheme X has finitely many irreducible components X_i. If the theorem is demonstrated for each reduced subscheme X_i, and if $f_i : X'_i : X_i$ is the corresponding hommorphism which induces an isomorphism $f_i^{-1}(U_i) \cong U_i$ with $U_i \subseteq X_i$, the sum $X' = \coprod_i X'_i$ is then quasi-projective over S (Corollary 23.5.16 and Proposition 23.5.15) and the morphism $f : X' \to X$ whose restriction on X'_i equals to $j_i \circ f_i$ (where $j_i : X_i \to X$ is the canonical injection), is then surjective and projective (Proposition 23.5.26); it is immediate to see that X' is reduced if each X'_i is. We now choose U to be the union of $U_i \cap (\bigcup_{j\neq i} X_j)^c$; since U_i is dense in X_i and X_i is maximal irreducible, we conclude that each $U_i \cap (\bigcup_{j\neq i} X_j)$ is nonempty. The open subset U is then dense in X and f clearly induces an isomorphism $f^{-1}(U) \cong U$.

So suppose now that X is irreducible. As the structural morphism $\eta : X \to S$ is of finite type, there exists a finite covering (S_i) of S by affine opens, and for each i there is a finite covering (T_{ij}) of $\eta^{-1}(S_i)$ by affine opens, with the morphism $T_{ij} \to S_i$ being affine and of finite type, hence quasi-projective (Proposition 23.5.15(i)). As in both hypotheses the immersion

$S_i \to S$ is quasi-compact, it is quasi-projective by Proposition 23.5.15(i), so the restriction of η to T_{ij} is quasi-projective (Proposition 23.5.15(ii)). We relabel the T_{ij} by U_k with $1 \leq k \leq n$. There exists, for each index k, an open immersion $\varphi_k : U_k \to P_k$, where P_k is projective over S (Proposition 23.5.13). Let $U = \bigcap_k U_k$; as X is irreducible and the U_k is nonempty, U is nonempty, and therefore is dense in X; the restrictions of φ_k to U together define a morphism

$$\varphi : U \to P = P_1 \times_S P_2 \times_S \cdots \times_S P_n$$

which fits into the diagram

$$\begin{tikzcd} U \arrow[r, "\varphi"] \arrow[d, "j_k"'] & P \arrow[d, "p_k"] \\ U_k \arrow[r, "\varphi_k"] & P_k \end{tikzcd} \tag{5.6.1}$$

where j_k is the canonical injection and p_k is the canonical projection. If $j : U \to X$ is the canonical injection, the morphism $\psi = (j, \varphi)_S : U \to X \times_S P$ is then an immersion by Corollary 22.5.16. Under the hypotheses of (a), $X \times_S P$ is locally Noetherian (Proposition 23.3.21 and Corollary 22.6.22), and under the hypotheses of (b), $X \times_S P$ is quasi-compact. In both cases the scheme-theoretic image X' of ψ in $X \times_S P$ exists (which is the closure of $\psi(U)$ in $X \times_S P$) and ψ factors into

$$\psi : U \xrightarrow{\psi'} X' \xrightarrow{h} X \times_S P$$

where ψ' is a dominant open immersion and h is a closed immersion. Let $q_1 : X \times_S P \to X$ and $q_2 : X \times_P \to P$ be the canonical projections; we put

$$f : X' \xrightarrow{h} X \times_S P \xrightarrow{q_1} X, \quad g : X' \xrightarrow{h} X \times_S P \xrightarrow{q_2} P. \tag{5.6.2}$$

We shall verify that the scheme X' and the morphism f satisfy the requirements. First we show that f is projective and surjective, and that the restriction of $U' = f^{-1}(U)$ is an isomorphism from U' to U. As the P_k are projective over S, so is P (Proposition 23.5.25(iv)), and $X \times_S P$ is projective over X by Proposition 23.5.25(iii); then X' is also projective over X, since it is a closed subscheme of $X \times_S P$. On the other hand, we have $f \circ \psi' = q_1 \circ (h \circ \psi') = q_1 \circ \psi = j$, so $f(X')$ contains the dense open subset U of X; but f is proper by Theorem 23.5.24, so $f(X') = X$. Now $q_1^{-1}(U) = U \times_S P$ is an open subscheme of $X \times_S P$, and the the immersion ψ factors into

$$\psi : U \xrightarrow{\Gamma_\varphi} U \times_S P \xrightarrow{j \times 1} X \times_S P.$$

By Proposition 22.6.67, $U' = h^{-1}(U \times_S P)$ is the scheme-theoretic image of $\psi^{-1}(U \times_S P) = U$ under $\psi_U : U \to U \times_S P$, and therefore the closure of the image of Γ_φ in $U \times_S P$. As P is separted over S, Γ_φ is a closed immersion (Corollary 22.5.19), so we conclude that $U' = \psi(U)$. As ψ is an immersion, the restriction of f to U' is then an isomorphism, with inverse ψ'. Finally, by definition, $U' = \psi(U) = \psi'(U)$ is open and dense in X'.

We now show that g is an immersion, which implies that X' is quasi-projective over S, since P is projective over S. Let $V_k = \varphi_k(U_k)$ be the image of U_k in P_k, $W_k = p_k^{-1}(V_k)$ be the inverse image in P, and put $U'_k = f^{-1}(U_k)$, $U''_k = g^{-1}(W_k)$. Since the U_k cover X, it clear that the U'_k form an open covering of X'; we first shows that this is also ture for the U''_k, by proving that

$U'_k \subseteq U''_k$. For this, it suffices to estabilsh the commutativity of the diagram

$$\begin{tikzcd} U'_k \arrow[r, "g|_{U'_k}"] \arrow[d, "f|_{U'_k}"'] & P \arrow[d, "p_k"] \\ U_k \arrow[r, "\varphi_k"] & P_k \end{tikzcd} \tag{5.6.3}$$

Since $U'_k = h^{-1}(U_k \times_S P)$ and $\psi^{-1}(U_k \times_S P) = U$, by Proposition 22.6.67 U'_k is the scheme-theoretic image of U in $U_k \times_S P$ under the morphism $\psi_k : U \to U_k \times_S P$ induced by ψ. It then suffices to prove the commutativity of the diagram obtained by composing (5.6.3) with the morphism ψ_k (Corollary 22.6.65), and this comes from the commutative diagram (5.6.1).

The W_k then form an open covering of $g(X')$, so to show that g is an immersion, it suffices to show the restriction $g|_{U''_k}$ is an immersion into W_k (Corollary 22.4.10). For this, consider the morphism

$$u_k : W_k \xrightarrow{p_k} V_k \xrightarrow{\varphi_k^{-1}} U_k \to X$$

which fits into the following commutative diagram

$$\begin{tikzcd} U' \arrow[r, hook] \arrow[dr] & U'_k \arrow[r, hook] \arrow[dr] & U''_k \arrow[r, hook, "h|_{U''_k}"] \arrow[dr, "f|_{U''_k}"] \arrow[rr, bend left, "g|_{U''_k}"] & X \times_S W_k \arrow[r, "q_2"] \arrow[d, "q_1"] & W_k \arrow[l, bend right, "\Gamma_{u_k}"'] \arrow[dl, "u_k"] \arrow[d, "p_k"] \\ & U \arrow[r, hook] & U_k \arrow[r, hook] \arrow[rr, bend right, "\cong", "\varphi_k"'] & X & V_k \end{tikzcd}$$

By the definition of g (formula (5.6.2)), we have $U''_k = h^{-1}(X \times_S W_k) \subseteq X'$ and $\psi^{-1}(X \times_S W_k) = U$, so by Proposition 22.6.67, U''_k is the scheme-theoretic image of U under the morphism $U \to X \times_S W_k$ induced by ψ; since $U' = \psi(U)$, it is therefore dense in U''_k. On the other hand, as X is separted over S, the graph morphism $\Gamma_{u_k} : W_k \to X \times_S W_k$ is a closed immersion, so the graph $T_k = \Gamma_{u_k}(W_k)$ is a closed subscheme of $X \times_S W_k$. If we can prove that T_k dominates the canonical image of the open subscheme U' in $X \times_S W_k$, it will then dominates the subscheme U''_k. As the restriction of q_2 to T_k is an isomorphism onto W_k and h is a closed immersion, the restriction of g to X''_k will then be an immersion in W_k, and our assertion will be proved. For this, we let $v_k : U' \to X \times_S W_k$ be the canonical injection, and $w_k = q_2 \circ v_k$; then from the definition of Γ_{u_k} we have $v_k = \Gamma_{u_k} \circ w_k$, and the image of U' in $X \times_S W_k$ is therefore contained in T_k, verifying our claim.

It is clear that U, and therefore U', are irreducible, and so is X' by our construction, and that f is birational. If X is reduced, so is U', and X' is then reduced (Proposition 22.6.66). This completes the proof. □

Corollary 23.5.29. *Suppose the hypotheses of Theorem 23.5.28. For X to be proper over S, it is necessary and sufficient that there exists a projective S-scheme X' and a surjective S-morphism $f : X' \to X$ (which is projective by Proposition 23.5.25(v)). If this is the case, we can choose an open dense subset*

U of X such that f induces an isomorphism $f^{-1}(U) \cong U$ and that $f^{-1}(U)$ is dense in X'. If X is irreducible (resp. reduced), we can choose X' to be irreducible (resp. reduced). If X and X' are irreducible, f is then a birational morphism.

Proof. The conditions is sufficient by Theorem 23.5.24 and Corollary 23.5.18(b). This is necessary because with the notations of Theorem 23.5.28, if X is proper over S, X' is then proper over S (since it is proper over X by Theorem 23.5.24), and our assertion follows from Proposition 23.5.17(ii). Moreover, as X' is quasi-projective over S, it is projective over S in view of Theorem 23.5.24. □

Corollary 23.5.30. *Let S be a locally Noetherian scheme, X be an S-scheme of finite type, and $\varphi : X \to S$ be the structural morphism. For X to be proper over S, it is necessary and sufficient that for any morphism of finite type $S' \to S$, the morphism $\varphi_{(S')} : X_{(S')} \to S'$ is closed. Moreover, it suffices to verify this condition for any S-scheme of the form $S' = S \otimes_{\mathbb{Z}} \mathbb{Z}[T_1, \dots, T_n]$.*

Proof. The conditions is clearly necessary, and we now prove the sufficiency. The question is local over S and S', so we may assume that S, S' are affine and Noetherian. By Chow's lemma, there exists a projective S-scheme P, an immersion $j : X' \to P$, and a projective surjective morphism $f : X' \to X$ such that the diagram

$$\begin{tikzcd}
X' \arrow[dr, "\psi"] \arrow[drr, bend left, "f"] \arrow[ddr, bend right, "j"'] & & \\
& X \times_S P \arrow[r, "q_1"] \arrow[d, "q_2"'] & X \arrow[d, "\varphi"] \\
& P \arrow[r, "r"] & S
\end{tikzcd}$$

is commutative; let $\psi = (f, j)_S$. As P is of finite type over S, the projection $q_2 : X \times_S P \to P$ is a closed morphism by hypotheses. On the other hand, since f is projective and the projection $q_1 : X \times_S P \to X$ is separated (since P is separated over S), we conclude from Proposition 23.5.25(v) that ψ is projective, hence closed. Since the immersion j is the composition of q_2 with ψ, it is therefore a closed immersion, whence proper. Moreover, the structural morphism $r : P \to S$ is projective, hence proper (Theorem 23.5.24), so $\varphi \circ f = r \circ j$ is proper. As f is surjective, we conclude by Corollary 23.5.18(b) that φ is proper.

To estabilsh the second assertion of the proposition, it suffices to prove that it implies that $\varphi_{(S')}$ is closed for any morphism $S' \to S$ of finite type. Now if S' is affine and of finite type over $S = \operatorname{Spec}(A)$, we have $S' = \operatorname{Spec}(A[x_1, \dots, x_n])$, and S' is then isomorphic to a closed subscheme of $S'' = \operatorname{Spec}(A[T_1, \dots, T_n])$ (where T_i are indeterminates). In the following commutative diagram

$$\begin{tikzcd}
X \times_S S' \arrow[r, "1_X \times j"] \arrow[d, "\varphi_{(S'')}"'] & X \times_S S'' \arrow[d, "\varphi_{(S'')}"] \\
S' \arrow[r, "j"] & S''
\end{tikzcd}$$

where j and $q_X \times j$ are closed immersions (Corollary 22.4.12) and $\varphi_{(S'')}$ is closed by hypothesis. We then conclude that $\varphi_{(S')}$ is closed, whence the claim. □

23.6 Integral morphisms and finite morphisms

23.6.1 Integral and finite morphisms

Let X be an S-scheme and $f : X \to S$ be the structural morphism. We say that X is **integral over S**, or that f is an **integral morphism**, if there exists an affine open covering (S_α) of S such that for each α, the open subscheme $f^{-1}(S_\alpha)$ of X is affine and its ring $B_\aleph$ is an integral algebra over the ring A_α of S_α. We say that X is **finite over** S, or that f is a **finite morphism**, if X is integral and of finite type over S. If S is affine with ring A, we also say that X is inegral or finite over A.

It is clear that any integral S-scheme is affine over S. Conversely, form the definition of integral morphisms, we see that for an affine S-scheme X to be integral over S (resp. finite), it is necessary and sufficient that the associated quasi-coherent $\mathscr{O}_S$-algebra $\mathscr{A}(X)$ is such that there exists an affine open covering (S_α) of S such that for each α, $\Gamma(S_\alpha, \mathscr{A}(X))$ is an integral algebra (resp. an integral algebra of finite type) over $\Gamma(S_\alpha, \mathscr{O}_S)$. A quasi-coherent $\mathscr{O}_S$-algebra satisfying this property is said to be **integral** (resp. **finite**) over $\mathscr{O}_S$. We note that a quasi-coherent $\mathscr{O}_S$-algebra $\mathscr{B}$ is finite if and only if it is an $\mathscr{O}_S$-module of finite type; it amounts to the same thing to say that $\mathscr{B}$ is an integral $\mathscr{O}_S$-algebra of finite type, because an integer algebra of finite type over a ring A is an A-module of finite type.

Proposition 23.6.1. *Let S be a locally Noetherian scheme. For an S-scheme X affine over S to be finite over S, it is necessary and sufficient that the $\mathscr{O}_S$-algebra $\mathscr{A}(X)$ is coherent.*

Proof. With the preceding remark, this follows from the fact that if S is locally Noetherian, then a quasi-coherent $\mathscr{O}_S$-module is of finite type if and only if it is coherent (Theorem 22.1.29). □

Proposition 23.6.2. *Let X be an integral (resp. finite) scheme over S with $f : X \to S$ the structural morphism. Then for any affine open subset $U \subseteq S$ with ring A, $f^{-1}(U)$ is affine and its ring B is an integral (resp. finite) algebra over A.*

Proof. To prove this proposition, we need Proposition 10.4.51. We now that $f^{-1}(U)$ is affine by Proposition 23.1.3. If $\varphi : A \to B$ is the corresponding homomorphism, there exists a finite covering of U by open subsets $D(g_i)$ ($g_i \in A$) such that, if $h_i = \varphi(g_i)$, then B_{h_i} is an integral (resp. finite) algebra over A_{g_i}. In fact, by assumption, there is a covering of U by affine open subsets $V_\alpha \subseteq U$ such that if $A_\alpha = \Gamma(V_\alpha, \mathscr{O}_S)$ and $B_\alpha = \Gamma(f^{-1}(V_\alpha), \mathscr{O}_X)$, then B_α is an integral (resp. finite) algebra over A_α. Any $x \in U$ belongs to one V_α, so there exists $g \in A$ such that $x \in D(g) \subseteq V_\alpha$. If g_α is the image of g in A_α, we have $\Gamma(D(g), \mathscr{O}_S) = A_g = (A_\alpha)_{g_\alpha}$; let $h = \varphi(g)$, and let h_α be the image of g_α in B_α. We have

$$\Gamma(D(h), \mathscr{O}_S) = B_h = (B_\alpha)_{h_\alpha}$$

and as B_α is integral over A_α, $(B_\alpha)_{h_\alpha}$ is integral (resp. finite) over $(A_\alpha)_{g_\alpha}$. Since U is quasi-compact, we obtain a finite cover.

If we suppose first that each B_{h_i} is a finite algebra over A_{g_i}, then as an A_{g_i}-module, B_{h_i} is finitely generated, so Proposition 10.4.51 shows that B is a finitely generated A-module. Now assume that each B_{h_i} is integral over A_{g_i}; let $b \in B$, and let C be a sub-A-algebra of B generated by b. For each i, C_{h_i} is the A_{g_i}-algebra generated by $b/1$ over B_{h_i}. It then follows from the

hypothesis that each C_{h_i} is finitely generated A_{g_i}-module, so by Proposition 10.4.51 C is a finitely generated A-module. This shows that B is integral over A. □

Proposition 23.6.3 (Properties of Integral and Finite morphisms).

(i) A closed immersion is finite (and a fortiori integral).

(ii) The composition of two integral morphisms (resp. finite) is integral (resp. finite).

(iii) If $f : X \to Y$ is an integral (resp. finite) S-morphism, $f_{(S')} : X_{(S')} \to Y_{(S')}$ is integral (resp. finite) for any base change $S' \to S$.

(iv) If $f : X \to Y$ and $g : X' \to Y'$ are two integral (resp. finite) S-morphisms, so is $f \times_S g$.

(v) If $f : X \to Y$ and $g : Y \to Z$ are two morphisms such that $g \circ f$ is integral (resp. finite) and g is separated, then f is integral (resp. finite).

(vi) If $f : X \to Y$ is an integral (resp. finite) morphism, so is f_{red}.

Proof. In view of Proposition 22.5.22, it suffices to prove (i), (ii), and (iii). To prove that a closed immersion $X \to S$ is finite, we can assume that $S = \mathrm{Spec}(A)$, and this then follows from the fact that a quotient ring $A/\mathfrak{a}$ is a finitely generated A-module. To prove the composition of two integral (resp. finite) morphisms $X \to Y$, $Y \to Z$ is integral (finite), we can assume that Z (and therefore X and Y) is affine, and the assertion is then equivalent to that if B is an integral (resp. finite) A-algebra and C is an integral (resp. finite) B-algebra, then C is an integral (resp. finite) A-algebra, which is immediate. Finally, to prove (iii), we can Simialrly assume that $S = \mathrm{Spec}(A)$, $S' = \mathrm{Spec}(A')$; then X is affine with ring B (Proposition 23.6.2), $X_{(S')}$ is affine with ring $A' \otimes_A B$, and it suffices to note that if B is an integral (resp. finite) A-algebra, then $A' \otimes_A B$ is an integral (resp. finite) A'-algebra. □

Note also that if X and Y are two integral (resp. finite) S-schemes, the sum $X \amalg Y$ is an integral (resp. finite) over S, because a product of two integral (resp. finite) A-algebras is still integral (resp. finite).

Corollary 23.6.4. *If X is an integral (resp. finite) scheme over S, then for any open subset $U \subseteq S$, $f^{-1}(U)$ is integral (resp. finite) over U.*

Proof. This is a particular case of Proposition 23.6.3(iii). □

Corollary 23.6.5. *Let $f : X \to Y$ be a finite morphism. Then for any $y \in Y$, the fiber $f^{-1}(y)$ is a finite algebraic scheme over $\kappa(y)$, and a fortiori with discrete and finite underlying space.*

Proof. The $\kappa(y)$-scheme $f^{-1}(y)$ is identified with $X \times_Y \mathrm{Spec}(\kappa(y))$, so is finite over $\kappa(y)$ by Proposition 23.6.3(iii). This is then an affine scheme whose ring is a finite dimensional $\kappa(y)$-algebra, so is Artinian. The proposition then follows from Proposition 22.2.30. □

Corollary 23.6.6. *Let X and S be integral schemes and $f : X \to S$ be a dominant morphism. If f is integral (resp. finite), then the rational function field $K(X)$ of X is an algebraic (resp. finite) extension of $K(S)$.*

Proof. Let s be the generic point of S; the $\kappa(s)$-scheme $f^{-1}(s)$ is integral (resp. finite) over $\operatorname{Spec}(\kappa(s))$ by Proposition 23.6.3(iii), and contains by hypothesis the generic point of x of X; the local ring of $f^{-1}(s)$ at x, equal to $\kappa(x)$ (Proposition 22.3.34), is a localization of an integral (resp. finite) algebra over $\kappa(s)$, whence the corollary. □

Proposition 23.6.7. *Any integral morphism is universally closed.*

Proof. Let $f : X \to Y$ be an integral morphism. In view of Proposition 23.6.3(iii), it suffices to prove that f is closed. Let Z be a closed subset of X. In view of Proposition 23.6.3(vi), we can suppose that X and Y are reduced; moreover, if T is the reduced closed subscheme of Y with underlying space $\overline{f(X)}$, we see that f factors into

$$f : X \xrightarrow{g} T \xrightarrow{j} Y,$$

where $j : T \to Y$ is the canonical injection, and as j is separated, it follows from Proposition 23.6.3(v) that g is an integral morphism. We can then assume that $f(X)$ is dense in Y, and prove that $f(X) = Y$. Since the question is local over Y, we can assume that $Y = \operatorname{Spec}(A)$ is affine, so $X = \operatorname{Spec}(B)$ where B is an integral algebra over A (Proposition 23.6.2); moreover A is reduced and the hypothesis that $f(X)$ is dense in Y implies that the corresponding homomorphism $\varphi : A \to B$ is injective (Corollary 10.4.19). The condition that $f(X) = Y$ then follows from Theorem 13.1.67. □

Remark 23.6.1. The hypothesis that g is separated is essential for the validity of Proposition 23.6.3(v): in fact, if Y is not separated over Z, the identity 1_Y is the composition morphism

$$Y \xrightarrow{\Delta_Y} Y \times_Z Y \xrightarrow{p_1} Y$$

but Δ_Y is not integral, since it is not closed (Proposition 23.6.7).

Corollary 23.6.8. *Any finite morphism $f : X \to Y$ is projective.*

Proof. As f is affine, $\mathscr{O}_X$ is a very ample $\mathscr{O}_X$-module relative to f; moreover $f_*(\mathscr{O}_X)$ is a quasi-coherent $\mathscr{O}_Y$-algebra of finite type by hypothesis. Finally, f is separated, of finite type, and universally closed (Proposition 23.6.7), and we then have the conditions of Remark 23.5.7. □

Lemma 23.6.9. *Let Y be a scheme, $\mathscr{E}$ be a locally free $\mathscr{O}_Y$-module of rank r, and Z be a finite subset of Y contained in an affine open subset V. Then there exists an open neighborhood $U \subseteq V$ of Z such that $\mathscr{E}|_U$ is isomorphic to $\mathscr{O}_Y^r|_U$.*

Proof. □

Proposition 23.6.10. *Let $f : X' \to X$ be a finite morphism, and let $\mathscr{B} = f_*(\mathscr{O}_{X'})$ (which is a quasi-coherent finite $\mathscr{O}_X$-algebra). Let $\mathscr{F}'$ be a quasi-coherent $\mathscr{O}_{X'}$-module; for $\mathscr{F}'$ to be locally free of rank r, it is necessary and sufficient that $f_*(\mathscr{F}')$ is a locally free $\mathscr{B}$-module of rank r.*

Proof. It is clear that if $f_*(\mathscr{F}')|_U$ is isomorphic to $\mathscr{B}^r|_U$ (where U is open in X), $\mathscr{F}'|_{f^{-1}(U)}$ is isomorphic to $\mathscr{O}_{X'}^r|_{f^{-1}(U)}$ (Corollary 23.1.17). Conversely, suppose that $\mathscr{F}'$ is locally free of rank r and we prove that $f_*(\mathscr{F}')$ is locally isomorphic to $\mathscr{B}^r$ as $\mathscr{B}$-modules. Let x be a point of X; if

U runs through affine neighborhoods of x, $f^{-1}(U)$ form a fundamental system of affine neighborhoods (Proposition 23.1.3) of the finite subset $f^{-1}(x)$, since f is closed (Proposition 23.6.7). The proposition then follows from Lemma 23.6.9. □

Proposition 23.6.11. *Let $g : X' \to X$ be an integral morphism of schemes, Y be a locally integral and normal scheme, f be a rational map from Y to X' such that $g \circ f$ is a everywhere defined rational map; then f is everywhere defined.*

Proof. Recall that we say a scheme X is normal if it is normal as a ringed space, which means the stalk $\mathcal{O}_{X,x}$ is an integrally closed domain for every $x \in X$. If f_1 and f_2 are two morphisms (densely defined from Y to X') in the class of f, it is clear that $g \circ f_1$ and $g \circ f_2$ are equivalent morphisms, which justifies the notation $g \circ f$ for their equivalent class. We recall also that if Y is locally Noetherian, then the hypothesis on Y implies that Y is locally integral (Proposition 22.4.32).

To prove the proposition, we first note that the question is local over Y and we can assume that there exists a morphism $h : Y \to X$ in the class of $g \circ f$. Consider the inverse image $Y' = X'_{(h)} = X'_{(Y)}$, and note that the morphism $g' = g_{(Y)} : Y' \to Y$ is integral by Proposition 23.6.3(iii). Via the correspondence of rational maps from Y to X' with rational Y-sections of Y', we see that we are reduced to the case $X = Y$. □

Corollary 23.6.12. *Let X be a locally integral and normal scheme, $g : X' \to X$ be an integral morphism, and f be a rational X-section of X'. Then f is everywhere defined.*

Proof. □

Corollary 23.6.13. *Let X be a normal and integral scheme, X' be an integral scheme, and $g : X' \to X$ be an integral morphism. If there exists a rational X-section f of X', g is an isomorphism.*

23.6.2 Quasi-finite morphisms

Proposition 23.6.14. *Let $f : X \to Y$ be a morphism locally of finite type, x be a point of X and $y = f(x)$. The following conditions are equivalent:*

(i) The point x is isolated in the fiber X_y.

(ii) The point x is closed in X_y and there is no generalization of x in X_y.

(iii) The $\mathcal{O}_{Y,y}$-module $\mathcal{O}_{X,x}$ is quasi-finite.

Proof. The question is local over X and Y, so we can suppose that $X = \operatorname{Spec}(B)$ and $Y = \operatorname{Spec}(A)$ are affine, where B is finite A-algebra. Moreover, we can replace X by $X \times_Y \operatorname{Spec}(\mathcal{O}_{Y,y})$ without changing the fiber X_y and the local ring $\mathcal{O}_{X,x}$ (Proposition 22.3.34). We can then suppose that A is a local ring with maximal ideal $\mathfrak{m}$ (which equals to the local ring $\mathcal{O}_{Y,y}$). The fiber X_y is then the affine sheme of the ring $B/\mathfrak{m}B$, of finite type over $\kappa(y) = A/\mathfrak{m}$ (Proposition 22.6.47). Let $\mathfrak{P}$ be the prime ideal of B corresponding to x.

We note that the fiber $X_y = X \times_Y \operatorname{Spec}(\kappa(y)) = \operatorname{Spec}(B \otimes_A \kappa(y))$ is Jacobson. If (ii) is satisfied, then $\{x\}$ is an open subset of X_y, hence contains a closed point (by the Jacobson property) which must be x, and x is therefore closed in X_y. Also, since $\{x\}$ is open in X_y, it is clear that there is no further generalization x' of x (which means $x \in \overline{\{x'\}}$) in X_y; this proves (ii).

We now consider the condition in (ii). Consider the ring $\overline{B} = B \otimes_A \kappa(y) = B/\mathfrak{m}B$ and let $\overline{\mathfrak{P}}$ be the prime ideal corresponding to $\mathfrak{P}$. If x is closed in X_y, we see that $\overline{\mathfrak{P}}$ is maximal in $\overline{B}$ and by condition (ii) there is no prime ideal of $\overline{B}$ contained in $\overline{\mathfrak{P}}$. This shows that $\overline{B}_{\overline{\mathfrak{P}}}$ is Artinian, so we conclude that the ring homomorphism $A \to B$ is quasi-finite at $\mathfrak{P}$; that is, the $\mathcal{O}_{Y,y}$-module $\mathcal{O}_{X,x}$ is quasi-finite. Conversely, if $\overline{B}_{\overline{\mathfrak{P}}}$ is Artinian, then $\overline{\mathfrak{P}}$ is maximal and there is no prime ideal of $\overline{B}$ contained in $\overline{\mathfrak{P}}$; we then conclude that x is closed in X_y and there is no generalization of x in X_y. This shows that (ii)$\Leftrightarrow$(iii).

We finally prove that (ii) implies (i). If (ii) is satisfied, then the prime ideal $\mathfrak{P}$ is maximal and minimal in B since $\overline{B}_{\overline{\mathfrak{P}}}$ is Artinian. Let $\overline{\mathfrak{P}}_1 = \overline{\mathfrak{P}}, \overline{\mathfrak{P}}_2, \dots, \overline{\mathfrak{P}}_r$ be the minimal prime ideals of $\overline{B}$. Then the intersection $\bigcap_{i=1}^r \overline{\mathfrak{P}}_i$ is equal to the nilradical of $\overline{B}$, and $\bigcap_{i=2}^r \overline{\mathfrak{P}}_i$ is contained in this intersection in view of Proposition 10.1.5, so there exists an element $\overline{b} \in \bigcap_{i=2}^r \overline{\mathfrak{P}}_i$ that is not nilpotent. The open subset $D_{\overline{B}}(\overline{b})$ of $X_y = \operatorname{Spec}(\overline{B})$ then reduces to $\{x\}$, which shows that x is isolated. □

Corollary 23.6.15. *Let $f : X \to Y$ be a morphism of finite type. Then the following conditions are equivalent:*

(i) Any point $x \in X$ is isolated in the fiber $X_{f(x)}$ (that is, $X_{f(x)}$ is discrete).

(ii) For any $x \in X$, $X_{f(x)}$ is a finite $\kappa(f(x))$-scheme.

(iii) For any $x \in X$, the $\mathcal{O}_{Y,y}$-module $\mathcal{O}_{X,x}$ is quasi-finite.

Proof. The equivalence of (i) and (iii) follows from Proposition 23.6.14. On the other hand, as $X_{f(x)}$ is an algebraic $\kappa(f(x))$-scheme, the equivalence of (i) and (ii) follows from Proposition 22.6.43. □

We say a morphism $f : X \to Y$ of finite type is **quasi-finite**, or X is quasi-finite over Y, if it satisfies the equivalent conditions of Corollary 23.6.15. From Corollary 23.6.5, it is clear that any finite morphism is quasi-finite.

Proposition 23.6.16 (Properties of Quasi-finite Morphisms).

(i) Any quasi-compact immersion (in particular any closed immersion) is quasi-finite.

(ii) If $f : X \to Y$ and $g : Y \to Z$ are quasi-finite morphisms, $g \circ f$ is quasi-finite.

(iii) If $f : X \to Y$ is a quasi-finite S-morphism, $f_{(S')} : X_{(S')} \to Y_{(S')}$ is quasi-finite for any base change $S' \to S$.

(iv) If $f : X \to Y$ and $g : X' \to Y'$ are quasi-finite S-morphisms, $f \times_S g$ is quasi-finite.

(v) Let $f : X \to Y$ and $g : Y \to Z$ be two morphisms such that $g \circ f$ is quasi-finite; then, if g is separated, or X is Noetherian, or $X \times_Z Y$ is locally Noetherian, then f is quasi-finite.

(vi) If f is quasi-finite, so is f_{red}.

Proof. If $f : X \to Y$ is an immersion, any fiber is reduced to a singleton, so (i) follows from Proposition 22.6.35(i). For (ii), we note that $h = g \circ f$ is of finite type by Proposition 22.6.35(ii); if $z = h(x)$ and $y = f(x)$, y is isolated in $g^{-1}(z)$, so there exists an open neighborhood V of y in Y not containing other points of $g^{-1}(z)$; $f^{-1}(V)$ is then an open neighborhood of x not

containing other points of $f^{-1}(y')$, where $y' \neq y$ is in $g^{-1}(z)$, and therefore not containing points $x' \neq x$ in $h^{-1}(z)$ that is not in $f^{-1}(y)$. As x is isolated in $f^{-1}(y)$ by hypothesis, it is then isolated in $h^{-1}(z) = f^{-1}(g^{-1}(z))$. As for (iii), we can limit ourselves to the case where $Y = S$ (Corollary 22.3.8); we first note that $f' = f_{(S')}$ is of finite type (Proposition 22.6.35(iii)). On the other hand, if $x' \in X' = X_{(S')}$ and $y' = f'(x')$, $X'_{y'}$ is identified with $X_y \otimes_{\kappa(y)} \kappa(y')$ by Proposition 22.3.35. As X_y is of finite dimension over $\kappa(y)$ by hypothesis, $X'_{y'}$ is of finite dimension over $\kappa(y')$, hence discrete. The assertions (iv), (v), (vi) then follows from the first three assertions in view of the general principle Proposition 22.5.22, where in (v) we assume that g is separated. The other cases, we first remark that if x is isolated in $X_{g(f(x))}$, it is also isolated in $X_{f(x)}$; the fact that f is of finite type follows from Proposition 22.6.35. □

Proposition 23.6.17. *Let A be a complete Noetherian local ring, $Y = \operatorname{Spec}(A)$, X be a separated Y-scheme locally of finite type, x be a point over the closed point y of Y, and suppose that x is isolated in the fiber X_y. Then $\mathscr{O}_{X,x}$ is a finitely generated A-module and X is Y-isomorphic to the sum of $X' = \operatorname{Spec}(\mathscr{O}_{X,x})$ (which is a finite Y-scheme) and an A-scheme X''.*

Proof. It follows from Proposition 23.6.14 that $\mathscr{O}_{X,x}$ is a quasi-finite A-module. As $\mathscr{O}_{X,x}$ is Noetherian (Proposition 22.6.20) and the homomorphism $A \to \mathscr{O}_{X,x}$ is local, the hypothesis that A is complete implies that $\mathscr{O}_{X,x}$ is a finitely generated A-module (**??**). Let $X' = \operatorname{Spec}(\mathscr{O}_{X,x})$ be the local scheme of X at x and $g : X' \to X$ be the canonical morphism. The composition $f \circ g : X' \to Y$ is then finite, and since f is separated, g is finite by Proposition 23.6.3, so $g(X')$ is closed in X (Corollary 23.6.8). On the other hand, as g is of finite type and A is Noetherian, it is of finite presentation, and hence a local immersion at the closed point x' of X' (Proposition 22.6.52 and the definition of g). But X' is the only open neighborhood of x' in X', so it follows that $g(X')$ is open in X, which proves our assertion. □

Corollary 23.6.18. *Let A be a complete Noetherian local ring, $Y = \operatorname{Spec}(A)$, $f : X \to Y$ be a quasi-finite and separted morphism. Then X is Y-isomorphic to a sum $X' \amalg X''$, where X' is a finite Y-scheme and X'' is a quasi-finite Y-scheme such that, if y is the closed point of y, $X'' \cap f^{-1}(y) \neq \varnothing$.*

Proof. The fiber $f^{-1}(y)$ is finite and discrete by hypothesis, and the corollary then follows by recurrence on the number of points of $f^{-1}(y)$, using Proposition 23.6.17. □

23.6.3 Integral closure of a scheme

Proposition 23.6.19. *Let $(X, \mathscr{A})$ be a ringed space, $\mathscr{B}$ be an $\mathscr{A}$-algebra, and f be a section of $\mathscr{B}$ over X. The following properties are equivalent:*

(i) The sub-$\mathscr{A}$-algebra of $\mathscr{B}$ generated by f is finite (that is, of finite type as an $\mathscr{A}$-module).

(ii) There exists a sub-$\mathscr{A}$-algebra $\mathscr{C}$ of $\mathscr{B}$, which is an $\mathscr{A}$-module of finite type, such that $f \in \Gamma(X, \mathscr{C})$.

(iii) For any $x \in X$, f_x is integral over the fiber $\mathscr{A}_x$.

*If these equivalent conditions are satisfied, the section f is said to be **integral** over $\mathscr{A}$.*

Proof. As the sub-$\mathscr{A}$-module of $\mathscr{B}$ genearted by f^n is an $\mathscr{A}$-algebra, it is clear that (i) implies (ii). On the other hand, (ii) implies that for any $x \in X$, the $\mathscr{A}_x$-module $\mathscr{C}_x$ is of finite type, which

implies that any element of the algebra $\mathscr{C}_x$, and in particular f_x, is integral over $\mathscr{A}_x$. Finally, if for any point $x \in X$, we have a relation

$$f_x^n + (a_1)_x f_x^{n-1} + \cdots + (a_n)_x = 0$$

where a_i are sections of $\mathscr{A}$ over an open neighborhood U of x, the section $f^n|_U + a_1 \cdot f^{n-1}|_U + \cdots + a_n$ is zero over an open neighborhood $V \subseteq U$ of x, so $f^k|_V$ (for $k \geq 0$) is a linear combination over $\Gamma(V, \mathscr{A})$ of $f^j|_V$ with $0 \leq j \leq n-1$. We then conclude that (iii) implies (i). □

Corollary 23.6.20. *Under the hypothesis of Proposition 23.6.19, there exists a (unique) sub-$\mathscr{A}$-algebra $\mathscr{A}'$ of $\mathscr{B}$ such that for any $x \in X$, $\mathscr{A}'_x$ is the set of germs $f_x \in \mathscr{B}_x$ that is integral over $\mathscr{A}_x$. For any open subset $U \subseteq X$, the sections of $\mathscr{A}'$ over U is the sections of $\Gamma(U, \mathscr{B})$ that is integral over $\mathscr{A}|_U$. We say that $\mathscr{A}'$ is the* ***integral closure*** *of $\mathscr{A}$ in $\mathscr{B}$.*

Proof. The existence of $\mathscr{A}'$ is immediate, by setting $\Gamma(U, \mathscr{A}')$ to be the set of $f \in \Gamma(U, \mathscr{B})$ such that f_x is integral over $\mathscr{A}_x$ for any $x \in U$. It is clear that $\mathscr{A}'$ is an algebra, and the second assertion follows from Proposition 23.6.19. □

Let $(X, \mathscr{A})$, $(Y, \mathscr{B})$ be two ringed space and $f : X \to Y$ be a morphism. Let $\mathscr{C}$ (resp. $\mathscr{D}$) be an $\mathscr{A}$-algebra (resp. $\mathscr{B}$-algebra) and let $u : \mathscr{D} \to \mathscr{C}$ be a f-morphism. Then, if $\mathscr{A}'$ (resp. $\mathscr{B}'$) is the integral closure of $\mathscr{A}$ (resp. $\mathscr{B}$) in $\mathscr{C}$ (resp. $\mathscr{D}$), the restriction of u to $\mathscr{B}'$ is then a f-morphism $u' : \mathscr{B}' \to \mathscr{A}'$. In fact, if j is the canonical injection $\mathscr{B}' \to \mathscr{D}$, it suffices to show that

$$v = u^\sharp \circ f^*(j) : f^*(\mathscr{B}') \to \mathscr{C}'$$

maps $f^*(\mathscr{B}')$ into $\mathscr{A}'$. Now an element of $(f^*(\mathscr{B}'))_x = \mathscr{B}'_{f(x)} \otimes_{\mathscr{B}_{(f(x))}} \mathscr{A}_x$ is integral over $\mathscr{A}_x$ by the definition of $\mathscr{B}'$, and hence so is its image under v_x, which proves our assertion.

Proposition 23.6.21. *Let X be a scheme and $\mathscr{A}$ be a quasi-coherent $\mathscr{O}_X$-algebra. The integral closure $\mathscr{O}'_X$ of $\mathscr{O}_X$ in $\mathscr{A}$ is then a quasi-coherent $\mathscr{O}_X$-algebra, and for any affine open U of X, $\Gamma(X, \mathscr{O}'_X)$ is the integral closure of $\Gamma(U, \mathscr{O}_X)$ in $\Gamma(U, \mathscr{A})$.*

Proof. We can assume that $X = \operatorname{Spec}(B)$ is affine and $\mathscr{A} = \widetilde{A}$, where A is an B-algebra. Let B' be the integral closure of B in A. It then boils down to seeing that for any $x \in X$, an element of A_x, integer over B_x, necessarily belongs to B'_x, which follows from the fact that taking integral closure commutes with localization (Proposition 13.1.38). □

Under the hypothesis of Proposition 23.6.21, the X-scheme $X' = \operatorname{Spec}(\mathscr{O}'_X)$ is then called the **integral closure of X relative to $\mathscr{A}$**. We also deduce from Proposition 23.6.21 that if $f : X' \to X$ is the structural morphism, then for any open subset U of X, $f^{-1}(U)$ is the integral closure of the induced subscheme U by X, relative to $\mathscr{A}|_U$. In particular, we conclude that f is integral.

Let X and Y be schemes, $f : X \to Y$ be a morphism, $\mathscr{A}$ (resp. $\mathscr{B}$) be a quasi-coherent $\mathscr{O}_X$-algebra (resp. a $\mathscr{O}_Y$-algebra), and $u : \mathscr{B} \to \mathscr{A}$ be an f-morphism. We have seen that we have an induced f-morphism $u' : \mathscr{O}'_Y \to \mathscr{O}'_X$, where $\mathscr{O}'_X$ (resp. $\mathscr{O}'_Y$) is the integral closure of $\mathscr{O}_X$ (resp. $\mathscr{O}_Y$) relative to $\mathscr{A}$ (resp. $\mathscr{B}$), we deduce a canonical morphism $f' : \operatorname{Spec}(u') : X' \to Y'$

(Corollary 23.1.10) fitting into the following commutative diagram

$$\begin{tikzcd} X' \arrow[r, "f'"] \arrow[d] & Y' \arrow[d] \\ X \arrow[r, "f"] & Y \end{tikzcd} \tag{6.3.1}$$

Suppose that X has only finitely many irreducible components $(X_i)_{1\leq i\leq r}$, with generic points $(\xi_i)_{1\leq i\leq r}$, and consider in particular the integral closure of X relative to a quasi-coherent $\mathscr{K}_X$-algebra $\mathscr{A}$. By Corollary 22.7.19 and Corollary 22.7.20, $\mathscr{A}$ is the direct product of r quasi-coherent $\mathscr{O}_X$-algebras $\mathscr{A}_i$, the support of $\mathscr{A}_i$ being contained in X_i, and the induced sheaf of $\mathscr{A}_i$ over X_i is the constant sheaf whose fiber A_i is an algebra over $\mathscr{O}_{X,\xi_i}$. It is clear that the integral closure $\mathscr{O}'_X$ of $\mathscr{O}_X$ is the direct product of the integral closures $\mathscr{O}_X^{(i)}$ of $\mathscr{O}_X$ in each $\mathscr{A}_i$, and therefore the integral closure $X' = \operatorname{Spec}(\mathscr{O}'_X)$ of X relative to $\mathscr{A}$ is an X-scheme which is the sum of $\operatorname{Spec}(\mathscr{O}_X^{(i)}) = X'_i$.

Now suppose that the $\mathscr{O}_X$-algebra $\mathscr{A}$ is reduced, or equivalently, each algebra A_i is reduced, and therefore can be considered as an algebra over the field $\kappa(\xi_i)$ (equal to the rational function field of the reduced subscheme X_i of X); then the X'_i is a reduced X-scheme and X' is also the integral closure of X_{red}. Suppose moreover that the algebras A_i is a direct product of finitely many field K_{ij} $(1 \leq j \leq s_i)$; if $\mathscr{K}_{ij}$ is the subalgebra of $\mathscr{A}_i$ corresponding to K_{ij}, it is clear that $\mathscr{O}_X^{(i)}$ is the direct product of integral closures $\mathscr{O}_X^{(ij)}$ of $\mathscr{O}_X$ in $\mathscr{K}_{ij}$. Therefore, X'_i is the sum of $X'_{ij} = \operatorname{Spec}(\mathscr{O}_X^{(ij)})$. Moreover, under this hypothesis, we have the following:

Proposition 23.6.22. *Each X'_{ij} is an integral and normal X-scheme, and its rational function field $K(X'_{ij})$ is canonically identified with the algebraic closure K'_{ij} of $\kappa(\xi_i)$ in K_{ij}.*

Proof. In view of the preceding remarks, we can assume that X is integral, so $r = 1$, $s_1 = 1$, so that the unique algebra A_1 is a field K; let ξ be the generic point of X, and let $f : X' \to X$ be the structural morphism. For any nonempty affine open U of X, $f^{-1}(U)$ is identified with the integral closure B'_U in the field K of the intagral ring $B_U = \Gamma(U, \mathscr{O}_X)$ (Proposition 23.6.21); as the ring B'_U is integrally closed, so is its localizations, and $f^{-1}(U)$ is by definition an integral and normal scheme. Moreover, as (0) is the unique prime ideal of B'_U lying over the prime ideal (0) of B_U, $f^{-1}(\xi)$ is reduced to a singleton ξ', and $\kappa(\xi')$ is the fraction field K' of B'_U, which is none other than the algebraic closure of $\kappa(\xi)$ in K. Finally, X' is irreducible, because if U runs through the nonempty affine open subsets of X, the $f^{-1}(U)$ constitute an open covering of X' formed by irreducible open subsets; moreover the intersection $f^{-1}(U \cap V)$ two two opens contains ξ', hence nonempty, and we conclude from Proposition 4.1.5 that X' is irreducible. □

Corollary 23.6.23. *Let X be a reduced scheme with finitely many irreducible components (X_i), and let ξ_i be the generic point of X_i. The integral closure X' of X relative to $\mathscr{K}_X$ is the sum of r separated X-schemes X'_i which are integral and normal. If $f : X' \to X$ is the structural morphism, $f^{-1}(\xi_i)$ is reduced to the generic point ξ'_i of X'_i and we have $\kappa(\xi'_i) = \kappa(\xi_i)$, which means f is birational.*

Proof. This is a particular case of Proposition 23.6.22 by taking $K'_{ij} = \kappa(\xi_i)$. The rational function field of X'_i (which is $\kappa(\xi'_i)$) is then equal to $\kappa(\xi_i)$, whence our claim. □

The integral closure X' of X relative to $\mathscr{K}_X$ is called that **normalization** of the reduced scheme X. We note that the morphism $f : X' \to X$, being birational and integral, is closed

by Proposition 23.6.7, hence surjective (recall that a birational morphism is dominant). For $X' = X$, it is necessary and sufficient that X is normal. If X is an integral scheme, it follows from Corollary 23.6.23 that its normalization X' is integral.

Let X, Y be integral schemes, $f : X \to Y$ be a dominant morphism, $L = K(X)$, $K = K(Y)$ be the rational function field of X and Y. The morphism f corresponds to an injection $K \to L$, and if we identify K (resp. L) with the simple sheaf $\mathscr{K}_Y$ (resp. $\mathscr{K}_X$), this injection is an f-morphism. Let K_1 (resp. L_1) be an extension of K (resp. L) and suppose that we are given a monomorphism $K_1 \to L_1$ such that the diagram

$$\begin{tikzcd} K_1 \arrow[r] & L_1 \\ K \arrow[r] \arrow[u] & L \arrow[u] \end{tikzcd}$$

is commutative; if K_1 (resp. L_1) is considered as a simple sheaf over Y (resp. X), hence a $\mathscr{K}_Y$-algebra (resp. a $\mathscr{K}_X$-algebra), this signifies that $K_1 \to L_1$ is an f-morphism. Now if X' (resp. Y') is the integral closure of X (resp. Y) relative to L_1 (resp. K_1), X' (resp. Y') is a normal and integral scheme (Proposition 23.6.22) and its rational function field is canonically identified with the algebraic closure L' (resp. K') of L (resp. K) in L_1 (resp. K_1), and there exists a canonical morphism (necessarily dominant) $f' : X' \to Y'$ rendering the diagram (6.3.1). The important case is that $L_1 = L$, K_1 is an extension of K contained in L, and where we suppose that X is integral and normal, hence $X' = X$.

The preceding arguments then show that if X is a normal scheme and Y' is integrally closure of Y relative to a field $K_1 \subseteq L = K(X)$, any dominant morphism $f : X \to Y$ factors into

$$f : X \xrightarrow{f'} Y' \to Y$$

where f' is dominant; if the monomorphism $K_1 \to L$ is fixed, f' is necessarily unique (this can be verified when X and Y are both affine). We then say that given Y, L, and a K-monomorphism $K_1 \to L$, the integral closure Y' of Y relative to K_1 is a universal object.

Remark 23.6.2. Retain the hypothesis of Proposition 23.6.22 and suppose moreover that each algebra A_i is of finite dimension over $\kappa(\xi_i)$ (which implies that A_i is a direct product of finitely many fields); we can prove that the structural morphism $X' \to X$ is finite. For this, we can reduce to the case where X is reduced and affine with ring C, and that C has finitely many minimal prime ideals $\mathfrak{p}_i$ $(1 \leq i \leq r)$ with $C_i = C/\mathfrak{p}_i$. Then by Proposition 23.6.21 X' is finite over X if the integral closure of each C_i in finite extension of its fraction field is a finitely generated C-module, or equivalently, if C_i is Japanese for each i. We know that this condition is true if C is an algebra of finite type over a field, or over $\mathbb{Z}$, or over a complete Noetherian local ring. We then conclude that $X' \to X$ is a finite morphism if X is a scheme of finite type over a field, or over $\mathbb{Z}$, or over a complete Noetherian local ring.

23.6.4 Determinant of an endomorphism of $\mathscr{O}_X$-modules

Let A be a ring, E be a free A-module of rank n, and $u : E \to E$ be an endomorphism of E; recall that in order to define the characteristic polynomial of u, we consider the endomorphism $u \otimes 1$ of free the $A[T]$-module $E \otimes_A A[T]$ (which is of rank n), and we put

$$P(u, T) = \det(T \cdot I - (u \otimes 1))$$

(I is the identity morphism on $E \otimes_A A[T]$). We have

$$P(u,T) = T^n - \sigma_1(u)T^{n-1} + \cdots + (-1)^n\sigma_n(u)$$

where $\sigma_i(u)$ is an element of A, equal to a homogeneous polynomial of degree i (with integer coefficients) with entries the elements of the matrix of u relative to any basis of E. We say that the $\sigma_i(u)$ are the **elementray symmetric functions** of u, and we have in particular $\sigma_1(u) = \mathrm{tr}(u)$ and $\sigma_n(u) = \det(u)$. By Hamilton-Cayley theorem, we have

$$P(u,u) = u^n - \sigma_1(u)u^{n-1} + \cdots + (-1)^n\sigma_n(u) = 0 \tag{6.4.1}$$

which can also be written as

$$(\det(u)) \cdot 1_E = uQ(u) \tag{6.4.2}$$

(1_E is the identity morphism on E), where

$$Q(u) = (-1)^{n+1}(u^{n-1} - \sigma_1(u)u^{n-2} + \cdots + (-1)^{n-1}\sigma_{n-1}(u)) \tag{6.4.3}$$

Let $\varphi : A \to B$ be a homomorphism of rings; consider the B-module $E_{(B)} = E \otimes_A B$ which is free of rank n, and the extension $u \otimes 1$ of u to an endomorphism on $E_{(B)}$. It is immediate that we have $\sigma_i(u \otimes 1) = \varphi(\sigma_i(u))$ for all i.

Suppose now that A is an integral domain, with fraction field K, and E is a finitely generated A-module (not necessarily free now). Let n be the rank of E, which equals to the dimension of $E \otimes_A K$ over K. Any endomorphism u of E corresponds canonically to the endomorphism $u \otimes 1$ of $E \otimes_A K$. By abuse of language, we call $P(u \otimes 1, T)$ the characteristic polynomial of u and denoted by $P(u,T)$, and the coefficients $\sigma_i(u \otimes 1)$ is called the elementray symmetric functions of u and denoted by $\sigma_i(u)$. In particular the determinant $\det(u) = \det(u \otimes 1)$ is defiend. With these notations, the formulas (6.4.1) and (6.4.2) are meaningful and still valid, if we interpret the u^i as the homomorphism $E \to E \otimes_A K$ whici is the composition of the endomorphism $u^j \otimes 1 = (u \otimes 1)^j$ of $E \otimes_A K$ and the canonical homomorphism $x \mapsto x \otimes 1$.

If F is the torsion module of R and $E_0 = E/F$, we have $u(F) \subseteq F$, hence, by taking quotient, u induces an endomorphism u_0 of E_0; moreover $E \otimes_A K$ is identified with $E_0 \otimes_A K$ and $u \otimes 1$ is identified with $u_0 \otimes 1$, hence $\sigma_i(u) = \sigma_i(u_0)$ for $1 \leq i \leq n$.

If E is torsion-free, E is identified with a sub-A-module of $E \otimes_A K$, and the relation $u \otimes 1 = 0$ is equivalent to $u = 0$. If E is a free A-module, the two definitions of $\sigma_i(u)$ given above coincide according to the preceding remarks, which justifies the notations adopted. We also note that if E is a torsion module then $E_0 = \{0\}$, the exterior algebra of E_0 is reduced to K and the determinant of the endomorphism u_0 of E_0 is equal to 1.

Proposition 23.6.24. *Let A be an integral domain, E be a finitely generated A-module, u be an endomorphism of u. Then the elementray symmetric functions $\sigma_i(u)$ of u (and in particular* $\det(u)$*) are integral elements of K over A.*

Proof. This is a particular case of Proposition 13.1.44, where we set $B = K$ and note that condition (ii) is satisfied for $M = E$. □

Corollary 23.6.25. *Under the hypothesis of Proposition 23.6.24, if A is normal, the $\sigma_i(u)$ belong to A.*

Proposition 23.6.26. *Let A be an integral domain, E be a finitely generated A-module, of rank n, and u be an endomorphism of E such that the $\sigma_i(u)$ belong to A for each i. For u to be an automorphism of E, it is necessary that* $\det(u)$ *is invertible in A; this condition is sufficient if E is torsion free.*

Proof. This conditions is sufficient by (6.4.2) and (6.4.3), if E is torsion free, since E is then a sub-A-module of $E \otimes_A K$, and $(\det(u))^{-1}Q(u)$ is the inverse of u. Conversely, this is necessary, because if u is invertible, it follows from Proposition 23.6.24 that $\det(u^{-1})$ belongs to the integral closure A' of A in K, and is clearly the inverse of $\det(u)$ in A'. If $\det(u)$ is not invertible in A, then it belongs to a maximal ideal $\mathfrak{m}$ of A, which is the contraction of a maximal ideal of A' (Theorem 13.1.67), contradiction. □

We note a generalization of the preceding results. Consider a reduced Noetherian ring A and let $\mathfrak{p}_i$ $(1 \leq i \leq r)$ be the minimal prime ideals of A, and K_i be the fractional field of $A_i = A/\mathfrak{p}_i$. Then the total fraction field K of A is the direct product of the fields K_i (Proposition 12.2.24). Let E be a finitely generated A-module, and suppose that $E \otimes_A K$ is a K-module of dimension n. Then each K_i-vector space $E_i = E \otimes_A K_i$ is of dimension n. If u is an endomorphism of E, we put $P(u,T) = P(u \otimes 1, T)$ and $\sigma_j(u) = \sigma_j(u \otimes 1)$, and in particular $\det(u) = \det(u \otimes 1)$; the $\sigma_j(u)$ are then elements of K. It is immediate that $E \otimes_A K$ is a direct sum of E_i and each of them is stable under $u \otimes 1$. The restriction of $u \otimes 1$ to E_i is just the extension of u to E_i, and we conclude that $\sigma_j(u)$ is the element of K with component in K_i being $\sigma_j(u_i)$. As the integral closure of A in K is the direct product of that of A in K_i (Proposition 13.1.22), the $\sigma_j(u)$ are integral over A.

Lemma 23.6.27. *The sub-A-algebra of K genrated by the elements $\sigma_j(u)$ $(1 \leq j \leq n)$ for $u \in$* $\mathrm{Hom}_A(E,E)$*, is a finitely generated A-module.*

Let $(X, \mathscr{A})$ be a ringed space, $\mathscr{E}$ be a locally free $\mathscr{A}$-module (of finite rank). There is then by hypothesis a basis $\mathfrak{B}$ of X such that for any $V \in \mathfrak{B}$, $\mathscr{E}|_V$ is isomorphic to $\mathscr{A}^n|_V$ (the integer n may vary with V). Let u be an endomorphism of $\mathscr{E}$; for any $V \in \mathfrak{B}$, u_V is then an endomorphism of the $\Gamma(V, \mathscr{A})$-module $\Gamma(V, \mathscr{E})$, which is free by hypothesis; the determinant of u_V is then defined and belongs to $\Gamma(V, \mathscr{A})$. Moreover, if $e_1, \dots, e_n$ is a basis of $\Gamma(V, \mathscr{E})$, their restriction to any open subset $W \subseteq V$ form a basis of $\Gamma(W, \mathscr{E})$ over $\Gamma(W, \mathscr{A})$, so $\det(u_W)$ is the restriction of $\det(u_V)$ to W. There then exists a unique section of $\mathscr{A}$ over X, which we denote by $\det(u)$ and call the **determinant** of u, such that the restriction of $\det(u)$ to any $V \in \mathfrak{B}$ is $\det(u_V)$. It is clear that for any $x \in X$, we have $\det(u)_x = \det(u_x)$; for two endomorphisms u, v of $\mathscr{E}$, we have

$$\det(u \circ v) = (\det(u))(\det(v)), \quad \det(1_{\mathscr{E}}) = 1_{\mathscr{A}}.$$

If $\mathscr{E}$ is of rank n (for example if X is connected), we have

$$\det(s \cdot u) = s^n \det(u)$$

for any $s \in \Gamma(X, \mathscr{A})$ (we note that $\det(0) = 0_{\mathscr{A}}$ if $n \geq 1$, but $\det(0) = 1_{\mathscr{A}}$ if $n = 0$). Moreover, for u to be an automorphism of $\mathscr{E}$, it is necessary and sufficient that $\det(u)$ is invertible in $\Gamma(X, \mathscr{A})$ (Proposition 23.6.26).

If $\mathscr{E}$ is of rank n, we can similarly define the elementary symmetric functions $\sigma_i(u)$ for u, which are elements of $\Gamma(X, \mathscr{A})$, and we also have the relations (6.4.2) and (6.4.3).

We have then define a homomorphism $\det : \mathrm{Hom}_{\mathscr{A}}(\mathscr{E},\mathscr{E}) \to \Gamma(X,\mathscr{A})$ of multiplicative monoids. Note that $\mathrm{Hom}_{\mathscr{A}}(\mathscr{E},\mathscr{E}) = \Gamma(X,\mathscr{H}om_{\mathscr{A}}(\mathscr{E},\mathscr{E}))$ by definition, so we can replace X by any open subset U in this definition of det, and therefore obtain a homomorphism $\det : \mathscr{H}om_{\mathscr{A}}(\mathscr{E},\mathscr{E}) \to \mathscr{A}$ of sheaves of multiplicative monoids. If $\mathscr{E}$ is of constant rank, we can similarly define the homomorphisms $\sigma_i : \mathscr{H}om_{\mathscr{A}}(\mathscr{E},\mathscr{E}) \to \mathscr{A}$ of sheaves of sets; for $i = 1$, the homomorphism $\sigma_1 = \mathrm{tr}$ is a homomorphism of $\mathscr{A}$-modules.

Let $(Y,\mathscr{B})$ be a second ringed space and $f : (X,\mathscr{A}) \to (Y,\mathscr{B})$ be a morphism of ringed spaces; if $\mathscr{F}$ is a locally free $\mathscr{B}$-module, $f^*(\mathscr{F})$ is a locally free $\mathscr{A}$-module (with the same rank of $\mathscr{F}$). For any endomorphism v of $\mathscr{F}$, $f^*(v)$ is then an endomorphism of $f^*(\mathscr{F})$, and it follows from these definitions that $\det(f^*(v))$ is the section of $\mathscr{A} = f^*(\mathscr{B})$ over X which corresponds canonically to $\det(v) \in \Gamma(Y,\mathscr{B})$. We can then say that the homomorphism $f^*(\det) : f^*(\mathscr{H}om_{\mathscr{B}}(\mathscr{F},\mathscr{F})) \to f^*(\mathscr{B}) = \mathscr{A}$ is the composition

$$f^*(\mathscr{H}om_{\mathscr{B}}(\mathscr{F},\mathscr{F})) \xrightarrow{\gamma^\sharp} \mathscr{H}om_{\mathscr{A}}(f^*(\mathscr{F}), f^*(\mathscr{F})) \xrightarrow{\det} \mathscr{A} \tag{6.4.4}$$

(formula (3.4.5)). We have a similar result for σ_i.

Suppose now that X is a locally integral scheme, so its sheaf of rational function $\mathscr{K}_X$ is locally simple over X (Corollary 22.7.19) and quasi-coherent as $\mathscr{O}_X$-module. If $\mathscr{E}$ is a qausi-coherent $\mathscr{O}_X$-module of finite type, $\mathscr{E}' = \mathscr{E} \otimes_{\mathscr{O}_X} \mathscr{K}_X$ is then a locally free $\mathscr{K}_X$-module (Corollary 22.7.21). For any endomorphism u of $\mathscr{E}$, $u \otimes 1_{\mathscr{K}_X}$ is then an endomorphism of $\mathscr{E}'$, and $\det(u \otimes 1)$ is a section of $\mathscr{K}_X$ over X, which is called the **determinant** of u and denoted by $\det(u)$. It follows from Proposition 23.6.24 that $\det(u)$ is a section of the integral closure of $\mathscr{O}_X$ in $\mathscr{K}_X$; if X is also normal, $\det(u)$ is then a section of $\mathscr{O}_X$ over X, and if we suppose moreover that $\mathscr{E}$ is torsion free, for u to be an automorphism of $\mathscr{E}$, it is necessary and sufficient that $\det(u)$ is invertible (Proposition 23.6.26). The formulae (6.4.2) and (6.4.3) are still valid; the homomorphism $u \mapsto \det(u)$ then defines a homomorphism $\det : \mathscr{H}om_{\mathscr{O}_X}(\mathscr{E},\mathscr{E}) \to \mathscr{K}_X$, which has values in $\mathscr{O}_X$ if X is normal. We have analogous results for the elementary symmetric function functions $\sigma_j(u)$, if $\mathscr{E}'$ has constant rank; if moreover X is normal, the $\sigma_j(u)$ are sections of $\mathscr{O}_X$ over X.

Finally, let X and Y be integral schemes, and $f : X \to Y$ be a dominant morphism. We see that there exists a canonical homomorphism $f^*(\mathscr{K}_Y) \to \mathscr{K}_X$, whence induces, for any quasi-coherent $\mathscr{O}_Y$-module $\mathscr{F}$ of finite type, a canonical homomorphism $\theta : f^*(\mathscr{F} \otimes_{\mathscr{O}_Y} \mathscr{K}_Y) \to f^*(\mathscr{F}) \otimes_{\mathscr{O}_X} \mathscr{K}_X$. If v is an endomorphism of $\mathscr{F}$, $f^*(v \otimes 1_{\mathscr{K}_Y})$ is an endomorphism of $f^*(\mathscr{F} \otimes_{\mathscr{O}_Y} \mathscr{K}_Y)$, and we have a commutative diagram

$$\begin{tikzcd}
f^*(\mathscr{F} \otimes_{\mathscr{O}_Y} \mathscr{K}_Y) \arrow[r, "f^*(v\otimes 1)"] \arrow[d, "\theta"'] & f^*(\mathscr{F} \otimes_{\mathscr{O}_Y} \mathscr{K}_Y) \arrow[d, "\theta"] \\
f^*(\mathscr{F}) \otimes_{\mathscr{O}_X} \mathscr{K}_X \arrow[r, "f^*(v)\otimes 1"] & f^*(\mathscr{F}) \otimes_{\mathscr{O}_X} \mathscr{K}_X
\end{tikzcd}$$

We then conclude that $\det(f^*(v))$ is the canonical image of the section $\det(v)$ of $\mathscr{K}_Y$ under the canonical homomorphism $f^*(\mathscr{K}_Y) \to \mathscr{K}_X$. In fact, it is immediate that we are reduced to the case where $X = \mathrm{Spec}(B)$ and $Y = \mathrm{Spec}(A)$ are affine, A, B being integral domains with fraction fields K, L respectively, the hommorphism $A \to B$ being injective and extends to a monomorphism $K \to L$. If $\mathscr{F} = \widetilde{M}$ where M is a finitely generated A-module, the dimension of $M \otimes_A K$

is equal to that of $(M \otimes_A B) \otimes_B L$ over L, and $\det((u \otimes 1) \otimes 1)$ is the image of $\det(u \otimes 1)$ in L for any endomorphism u of M, whence our conclusion.

Finally, suppose that X is a reduced locally Noetherian scheme, whose sheaf of rational functions $\mathscr{K}_X$ is quasi-coherent by Proposition 22.7.22. Let $\mathscr{E}$ be a coherent $\mathscr{O}_X$-module such that $\mathscr{E}' = \mathscr{E} \otimes_{\mathscr{O}_X} \mathscr{K}_X$ is locally free of rank n. We can then define for each endomorphism u of $\mathscr{E}$ the elementary symmetric functions $\sigma_j(u)$, which are sections of $\mathscr{K}_X$ over X.

23.6.5 Norm of an invertible sheaf

Let $(X, \mathscr{A})$ be a ringed space and $\mathscr{B}$ be an $\mathscr{A}$-algebra. The $\mathscr{A}$-module $\mathscr{B}$ is canonically identified with a sub-$\mathscr{A}$-module of $\mathscr{H}om_{\mathscr{A}}(\mathscr{B}, \mathscr{B})$, where a section f of $\mathscr{B}$ over an open subset U of X is identified with the multiplication by this section. Assume that $(X, \mathscr{A})$ and $\mathscr{B}$ satisfies the conditions given in the previous subsection, so that we can define $\det(f)$ (resp. $\sigma_j(f)$) to be a section of $\mathscr{K}_X$ over U, which is called the **norm** of f (resp. the elementary symmetric functions) of f and denoted by $N_{\mathscr{B}/\mathscr{A}}(f)$. We suppose that one of the following conditions is satisfied:

(α) $\mathscr{B}$ is a locally free $\mathscr{A}$-module of finite rank n.

(β) $(X, \mathscr{A})$ is a reduced locally Noetherian scheme, $\mathscr{B}$ is a coherent $\mathscr{A}$-module such that $\mathscr{B} \otimes_{\mathscr{A}} \mathscr{K}_X$ is a locally free $\mathscr{K}_X$-module of rank n, and for any section $f \in \Gamma(U, \mathscr{B})$ over an open subset $U \subseteq X$, $\sigma_j(f)$ $(1 \leq j \leq n)$ is a section of $\mathscr{A}$ over U (this is ture for example if X is normal).

The hypothesis that $\mathscr{B} \otimes_{\mathscr{A}} \mathscr{K}_X$ is locally free can be expressed by the following: denote by X_i the reduced closed subschemes of X with underlying space the irreducible components of X, which are then locally Noetherian integral schemes. Any $x \in X$ belongs to finitely many X_i, and $\mathscr{B} \otimes_{\mathscr{A}} \mathscr{K}_{X_i}$ is a locally free $\mathscr{K}_{X_i}$-module of constant rank k_i (Corollary 22.7.20); to say that $\mathscr{B} \otimes_{\mathscr{A}} \mathscr{K}_X$ is locally free $\mathscr{K}_X$-module signifies that, for any $x \in X$, the ranks k_i such that $x \in X_i$ are all equal. This question is in fact local, and we can assume that $X = \operatorname{Spec}(A)$, where A is a reduced Noetherian ring, and $\mathscr{B} = \widetilde{B}$ where B is a finite A-algebra. If $\mathfrak{p}_i$ $(1 \leq i \leq r)$ are the minimal prime ideals of A, the total fraction ring K of A is then the direct product of K_i, where K_i is the fraction field of $A_i = A/\mathfrak{p}_i$, and $B \otimes_A K$ is then the direct sum of $B \otimes_A K_i$, whence our conclusion.

It is clear that under the hypotheses (α) or (β), we then define a homomorphism $N_{\mathscr{B}/\mathscr{A}} : \mathscr{B} \to \mathscr{A}$ of sheaves of multiplicative monoids, which is also denoted by N if there is no confusion, and called the norm homomorphism. For two sections f, g of $\mathscr{B}$ over an open subset U, we then have

$$N_{\mathscr{B}/\mathscr{A}}(fg) = N_{\mathscr{B}/\mathscr{A}}(f)N_{\mathscr{B}/\mathscr{A}}(g), \quad N_{\mathscr{B}/\mathscr{A}}(1_{\mathscr{B}}) = 1_{\mathscr{A}} \tag{6.5.1}$$

for the corresponding sections of $\mathscr{A}$ over U. Also, for any section s of $\mathscr{A}$ over U, we have

$$N_{\mathscr{B}/\mathscr{A}}(s \cdot 1_{\mathscr{B}}) = s^n. \tag{6.5.2}$$

In case (α), for any $f \in \Gamma(U, \mathscr{B})$ to be invertible, it is necessary and sufficient that $N(f) \in \Gamma(U, \mathscr{A})$ is invertiblel; in case (β), this condition is necessary, and is sufficient if $\mathscr{B}$ is a torsion free $\mathscr{A}$-module.

Suppose the one of the hypotheses (α), (β) is satisfied, and let $\mathscr{L}'$ be an invertible $\mathscr{B}$-module. We can canonically associate an invertible $\mathscr{A}$-module by the following. Denote by $\mathscr{A}^\times$ (resp. $\mathscr{B}^\times$) the subsheaf of $\mathscr{A}$ (resp. $\mathscr{B}$) such that $\Gamma(U, \mathscr{A}^\times)$ (resp. $\Gamma(U, \mathscr{B}^\times)$) is the set of invertible elements of $\Gamma(U, \mathscr{A})$ (resp. $\Gamma(U, \mathscr{B})$) for any open subset $U \subseteq X$; this is a sheaf of multiplicative groups, and $N_{\mathscr{B}/\mathscr{A}}$, restricted to $\mathscr{B}^\times$, is a homomorphism $\mathscr{B}^\times \to \mathscr{A}^\times$ of sheaves of groups. Let $\mathfrak{L}$ be the set of couples $(U_\lambda, \eta_\lambda)$, with the following property: U_λ is an open subset of X and $\eta_\lambda : \mathscr{L}'|_{U_\lambda} \xrightarrow{\sim} \mathscr{B}|_{U_\lambda}$ is an isomorphism of $(B|_{U_\lambda})$-modules. By hypothesis, the U_λ for an open covering og X; for two indices λ, μ, we put $\omega_{\lambda\mu} = (\eta_\lambda|_{U_\lambda \cap U_\mu}) \circ (\eta_\mu|_{U_\lambda \cap U_\mu})^{-1}$, which is an automorphism of $\mathscr{B}|_{U_\lambda \cap U_\mu}$, and canonically identified with a section of $\mathscr{B}^\times$ over $U_\lambda \cap U_\mu$, and $(\omega_{\lambda\mu})$ is a 1-cocycle over the covering $\mathfrak{U} = (U_\lambda)$ with values in $\mathscr{B}^\times$. The fact that $N_{\mathscr{B}/\mathscr{A}} : \mathscr{B}^\times \to \mathscr{A}^\times$ is a homomorphism implies that $(N_{\mathscr{B}/\mathscr{A}}(\omega_{\lambda\mu}))$ is a 1-cocycle of $\mathfrak{U}$ with values in $\mathscr{A}^\times$, which then corresponds (up to isomorphism) to an invertible $\mathscr{A}$-module. This invertible $\mathscr{A}$-module is denoted by $N_{\mathscr{B}/\mathscr{A}}(\mathscr{L}')$ and is called the norm of the invertible $\mathscr{B}$-module $\mathscr{L}'$.

Let $\mathfrak{M}$ be a subset of $\mathfrak{L}$ such that the U_λ form an open covering of X, and let $\mathfrak{B}$ be a covering of X. The restriction of the cocycle $(\omega_{\lambda\mu})$ to $\mathfrak{B}$ defines a 1-cocycle $(N_{\mathscr{B}/\mathscr{A}}(\omega_{\lambda\mu}))$, which is the restriction of the 1-cocycle $(N_{\mathscr{B}/\mathscr{A}}(\omega_{\lambda\mu}))$ to $\mathfrak{U}$; it is clear that there is a canonical isomorphism of the invertible $\mathscr{A}$-modules thus defined, and we can therefore define $N_{\mathscr{B}/\mathscr{A}}(\mathscr{L}')$ by a refinement of the covering $\mathfrak{U}$. This shows that, if $\mathscr{L}'$ and $\mathscr{K}'$ are two invertible $\mathscr{B}$-modules, by (6.5.1) we have

$$N(\mathscr{L}' \otimes_{\mathscr{B}} \mathscr{K}') = N(\mathscr{L}') \otimes_{\mathscr{A}} N(\mathscr{K}'), \quad N_{\mathscr{B}/\mathscr{A}}(\mathscr{B}) = \mathscr{A}, \tag{6.5.3}$$

and therefore $N(\mathscr{L}'^{-1}) = N(\mathscr{L}')^{-1}$. Also, it follows from (6.5.2) that if $\mathscr{L}$ is an invertible $\mathscr{A}$-module, we have

$$N_{\mathscr{B}/\mathscr{A}}(\mathscr{L} \otimes_{\mathscr{A}} \mathscr{B}) = \mathscr{L}^{\otimes n}. \tag{6.5.4}$$

We show that $N_{\mathscr{B}/\mathscr{A}}$ is a covariant functor on the category of invertible $\mathscr{B}$-modules. Let $u' : \mathscr{L}' \to \mathscr{K}'$ be a homomorphism of invertible $\mathscr{B}$-modules, and let $\mathfrak{B} = (U_\lambda)$ be an open covering of X such that for any λ, we have an isomorphism $\eta_\lambda : \mathscr{L}'|_{U_\lambda} \xrightarrow{\sim} \mathscr{B}|_{U_\lambda}$ and $\tau_\lambda : \mathscr{K}'|_{U_\lambda} \xrightarrow{\sim} \mathscr{B}|_{U_\lambda}$; there is then for each λ an endomorphism u'_λ of $\mathscr{B}|_{U_\lambda}$ such that $u'_\lambda \circ \eta_\lambda = \tau_\lambda \circ (u'|_{U_\lambda})$, and we can evidently identify u'_λ with a section of $\mathscr{B}$ over U_λ. Hence, for any couple (λ, μ) of indices, the restriction of $(\tau_\lambda)^{-1} \circ u'_\lambda \circ \eta_\lambda$ and $(\tau_\mu)^{-1} \circ u'_\mu \circ \eta_\mu$ to $U_\lambda \cap U_\mu$ coincide. We then deduce for the 1-cocycle $(\omega_{\lambda\mu})$ corresponding to $\mathscr{L}'$ and the 1-cocycle $(\gamma_{\lambda\mu})$ corresponding to $\mathscr{K}'$ the relation

$$\gamma_{\lambda\mu} u'_\mu = u'_\lambda \omega_{\lambda\mu}.$$

If we put $u_\lambda = N(u'_\lambda)$, we then have the analogous relation

$$N(\gamma_{\lambda\mu}) u_\mu = u_\lambda N(\omega_{\lambda\mu})$$

and therefore the u_λ define a homomorphism $N(\mathscr{L}') \to N(\mathscr{K}')$, which is denoted by $N_{\mathscr{B}/\mathscr{A}}(u)$ or $N(u)$. In view of Proposition 23.6.26, it is clear that under the hypothesis (α), u' is an isomorphism if and only if u is, and this is ture under the hypothesis (β) if $\mathscr{B}$ is moreover torsion free. In particular, if consider the hommorphisms $\mathscr{B} \to \mathscr{L}'$, which correspond to global sections of

$\mathscr{L}'$, since $N_{\mathscr{B}/\mathscr{A}}(\mathscr{B}) = \mathscr{A}$, we get a canonical homomorphism

$$N_{\mathscr{B}/\mathscr{A}} : \Gamma(X, \mathscr{L}') \to \Gamma(X, N_{\mathscr{B}/\mathscr{A}}(\mathscr{L}')).$$

It also follows from (6.5.1) that if $f' \in \Gamma(X, \mathscr{L}')$, $g' \in \Gamma(X, \mathscr{K}')$, we have

$$N(f' \otimes g') = N(f') \otimes N(g'). \tag{6.5.5}$$

Also, for any invertible $\mathscr{A}$-module $\mathscr{L}$ and any section $f \in \Gamma(X, \mathscr{L})$, we have

$$N_{\mathscr{B}/\mathscr{A}}(f \otimes 1_{\mathscr{B}}) = f^{\otimes n}. \tag{6.5.6}$$

Finally, for the homomorphism $\mathscr{B} \to \mathscr{L}'$ corresponding to a section f' of $\mathscr{L}'$ over X to be an isomorphism, it is necessary and sufficient that f'_x generates $\mathscr{L}'_x$ for any $x \in X$; under condition (α), this is equivalent to that $N(f')_x$ generates $(N(\mathscr{L}'))_x$ for any x, and this is ture for condition (β) if $\mathscr{B}$ is torsion free.

Let $(X, \mathscr{A})$, $(X', \mathscr{A}')$ be two ringed spaces and $\varphi : X' \to X$ be a morphism, $\mathscr{B}$ be an $\mathscr{A}$-algebra, and $\mathscr{B}' = \varphi^*(\mathscr{B})$. Suppose that one of the following conditions is satisfied:

(i) $\mathscr{B}$ satisfies condition (α).

(ii) $(X, \mathscr{A})$ and $\mathscr{B}$ satisfy condition (β), $(X', \mathscr{A}')$ is a reduced locally Noehterian scheme, and if we denote by X_α and X'_β the reduced closed subschemes of X and X' with underlying space the irreducible components of these spaces, the restriction of φ to X'_β is a dominant morphism from X'_β to X_α.

Under these conditions, we claim that $\mathscr{B}'$ verifies the conditions (α) or (β); the first case is clear, and to prove the second one, it suffices to prove that for any $x' \in X'$, the ranks of $\mathscr{B}' \otimes_{\mathscr{O}_{X'}} \mathscr{K}_{X'_\beta}$ for the indices β such that $x' \in X'_\beta$ are the same. Now, if the restriction of φ to X'_β is a dominant morphism into X_α, the rank of $\mathscr{B}' \otimes_{\mathscr{O}_{X'}} \mathscr{K}_{X'_\beta}$ is equal to that of $\mathscr{B} \otimes_{\mathscr{O}_X} \mathscr{K}_{X_\alpha}$ (which can be seen from the affine case), whence our claim.

This being established, it follows that if f is a section of $\mathscr{B}$ over an open subset $U \subseteq X$, and f' is the inverse image of f under φ, $N_{\mathscr{B}'/\mathscr{A}'}(f')$ is the section of $\mathscr{A}'$ over $\varphi^{-1}(U)$ which is the inverse image of $N_{\mathscr{B}/\mathscr{A}}(f)$ under φ. If $\mathscr{L}$ is an invertible $\mathscr{B}$-module and if $\mathscr{L}' = \varphi^*(\mathscr{L})$ (which is an invertible $\mathscr{B}'$-module), we have

$$N_{\mathscr{B}'/\mathscr{A}'}(\mathscr{L}') = \varphi^*(N_{\mathscr{B}/\mathscr{A}}(\mathscr{L})). \tag{6.5.7}$$

Suppose now that $(X, \mathscr{A})$ is a scheme. Then giving a quasi-coherent finite $\mathscr{A}$-algebra $\mathscr{B}$ is equivalent to giving a finite morphism $\varphi : X' \to X$ such that $\varphi_*(\mathscr{O}_{X'}) = \mathscr{B}$, defined up to X-isomorphisms (Corollary 23.1.10), and in this case X' is isomorphic to the affine specturm $\mathrm{Spec}(\mathscr{B})$. Moreover, if this morphism $\varphi : X' \to X$ is fixed, then giving a quasi-coherent $\mathscr{O}_{X'}$-module $\mathscr{F}'$ is equivalent to giving a quasi-coherent $\mathscr{B}$-module such that $\varphi_*(\mathscr{F}') = \mathscr{F}$ (Proposition 23.1.18), and for $\mathscr{F}'$ to be invertible, it is necessary and sufficient that $\mathscr{F}$ is (Proposition 23.6.10). To utilize the preceding results for the finite morphism φ, it is then necessary to assume that $\mathscr{B} = \varphi_*(\mathscr{O}_{X'})$ satisfies condition (α) or (β). For any invertible $\mathscr{O}_{X'}$-module $\mathscr{L}'$, we

then set

$$N_{X'/X}(\mathscr{L}') := N_{\varphi_*(\mathscr{O}_{X'})/\mathscr{O}_X}(\varphi_*(\mathscr{L}')) \tag{6.5.8}$$

which is called the **norm** (relative to φ) of $\mathscr{L}'$. Similarly, if $u' : \mathscr{L}' \to \mathscr{K}'$ is a homomorphism of invertible $\mathscr{O}_{X'}$-modules, we put

$$N_{X'/X}(u') = N_{\varphi_*(\mathscr{O}_X)/\mathscr{O}_X}(\varphi_*(u')) : N_{X'/X}(\mathscr{L}') \to N_{X'/X}(\mathscr{K}'). \tag{6.5.9}$$

In particular, if we consider homomorphisms $\mathscr{O}_{X'} \to \mathscr{L}'$, we obtain a canonical homomorphism

$$N_{X'/X} : \Gamma(X', \mathscr{L}') \to \Gamma(X, N_{X'/X}(\mathscr{L}')). \tag{6.5.10}$$

Proposition 23.6.28. *Let $\varphi : X' \to X$ be a finite morphism and suppose that condition (i) or (ii) is satisfied. For a homomorphism $u' : \mathscr{L}' \to \mathscr{K}'$ of invertible $\mathscr{O}_{X'}$-modules to be an isomorphism, it is necessary and sufficient that, in the first case, that $N_{X'/X}(u')$ is an isomorphism; in the second case, this condition is necessary, and is sufficient if $\varphi_*(\mathscr{O}_{X'})$ is torsion free.*

Proof. This is a particular case of our previous discussions, where we put $\mathscr{B} = \varphi_*(\mathscr{O}_{X'})$, which is a quasi-coherent finite $\mathscr{O}_X$-algebra. We also note that by Corollary 23.1.17, for $\varphi_*(u')$ to be an isomorphism, it is necessary and sufficient that u' is an isomorphism. □

Corollary 23.6.29. *Retain the hypothesis of Proposition 23.6.28 and suppose that $\varphi_*(\mathscr{O}_{X'})$ is torsion free. Let $\mathscr{L}'$ be an invertible $\mathscr{O}_{X'}$-module, f' be a section of $\mathscr{L}'$ over X', and $f = N_{X'/X}(f')$ the section of $\mathscr{L} = N_{X'/X}(\mathscr{L}')$ over X corresponding to f'. Then we have $\varphi(X' - X'_{f'}) = X - X_f$ and X_f is the largest open subset of X such that $\varphi^{-1}(U) \subseteq X'_{f'}$.*

Proof. In fact, $\varphi(X' - X'_{f'})$ is closed in X by Proposition 23.6.7, and it then suffices to prove the second assertion. Now the relation $U \subseteq X_f$ is equivalent to that the hommorphism $\mathscr{O}_X|_U \to \mathscr{L}|_U$ defined by $f|_U$ is an isomorphism. In view of Proposition 23.6.28, this is equivalent to that the homomorphism $\mathscr{O}_{X'}|_{\varphi^{-1}(U)} \to \mathscr{L}'|_{\varphi^{-1}(U)}$ defined by $f'|_{\varphi^{-1}(U)}$ is an isomorphism, which means $\varphi^{-1}(U) \subseteq X'_{f'}$. □

Proposition 23.6.30. *Let $\varphi : X' \to X$ be a finite morphism, $\psi : Y \to X$ be a morphism; let $Y' = X'_{(Y)}$, $\varphi' = \varphi_{(Y)}$, $\psi' = \psi_{(X')}$ such that the following diagram is commutative*

$$\begin{tikzcd} Y' \arrow[r, "\psi'"] \arrow[d, "\varphi'"'] & X' \arrow[d, "\varphi"] \\ Y \arrow[r, "\psi"] & X \end{tikzcd}$$

Assume the hypotheses of Proposition 23.6.28. Then for any invertible $\mathscr{O}_{X'}$-module $\mathscr{L}'$, we have

$$N_{Y'/Y}(\psi'^*(\mathscr{L}')) = \psi^*(N_{X'/X}(\mathscr{L}')).$$

Proof. Note that we have $\psi^*(\varphi_*(\mathscr{L}')) = \varphi'_*(\psi'^*(\mathscr{L}'))$ in view of Corollary 23.1.28, and in particular $\varphi'_*(\mathscr{O}_{Y'}) = \psi^*(\varphi_*(\mathscr{O}_{X'}))$; if $\varphi_*(\mathscr{O}_{X'})$ is locally free, so is $\varphi'_*(\mathscr{O}_{Y'})$. The conclusion then follows from the definition of $N_{X'/X}$, $N_{Y'/Y}$, and (6.5.7). □

23.6.6 Application: a criterion of amplitude

Proposition 23.6.31. *Let $f : X \to Y$ be a quasi-compact morphism, $g : X' \to X$ be a finite and surjective morphism such that $(X, \mathscr{O}_X)$ and $g_*(\mathscr{O}_{X'})$ satisfy condition (β). Then, for an ample invertible $\mathscr{O}_{X'}$-module $\mathscr{L}'$ relative to $f \circ g$, $N_{X'/X}(\mathscr{L}') = \mathscr{L}$ is ample relative to f.*

Proof. We can suppose that Y is affine, and then, in view of Corollary 23.4.37, it suffices to prove that, if $\mathscr{L}'$ is ample, then $\mathscr{L} = N_{X'/X}(\mathscr{L}')$ is ample. For this, we can assume that $g_*(\mathscr{O}_{X'})$ is torsion free. In fact, let $\mathscr{T}$ be the kernel of the homomorphism $g_*(\mathscr{O}_{X'}) \to g_*(\mathscr{O}_{X'}) \otimes_{\mathscr{O}_X} \mathscr{K}_X$, which is a coherent ideal of $\mathscr{B} = g_*(\mathscr{O}_{X'})$ by hypothesis, and put $X'' = \operatorname{Spec}(\mathscr{B}/\mathscr{T})$; we then have a commutative diagram

$$\begin{tikzcd} X'' \arrow[rr, "j"] \arrow[dr, "g'"'] & & X' \arrow[dl, "g"] \\ & X & \end{tikzcd}$$

where j is a closed immersion (Proposition 23.1.25). Moreover, since $\mathscr{T}$ is a torsion sheaf, by Proposition 22.7.27 and Proposition 19.4.6 we see that the support of $\mathscr{T}$ is a closed subset that is rare in X, so for the generic point x of an irreducible component of X, there exists an affine open neighborhood U of x such that $\mathscr{B}|_U = (\mathscr{B}/\mathscr{T})|_U$. As g is by hypothesis surjective, we then conclude that $x \in g'(X'')$; g' is then dominant, and hence surjective by Proposition 23.6.7 since it is a finite morphism. By definition we have

$$g'_*(\mathscr{O}_{X''}) \otimes \mathscr{K}_X = (\mathscr{B}/\mathscr{T}) \otimes_{\mathscr{O}_X} \mathscr{K}_X = g_*(\mathscr{O}_{X'}) \otimes_{\mathscr{O}_X} \mathscr{K}_X,$$

so $(X, \mathscr{O}_X)$ and $g'_*(\mathscr{O}_{X''})$ satisfies condition (β), and $g'_*(\mathscr{O}_{X''})$ is torsion free. Finally, $j^*(\mathscr{L}') = \mathscr{L}''$ is an ample $\mathscr{O}_{X''}$-module (Proposition 23.4.45(ii)), and $N_{X''/X}(\mathscr{L}'') = N_{X'/X}(\mathscr{L}')$. To see this, we note that to define these two invertible $\mathscr{O}_X$-modules we can utilize an affine open covering (U_λ) of X such that $g_*(\mathscr{L}')$ and $g'_*(\mathscr{L}'')$ to U_λ are respectively isomorphic to $\mathscr{B}|_{U_\lambda}$ and $(\mathscr{B}/\mathscr{T})|_{U_\lambda}$. By Corollary 23.1.23, we immediately see that for any isomorphism $\eta_\lambda : g_*(\mathscr{L}')|_{U_\lambda} \to \mathscr{B}|_{U_\lambda}$ corresponds canonically to an isomorphism

$$\eta'_\lambda : g'_*(\mathscr{L}'')|_{U_\lambda} \to (\mathscr{B}/\mathscr{T})|_{U_\lambda}$$

so that, if $(\omega_{\lambda\mu})$ and $(\omega'_{\lambda\mu})$ are the 1-cocycles corresponding to the isomorphisms (η_λ) and (η'_λ), $\omega'_{\lambda\mu}$ is the canonical image of $\omega_{\lambda\mu} \in \Gamma(U_\lambda \cap U_\mu, \mathscr{B})$ to $\Gamma(U_\lambda \cap U_\mu, \mathscr{B}/\mathscr{T})$. In view of the definition of $\mathscr{T}$, we conclude that

$$N_{\mathscr{B}/\mathscr{A}}(\omega_{\lambda\mu}) = N_{(\mathscr{B}/\mathscr{T})/\mathscr{A}}(\omega'_{\lambda\mu})$$

(where $\mathscr{A} = \mathscr{O}_X$), whence the equality.

Suppose then that $g_*(\mathscr{O}_{X'})$ is torsion free. It then suffices to prove that if f runs through the sections of $\mathscr{L}^{\otimes n}$ ($n > 0$) over X, the X_f form a basis of X (Theorem 23.4.23). Now, let $x \in X$, and let U be an open neighborhood of x; as $g^{-1}(x)$ is finite by Corollary 23.6.5 and $\mathscr{L}'$ is ample, there exists an integer $n > 0$ and a section f' of $\mathscr{L}'^{\otimes n}$ over X' such that $X'_{f'}$ is an open neighborhood of $g^{-1}(x)$ contained in $g^{-1}(U)$. As we have $\mathscr{L}^{\otimes n} = N_{X'/X}(\mathscr{L}'^{\otimes n})$, it then suffices to choose $f = N_{X'/X}(f')$: in fact, we have $X - X_f = g(X' - X'_{f'})$ by Corollary 23.6.29, so $x \in X_f \subseteq U$. □

Corollary 23.6.32. *Under the hypotheses of Proposition 23.6.31, for an invertible $\mathscr{O}_X$-module $\mathscr{L}$ to be ample relative to f, it is necessary and sufficient that $\mathscr{L}' = g^*(\mathscr{L})$ is ample relative to $f \circ g$.*

Proof. This condition is necessary, since g is affine (Proposition 23.5.9). To see the sufficiency, we can assume that Y is affine, so X and X' are quasi-compact and $\mathscr{L}'$ is ample (Corollary 23.4.37). Now the set of points $x \in X$ such that there is a neighborhood of x over which $g_*(\mathscr{O}_{X'})$ (resp. $g_*(\mathscr{O}_{X'}) \otimes_{\mathscr{O}_X} \mathscr{K}_X$) is of rank n is open and closed in X by hypotheses, so X is a finite sum of such open subschemes (recall that X is quasi-compact), and we can therefore suppose that it is equal to one of them (Proposition 23.4.48). But we then have $N_{X'/X}(\mathscr{L}') = \mathscr{L}^{\otimes n}$, so $\mathscr{L}^{\otimes n}$ is ample in view of Proposition 23.6.31, and $\mathscr{L}$ is therefore ample. □

Corollary 23.6.33. *Under the hypotheses of Proposition 23.6.31, suppose moreover that $f : X \to Y$ is of finite type. Then, for f to be quasi-projective, it is necessary and sufficient that $f \circ g$ is quasi-projective. If we suppose that Y is quasi-compact and quasi-compact, then, for f to be projective, it is necessary and sufficient that $f \circ g$ is projective.*

Proof. The hypotheses implies that $f \circ g$ is of finite type. By the definition of quasi-projective morphisms, the first assertion then follows from Proposition 23.6.31 and Corollary 23.6.32. In view of this result and Theorem 23.5.24, it remains to prove that if f is quasi-projective, then for f to be proper, it is necessary and sufficient that $f \circ g$ is proper. But f is then separated and of fintie type, and as g is surjective, this follows from Corollary 23.5.18(ii). □

Corollary 23.6.34. *Let X be a scheme of finite type over a field K and K' be finite extension of K. For X to be projective (resp. quasi-projective) over K, it is necessary and sufficient that $X' \otimes_K K'$ is projective (resp. quasi-projective) over K'.*

Proof. This condition is necessary by Proposition 23.5.15(iii) and Proposition 23.5.25(iii). Conversely, suppose that X' is projective (resp. quasi-projective), and let $g : X' \to X$ be the canonical projective. Since K' is finite over K, it is clear that g is a finite morphism by Proposition 23.6.3 and is surjective (Proposition 22.3.26). Moreover, $g_*(\mathscr{O}_{X'})$ is a locally free $\mathscr{O}_X$-module, being isomorphic to $\mathscr{O}_X \otimes_K K'$ (Corollary 23.1.30). It then follows from the hypotheses and Corollary 23.6.8 and Proposition 23.5.25(ii) that X' is projective (resp. quasi-projective) over K. We then deduce from Corollary 23.6.33 that X is projective (resp. quasi-projective) over K. □

Remark 23.6.3. In fact, later we will see that the statement of Corollary 23.6.34 is valid for arbitrary extension K' of K.

The end of this subsection is devoted to the proof of the criterion in Proposition 23.6.39, which is a refinement of the techniques we have currently used.

Lemma 23.6.35. *Let X be a reduced Noetherian scheme and $\mathscr{E}$ be a coherent $\mathscr{O}_X$-module such that $\mathscr{E} \otimes_{\mathscr{O}_X} \mathscr{K}_X$ is locally free of rank n. Then there exists a reduced Noetherian scheme Z and a birational and finite morphism $h : Z \to X$ such that the homomorphisms $\sigma_i : \mathscr{H}om_{\mathscr{O}_X}(\mathscr{E}, \mathscr{E}) \to \mathscr{K}_X$ send $\mathscr{H}om_{\mathscr{O}_X}(\mathscr{E}, \mathscr{E})$ into the coherent $\mathscr{O}_X$-algebra $h_*(\mathscr{O}_Z)$.*

Corollary 23.6.36. *Under the hypotheses of Lemma 23.6.35, let W be an open subset of X such that for any $x \in W$, either X is normal at x or $\mathscr{E}_x$ is a free $\mathscr{O}_{X,x}$-module. Then we can choose h so that the restriction of h to $h^{-1}(W)$ is an isomorphism $h^{-1}(W) \cong W$.*

Proof. In fact, the hypotheses imply that if $U \subseteq W$ is an affine open subset, we have, in the notations of Lemma 23.6.35, that $(\sigma_i(u))_x \in A_x$ for any $x \in U$ (Proposition 23.6.24), hence $\sigma_i(u) \in A$, and the conclusion follows from the definition of h given in Lemma 23.6.35. □

Proof. Let X be a reduced Noetherian scheme, $g : X' \to X$ be a finite and surjective morphism such that $\mathscr{B} = g_*(\mathscr{O}_{X'})$ is a coherent $\mathscr{O}_X$-module. Suppose that $\mathscr{B} \otimes_{\mathscr{O}_X} \mathscr{K}_X$ is locally free of rank n. Then we can apply Lemma 23.6.35 on $\mathscr{E} = \mathscr{B}$, with the same notations, to obtain a homomorphism $\sigma_n : \mathscr{H}om_{\mathscr{O}_X}(\mathscr{B}, \mathscr{B}) \to h_*(\mathscr{O}_Z)$, and by composing with the canonical injection $\mathscr{B} \to \mathscr{H}om_{\mathscr{O}_X}(\mathscr{B}, \mathscr{B})$, we obtain a homomorphism of sheaves of multiplicative monoids:

$$\widetilde{N} : \mathscr{B} = g_*(\mathscr{O}_{X'}) \to h_*(\mathscr{O}_Z) = \mathscr{C}. \tag{6.6.1}$$

For any invertible $\mathscr{O}_{X'}$-module $\mathscr{L}'$, $g_*(\mathscr{L}')$ is an invertible $\mathscr{B}$-module by Proposition 23.6.10, and using the same method, we can define an invertible $\mathscr{C}$-module $\widetilde{N}(g_*(\mathscr{L}'))$, which is functorial on $\mathscr{L}'$. □

Lemma 23.6.37. *Let X be a reduced Noetherian scheme, $g : X' \to X$ be a finite and surjective morphism such that $g * (\mathscr{O}_{X'}) \otimes_{\mathscr{O}_X} \mathscr{K}_X$ is locally free of rank n. Then there exists a reduced Noetherian scheme Z and a finite and birational morphism $h : Z \to X$ such that for any ample $\mathscr{O}_X$-module $\mathscr{L}'$, the invertible $\mathscr{O}_Z$-module $\mathscr{M}$ such that $h_*(\mathscr{M}) = \widetilde{N}(g_*(\mathscr{L}'))$ is ample.*

Corollary 23.6.38. *Under the hypotheses of Lemma 23.6.37, for any invertible $\mathscr{O}_X$-module $\mathscr{L}$ such that $g^*(\mathscr{L})$ is ample, $h^*(\mathscr{L})$ is ample.*

Proposition 23.6.39. *Let Y be an affine scheme, X be a reduced Noetherian scheme, $f : X \to Y$ be a quasi-compact morphism, and $g : X' \to X$ be a finite and surjective morphism. Let W be an open subset of X such that, for any $x \in W$, either X is normal at x, or there exists an open neighborhood $T \subseteq W$ of x such that $(g_*(\mathscr{O}_{X'}))|_T$ is a locally free $(\mathscr{O}_X|_T)$-module. Then there exists a reduced Y-scheme Z and a finite and birational Y-morphism $h : Z \to X$ such that the restriction of h to $h^{-1}(W)$ is an isomorphism $h^{-1}(W) \cong W$ and satisfies the following property: for any invertible $\mathscr{O}_X$-module such that $g^*(\mathscr{L})$ is ample relative to $f \circ g$, $h^*(\mathscr{L})$ is ample relative to $f \circ h$.*

Corollary 23.6.40. *If in Proposition 23.6.39 we have $W = X$, then for an invertible $\mathscr{O}_X$-module $\mathscr{L}$ to be ample relative to f, it is necessary and sufficient that $g^*(\mathscr{L})$ is ample relative to $f \circ g$.*

Remark 23.6.4. We shall see in Chapter 24 that if Y is Noetherian, f is of finite type, and if the restriction of f to the reduced closed subscheme of X having $X - W$ as underlying space is proper, then the conclusion of Corollary 23.6.40 is still valid. But we will also give examples of algebraic schemes X over a field K (the structural morphism $X \to \mathrm{Spec}(K)$ not being proper) whose normalize X' is quasi-affine, but which is not quasi-affine (so that $\mathscr{O}_X$ is not ample, although $\mathscr{O}_{X'}$ is, cf. Proposition 23.5.1, and that the morphism $g : X' \to X$ is finite and surjective (c.f. Remark 23.6.2)). We will also see that this circumstance cannot occur when we replace "quasi-affine" by "affine" (by Chevalley's theorem).

23.6.7 Chevally's theorem

Lemma 23.6.41. *Let X, Y be integral Noetherian schemes, x (resp. y) be the generic point of X (resp. Y), and $f : X \to Y$ be a finite and surjective morphism. Let $\mathscr{L}$ be an invertible $\mathscr{O}_X$-module such that*

there exists an affine neighborhood U of y and a section $s \in \Gamma(X, \mathscr{L})$ such that $x \in X_s \subseteq f^{-1}(U)$. Then there exist integers $m, n > 0$, a homomorphism $u : \mathscr{O}_Y^m \to f_*(\mathscr{L}^{\otimes n})$ and an open neighborhood V of y such that the restriction $u|_V$ is an isomorphism $\mathscr{O}_Y^m|_V \xrightarrow{\sim} f_*(\mathscr{L}^{\otimes n})|_V$.

Theorem 23.6.42 (Chevalley). *Let X be an affine scheme, Y be a Noetherian scheme, and $f : X \to Y$ be a finite and surjective morphism. Then Y is an affine scheme.*

Proof. It is clear that $f_{\mathrm{red}} : X_{\mathrm{red}} \to Y_{\mathrm{red}}$ is fiite (Proposition 23.6.3(vi)); as X_{red} is an affine scheme, and Y is affine if and only if Y_{red} is (Corollary 22.4.34), we can assume that X, Y are reduced. For any closed subset Y' of Y, there is then a unique reduced subscheme subscheme structure on Y' whose inverse image $f^{-1}(Y')$, canonically isomorphic to $X \times_Y Y'$, is affine as a closed subscheme of X, and the restriction of f to $f^{-1}(Y')$, which is identified with $f \times_Y 1_{Y'}$, is a finite and surjective morphism (Proposition 22.3.26 and Proposition 23.6.3(iv)). In view of the Noetherian induction principle (Lemma 4.1.17), we are then (in view of Corollary 22.4.34) reduced to prove the theorem under the hypothesis that for any closed subset $Y' \neq Y$, any closed subscheme of Y with underlying space Y' is affine. With this hypothesis, we first note that, for any coherent $\mathscr{O}_Y$-module $\mathscr{F}$ whose support (closed) Z is distinct from Y, we have $H^1(Y, \mathscr{F}) = 0$. In fact, there exists a closed subscheme structure on Z such that, if $j : Z \to Y$ is the canonical injection, we have $\mathscr{F} = j_*(j^*(\mathscr{F}))$ (Corollary 22.6.18 and Theorem 22.1.29), and therefore $H^1(Y, \mathscr{F}) = H^1(Z, j^*(\mathscr{F})) = 0$ (Corollary 23.5.12, since j is affine).

Suppose first that Y is not irreducible, and let Y' be an irreducible component of Y; we endow Y' with the reduced subscheme structure, and let $j : Y' \to Y$ be the canonical injection. Let $\mathscr{F}$ be a coherent $\mathscr{O}_Y$-module, and consider the canonical homomorphism

$$\rho : \mathscr{F} \to \mathscr{F}' = j_*(j^*(\mathscr{F}));$$

Since j is proper and Y', Y are Noetherian schemes, $\mathscr{F}'$ is a coherent $\mathscr{O}_Y$-module by Proposition 19.4.26 (since we have $j_*(\mathscr{O}_{Y'}) = \mathscr{O}_Y/\mathscr{I}$, where $\mathscr{I}$ is the quasi-coherent ideal of $\mathscr{O}_Y$ defining the subscheme Y'), so $\mathscr{G} = \ker \rho$ and $\mathscr{K} = \operatorname{im} \rho$ are coherent $\mathscr{O}_Y$-modules (Proposition 19.4.18). On the other hand, by definition the fiber $\mathscr{F}'_y$ of $\mathscr{F}'$ at the generic point y of Y' is equal to $\mathscr{F}_y/\mathscr{I}_y\mathscr{F}_y$, and hence to $\mathscr{F}_y$ (Example 22.4.43), so y is not contained in the support of $\mathscr{G}$ and we conclude that $H^1(Y, \mathscr{G}) = 0$. Since the support of $\mathscr{F}'$ (and a fortiori that of $\mathscr{K}$) is contained in Y', it is distinct from Y, and we also conclude that $H^1(Y, \mathscr{K}) = 0$. From the exact sequence $0 \to \mathscr{G} \to \mathscr{F} \to \mathscr{K} \to 0$ we then get $H^1(Y, \mathscr{F}) = 0$, so by Serre's criterion Y is then affine.

Suppose now that Y is irreducible, and therefore integral. We can also assume that X is integral: in fact, if we denote by X_i the reduced closed subschemes of X with underlying spaces the irreducible components of X and by $f_i : X_i \to Y$ the restriction of f to X_i, then one of f_i is dominant (Y is irreducible, so if its generic point is contained in the image of f_i, then f_i is dominant, and we note that f is surjective), and as there are finite morphisms (Proposition 23.6.3), it is surjective (Proposition 23.6.7); as X_i is an affine scheme, we see that we can replace X by X_i. In this case, we can apply Lemma 23.6.41 to $\mathscr{L} = \mathscr{O}_X$, since X is affine, to obtain a homomorphism $u : \mathscr{O}_Y^m \to f_*(\mathscr{L}) = \mathscr{B}$ and an open neighborhood V of y such that $u|_V$ is an isomorphism. In view of Serre's criterion, it suffices to prove that for any coherent $\mathscr{O}_Y$-module $\mathscr{F}$ such that $\mathscr{F} \subseteq \mathscr{O}_Y$, we have $H^1(Y, \mathscr{F}) = 0$. We note that then $\mathscr{F}$ is torsion free since Y is integral, and we only need to show that $H^1(Y, \mathscr{F}) = 0$ for any torsion free coherent

$\mathscr{O}_Y$-module $\mathscr{F}$. Now the homomorphism u defines a homomorphism

$$v : \mathscr{G} = \mathscr{H}om_{\mathscr{O}_Y}(\mathscr{B}, \mathscr{F}) \to \mathscr{H}om_{\mathscr{O}_Y}(\mathscr{O}_Y^m, \mathscr{F}) = \mathscr{F}^m.$$

By hypotheses the support of $\mathscr{T} = \operatorname{coker} u$ does not meet V, so is a torsion $\mathscr{O}_Y$-module (Proposition 22.7.27). From the exact sequence $\mathscr{O}_Y^m \to \mathscr{B} \to \mathscr{T} \to 0$ induces, by the left exactness of $\mathscr{H}om_{\mathscr{O}_Y}$, an exact sequence

$$0 \longrightarrow \mathscr{H}om_{\mathscr{O}_Y}(\mathscr{T}, \mathscr{F}) \longrightarrow \mathscr{G} \xrightarrow{v} \mathscr{F}^m$$

But as $\mathscr{F}$ is torsion free and $\mathscr{T}$ is torsion, we have $\mathscr{H}om_{\mathscr{O}_Y}(\mathscr{T}, \mathscr{F}) = 0$, so v is injective. We then obtain an exact sequence

$$0 \longrightarrow \mathscr{G} \longrightarrow \mathscr{F}^m \longrightarrow \operatorname{coker} v \longrightarrow 0$$

where $\mathscr{G}$ and $\operatorname{coker} v$ are coherent $\mathscr{O}_Y$-modules (Proposition 19.4.18). In view of the exact sequence on cohomology, it suffices to prove that $H^1(Y, \mathscr{F}) = H^1(Y, \operatorname{coker} v) = 0$ since this implies $H^1(Y, \mathscr{F}^m) = (H^1(Y, \mathscr{F}))^m = 0$, so $H^1(Y, \mathscr{F}) = 0$. Now the restriction $v|_V$ is an isomorphism, so the support of $\operatorname{coker} v$ is distinct from Y, and we have $H^1(Y, \operatorname{coker} v) = 0$ by our hypothesis. On the other hand, $\mathscr{G}$ is a coherent $\mathscr{B}$-module by Corollary 22.2.28; as X is affine over Y, there exists a quasi-coherent $\mathscr{O}_X$-module $\mathscr{K}$ such that $\mathscr{G}$ is isomorphic to $f_*(\mathscr{K})$ (Proposition 23.1.18), and since $H^1(X, \mathscr{K}) = 0$ (X is affine), we then have $H^1(Y, \mathscr{G}) = 0$ by Corollary 22.6.18, which completes the proof. □

Corollary 23.6.43. *Let X be a Noetherian scheme and $(X_i)_{1 \le i \le n}$ be a finite covering of X by closed subsets. Then for X to be affine, it is necessary and sufficient that for each i, there exists a closed subscheme of X that is affine and has underlying space X_i.*

Proof. Let X' be the sum of the X_i, then it is clear that X' is affine if each X_i is affine, and we have a surjective morphism $f : X' \to X$ whose restriction to X_i is the canonical injection. To apply Theorem 23.6.42, it remains to verifying that f is finite, and this follows from Proposition 23.6.3(i). □

23.7 Valuative criterion

In this section we give the valuative criterion of sparation and properness of a morphis, which are criteria which involve a auxiliary scheme $\operatorname{Spec}(A)$, where A is a valuation ring. With a convenient "Noetherian" hypothesis, these criterion can be refined to the case where A is a discrete valuation ring, and this will probably be the only case that we will apply later.

23.7.1 Remainders for valuation rings

Among the vast properties that characterize valuation rings, we shall use the following one: a ring A is called a valuation ring if it is an integral domain which is not a field, and if in the set of proper local rinng contained in the fraction field K of A, A is maximal under the dominant relation. Recall that a valuation ring is integrally closed. If A is a valuation ring, then $A_{\mathfrak{p}}$ is also a valuation ring for any nonzero prime ideal $\mathfrak{p} \neq 0$.

Let K be a field, A be a proper local subring of K; then there exists a valuation ring of K dominating A (Theorem 14.1.7). On the other hand, let B be a valuation ring, k be its residue field, and K be the fraction field, L be an extension of k. Then there exists a complete valuation ring C dominating B with residue field equals to L. In fat, L is an algebraic extension of a purely transcendental extension $L' = k(T_\mu)_{\mu\in M}$; we can extend the valuation of K corresponding to B to a valuation of $K' = K(T_\mu)_{\mu\in M}$ with residue field L'; replace B by this complete valuation ring C, we can assume then that B is complete that L is an algebraic closure of k. If $\overline{K}$ is an algebraic closure of K, we can then extend the defining valuation of B to $\overline{K}$, and the corresponding residue field is an algebraic closure of k, as can be seen by lifting the coefficients of a monic polynomial of $k[T]$ to $\overline{K}$. We are therefore finally reduced to the case where $L = k$ and it suffices then to take for C the completion of B to answer the question.

Let K be a field and A be a subring of K; the integral closure A' of A in K is the intersection of valuation rings of the fraction field of A containing A (Theorem 14.1.8). The preceding argument then have the following geometric form:

Proposition 23.7.1. *Let Y be a scheme, $p : X \to Y$ be a morphism, x be a point of X, $y = p(x)$, and $y' \neq y$ be a specialization of y. Then there exists a local scheme Y', which is the specturm of a valuation ring, and a separated morphism $f : Y' \to Y$ such that, if a is the unique closed point of Y' and b is the generic point of Y', we have $f(a) = y'$ and $f(b) = y$. We can moreover suppose that one of the following additional conditions are satisfied:*

(i) Y' is the specturm of a complete valuation ring whose residue field is algebraically closed, and there exists a $\kappa(y)$-homomorphism $\kappa(x) \to \kappa(b)$.

(ii) There exists a $\kappa(y)$-isomorphism $\kappa(x) \cong \kappa(b)$.

Proof. Let Y_1 be the reduced closed subscheme of Y with $\overline{\{y\}}$ as underlying space, and X_1 be the closed subscheme $p^{-1}(Y_1)$; as $y' \in \overline{\{y\}}$ by hypothesis and $\kappa(x)$ is the same for X and X_1, by replacing Y with Y_1 and X with X_1, we can suppose that Y is integral with generic point y; $\mathscr{O}_{Y,y'}$ is then an integral local ring which is not a field, whose fraction field is $\mathscr{O}_{Y,y} = \kappa(y)$, and $\kappa(x)$ is an extension of $\kappa(y)$. To realize the conditions $f(a) = y'$ and $f(b) = y$ with the additional condition (i) (resp. (ii)), we choose $Y' = \operatorname{Spec}(A')$, where A' is a valuation ring dominating $\mathscr{O}_{Y,y'}$ and which is complete and with residue field an algebraically closed extension of $\kappa(x)$ (resp. a valuation ring dominating $\mathscr{O}_{Y,y'}$ with fraction field $\kappa(x)$); the existence of such rings are proved by the above remarks. □

Recall that a local ring $(A, \mathfrak{m})$ is of dimension if and only if any prime ideal of A distinct from $\mathfrak{m}$ is minimal; if A is integral, this means $\mathfrak{m}$ and (0) are the only prime ideals, and $\mathfrak{m} \neq (0)$; equivalent, $Y = \operatorname{Spec}(A)$ is reduced to two points a, b: a is the closed point, $\mathfrak{p}_a = \mathfrak{m}$, and $\kappa(a) = k$ is the residue field $A/\mathfrak{m}$; b is the generic point of Y, $\mathfrak{p}_b = (0)$, the set $\{b\}$ is the unique nontrivial open subset of Y, and $\kappa(b) = K$ is the fraction field of A. For an integral Noetherian local ring A of dimension 1, the following conditions are then equivalent:

(i) A is normal;

(ii) A is regular;

(iii) A is a valuation ring.

Moreover, if these are ture, A is then a discrete valuation ring.

Proposition 23.7.2. *Let A be a Noetherian local integral domain which is not a field, K be its fraction field, L be a extension of K of finite type. There then exists a discrete valuation ring of L dominating A.*

Proof. □

Corollary 23.7.3. *Let A be an integral Noetherian ring, K be its fraction field, and L be an extension of K of finite type. Then the integral closure of A in L is the intersection of discrete valuation rings of L containing A.*

Proposition 23.7.4. *Let Y be a locally Noetherian scheme, $p : X \to Y$ be a morphism locally of finite type, x be a point of X, $y = p(x)$, $y' \neq y$ be a specialization of y. Then there exists a local scheme Y', which is a specturm of a discrete valuation ring, and a separated morphism $f : Y' \to Y$ and rational Y-map $g : Y' \dashrightarrow X$ such that, if a is the closed point of Y' and b is the generic point, we have $f(a) = y'$, $f(b) = y$, $g(b) = x$, and in the following commutative diagram*

$$\begin{tikzcd} & \kappa(x) \\ \kappa(b) \arrow[ur, "\gamma"] & \kappa(y) \arrow[l, "\varphi"] \arrow[u, "\pi"'] \end{tikzcd}$$

(whee π, φ, γ are the homomorphisms corresponding to p, f and g), γ is a bijection.

Proof. □

23.7.2 Valuative criterion of separation

Proposition 23.7.5 (Valuative Criterion of Separation). *Let Y be a scheme (resp. a locally Noetherian scheme), $f : X \to Y$ be a morphism (resp. a morphism locally of finite type). The following conditions are equivalent:*

(i) f is separated.

(ii) f is quasi-separated and for any Y-scheme of the form $Y' = \mathrm{Spec}(A)$, where A is a valuation ring (resp. a discrete valuation ring), two Y-morphisms of Y' to X which coincide at the generic point of Y' are equal.

(iii) f is quasi-seaprated and for any Y-scheme of the form $Y' = \mathrm{Spec}(A)$, where A is a valuation ring (resp. a discrete valuation ring), two Y'-sections of $X' = X_{(Y')}$ which coincide at the generic point of Y' are equal.

Proof. The equivalence of (ii) and (iii) follows from the correspondence of Y-morphisms $Y' \to X$ and Y'-sections of X'. If X is separated over Y, condition (ii) follows from the proof of Proposition 22.7.10, since Y' is integral. It then remains to prove that condition (ii) implies that the diagonal morphism $\Delta : X \to X \times_Y X$ is closed, and for this we can use Proposition 22.6.6. Now, let z be a point of the diagonal $\Delta(X)$, $z' \neq z$ be a specialization of z in $X \times_Y X$. Then there exists by Proposition 23.7.1 a valuation ring A and a morphism $g : Y' \to X \times_Y X$ such that $g(a) = z'$, $g(b) = z$ (with the notations of Proposition 23.7.1, a is the closed point of Y' and b is the generic point of Y'); this morphism makes Y' an $(X \times_Y X)$-scheme, and a fortiori a

Y-scheme. If we compose g with the two projections of $X \times_Y X$, we obtain two Y-morphisms $g_1, g_2 : Y' \to X$, which by hypotheses send the point b to the same point in X; in view of (ii), these two morphisms coincide with a morphism $h : Y' \to X$, which signifies that g factors into $g = \Delta \circ h$, and therefore $z' \in \Delta(X)$. If we suppose that Y is locally Noetherian and f is of finite type, $X \times_Y X$ is locally Noetherian by Corollary 22.6.22, and we can therefore replace Proposition 22.7.10 by Proposition 23.7.4. □

The condition (ii) of Proposition 23.7.5 signifies that if $Y' = \operatorname{Spec}(A)$ and $X' = \operatorname{Spec}(K)$ where K is the fraction field of A, the canonical map

$$\operatorname{Hom}_Y(Y', X) \to \operatorname{Hom}_Y(X', X)$$

is injective. Equivalently, this means in the following diagram

$$\begin{tikzcd} X' \arrow[r] \arrow[d] & X \arrow[d, "f"] \\ Y' \arrow[r] \arrow[ur, dashed] & Y \end{tikzcd}$$

the dashed morphism $Y' \to X$, if exists, is necessarily unique.

Remark 23.7.1. In the criterion (ii) of Proposition 23.7.5, we can restrict ourselves to valuation rings A which is complete whose residue field is algebraically closed; this follows from the additional condition (i) of Proposition 22.7.10.

23.7.3 Valuative criterion of properness

Proposition 23.7.6. *Let A be a valuation ring, $Y = \operatorname{Spec}(A)$, b be the generic point of Y. Let X be an integral and separated scheme and $f : X \to Y$ be a closed morphism such that $f^{-1}(b)$ is reduced to a point x and the corresponding homomorphism $\kappa(b) \to \kappa(x)$ is bijective. Then f is an isomorphism.*

Proof. As f is closed and dominant, we have $f(X) = Y$; it then suffices to prove that for any $y' \neq b$ in Y, there exists a unique point x' such that $f(x') = y'$ and the corresponding homomorphism $\mathscr{O}_{Y,y'} \to \mathscr{O}_{X,x'}$ is bijective, because f is then a homeomorphism. Now, if $f(x') = y'$, $\mathscr{O}_{X,x'}$ is a local ring contained in $K = \kappa(x) = \kappa(y)$ and dominates $\mathscr{O}_{Y,y'}$; the later is the local ring $A_{y'}$, which a valuation ring for the fraction field K of A. But $\mathscr{O}_{X,x'} \neq K$ since x' is not the generic point of X, and we then conclude that $\mathscr{O}_{X,x'} = \mathscr{O}_{Y,y'}$ by maximality. As X is an integral scheme, the relation $\mathscr{O}_{X,x'} = \mathscr{O}_{X,x''}$ implies $x' = x''$ by Proposition 22.7.31, which proves our claim. □

Let A be a valuation ring, $Y = \operatorname{Spec}(A)$, b the generic point of Y, so that $\mathscr{O}_{Y,b} = \kappa(b)$ is equal to the fraction field K of A. Let $f : X \to Y$ be a morphism. We have seen that the rational Y-sections of X correspond to the germs of Y-sections (defined over a neighborhood of b) at b, whence a canonical map

$$\Gamma_{\mathrm{rat}}(X/Y) \to \Gamma(f^{-1}(b)/\operatorname{Spec}(K)) \tag{7.3.1}$$

where the elements of $\Gamma(f^{-1}(b)/\operatorname{Spec}(K))$ are identified with the rational points of $f^{-1}(b) = X \otimes_A K$ over K. If f is separted, it then follows from Corollary 22.5.21 that the map of (7.3.1) is injective, since Y is integral.

Composing (7.3.1) with the canonical map $\Gamma(X/Y) \to \Gamma_{\mathrm{rat}}(X/Y)$, we then obtain a canonical map

$$\Gamma(X/Y) \to \Gamma(f^{-1}(b)/\mathrm{Spec}(K)). \tag{7.3.2}$$

If f is separated, this map is injective by Corollary 22.5.21.

Proposition 23.7.7. *Let A be a valuation ring with fraction field K, $Y = \mathrm{Spec}(A)$, b be the generic point of Y, and $f : X \to Y$ be a separated and closed morphism. Then the canonical map (7.3.2) is bijective.*

Proof. Let x be a rational point of $f^{-1}(b)$ over K. As f is separated, so is the morphism $f^{-1}(b) \to \mathrm{Spec}(K)$ corresponding to f (Proposition 22.5.25(iv)), since and any section of $f^{-1}(b)$ a closed immersion by Corollary 22.5.19, $\{x\}$ is closed in $f^{-1}(b)$. Consider the reduced closed subscheme X' of X with underlying space $\overline{\{x\}}$ of $\{x\}$ in X. It is clear that the restriction of f to X' satisfies the conditions of Proposition 23.7.6 (note that since x is rational over K, we have $\kappa(x) = K$), hence an isomorphism from X' to Y, whose inverse isomorphism is the Y-section of X we want. □

Recall that if F is a subset of the scheme Y, the codimension of F in Y equal to the infimum of $\dim(\mathscr{O}_{Y,z})$ where $z \in F$ (this can be easily verified after reducing to affine case), and we denote this number by $\mathrm{codim}_Y(F)$.

Corollary 23.7.8. *Let Y be a reduced locally Noetherian scheme such that the subset N of $y \in Y$ where Y is not regular has codimension $\mathrm{codim}_Y(N) \geq 2$. Let $f : X \to Y$ be a separted and closed morphism of finite type and g be a rational Y-section of X. If Y' is the set of points of Y where g is not defined, then $\mathrm{codim}_Y(Y') \geq 2$.*

Proof. It suffices to prove that g is defined at any point $y \in Y$ such that $\dim(\mathscr{O}_{Y,y}) \leq 1$. If $\dim(\mathscr{O}_{Y,y}) = 0$, then y is the generic point of an irreducible component of Y. For any open dense subset V of Y, by restricting to an affine neighborhood of y and apply Proposition 4.1.12, we conclude that V contains y. In particular, y belongs to the defining domain of g. Suppose now that $\dim(\mathscr{O}_{Y,y}) = 1$; then $\mathscr{O}_{Y,y}$ is a regular local ring, hence a discrete valuation ring. Let $Z = \mathrm{Spec}(\mathscr{O}_{Y,y})$; as $U = Y - Y'$ is open and dense, by Corollary 22.2.10 and our preceding arguments, $U \cap Z$ is nonempty (contains the generic of an irreducible component of Y containing y), so we can consider the rational map $g' : Z \dashrightarrow X$ induced by g. It then suffices to prove that g' is a morphism (Proposition 22.7.17). Now, g' can be considered as a rational Z-section of the Z-scheme $f^{-1}(Z) = X \times_Y Z$; it is clear that the morphism $f^{-1}(Z) \to Z$ corresponding to f is closed, and is separted by Proposition 22.5.25(i). We then conclude from Proposition 23.7.7 that g' is everywhere defined, and as Z is reduced and X is separated over Y, g' is a morphism (Proposition 22.7.10). □

Corollary 23.7.9. *Let S be a locally Noetherian scheme, X, Y be S-scheme, and assume that X is proper over X. Suppose that Y is reduced and the subset N of $y \in Y$ where Y is not regular has codimension $\mathrm{codim}_Y(N) \geq 2$. Let $f : Y \dashrightarrow X$ be a rational map and Y' be the set of points where f is not defined, then $\mathrm{codim}_Y(Y') \geq 2$.*

Proof. The rational S-maps $Y \dashrightarrow X$ correspond to rational Y-sections of $X \times_S Y$; as the structural morphism $X \times_S Y \to Y$ is closed by Proposition 23.5.17, we can apply Corollary 23.7.8, whence the corollary. □

Remark 23.7.2. The hypothesis on Y in Corollary 23.7.8 and Corollary 23.7.9 are satisfied in particular if Y is normal (by Serre's criterion for normality).

Theorem 23.7.10 (Valuative Criterion of Properness). *Let Y be a (resp. locally Noetherian) scheme and $f : X \to Y$ be a quasi-compact and separted morphism (resp. a quasi-compact morphism of finite type). The following conditions are equivalent:*

(i) f is universally closed (resp. proper)

(ii) For any Y-scheme $Y' = \operatorname{Spec}(A)$ where A is a valuation ring (resp. a discrete valuation ring) with fraction field K, the canonical map (where $X' = \operatorname{Spec}(K)$)

$$\operatorname{Hom}_Y(Y', X) \to \operatorname{Hom}_Y(\operatorname{Spec}(K), X)$$

corresponding to the cannical injection $A \to K$, is surjective (resp. bijective).

(iii) For any Y-scheme $Y' = \operatorname{Spec}(A)$ where A is a valuation ring (resp. a discrete valuation ring) with fraction field K, the canonical map of (7.3.2) relative to the Y'-scheme $X' = X_{(Y')}$ is surjective (resp. bijective).

Proof. The equivalence of (ii) and (iii) follows from the correspondence of Y-morphisms $Y' \to X$ and Y'-morphisms $Y' \to X'$. If f is universally closed then $f_{(Y')}$ is closed and separated, and it then suffices to apply Proposition 23.7.7. It remains to prove that (ii) implies (i). Consider first the case where Y is arbitrary, f is separated and quasi-compact. If the condition of (ii) is satisfied for f, it is also true for $f_{(Y'')} : X_{(Y'')} \to Y''$, where Y'' is an arbitrary Y-scheme, in view of the equivalent of (ii) and (iii), and the fact that $X_{(Y'')} \times_{Y''} Y' = X \times_Y Y'$ for any morphism $Y' \to Y''$; as $f_{(Y'')}$ is also quasi-compact and separated, we then conclude that we only need to prove (ii) implies f is closed, and for this we shall use Proposition 22.6.6. Let $x \in X$, $y' \neq y$ be a specialization of $y = f(x)$; in view of Proposition 23.7.1, there is a scheme $Y' = \operatorname{Spec}(A)$ where A is a valuation ring, and a separated morphism $g : Y' \to Y$ such that, if a is the closed point and b is the generic point of Y, we have $g(a) = y'$, $g(b) = y$, and there exists a $\kappa(y)$-hommorphism $\kappa(x) \to \kappa(b)$. This homomorphism corresponds to a canonical Y-morphism $\operatorname{Spec}(\kappa(b)) \to X$ (Corollary 22.2.15), and it then follows from condition (ii) that there exists a Y-morphism $h : Y' \to X$ which corresponds the previous morphism such that the following diagram commutes

$$\begin{tikzcd} \operatorname{Spec}(\kappa(b)) \arrow[r] \arrow[d] & X \arrow[d, "f"] \\ \operatorname{Spec}(A) \arrow[r, "g"] & Y \end{tikzcd}$$

We then have $h(b) = x$, and if we put $h(a) = x'$, x' is then a specialization of x, and we have $f(x') = f(h(a)) = g(a) = y'$.

If now Y is locally Noetherian and f is a quasi-compact morphism of finite type, then condition (ii) implies that f is separated (Proposition 23.7.5), so the diagonal morphism $\Delta : X \to X \times_Y X$ is quasi-compact. Moreover, to verify that f is proper, it suffices to show that $f_{(Y'')} : X_{(Y'')} \to Y''$ is closed for any Y-scheme Y'' of finite type (Corollary 23.5.30). As then Y'' is locally Noetherian, we can resume the reasoning given in the first case by taking for Y' the specturm of discrete valuation ring, and applying Proposition 23.7.1 instead of Proposition 23.7.4. □

Remark 23.7.3. We deduce from the criterion (iii) of Theorem 23.7.10 a new proof of the fact that a projective morphism $X \to Y$ is closed, which is closer to classical methods. We can in fact assume that Y is affine, and X is therefore a closed subscheme of a projective bundle $\mathbb{P}^n_Y$ (Corollary 23.5.14). To show that $X \to Y$ is closed, it suffices to verify that the structural morphism $\mathbb{P}^n_Y \to Y$ is closed. The criterion (iii) of Theorem 23.7.10, together with (4.1.1), show that we are reduced to proving the following fact: if Y is the spectrum of a valuation ring A with fraction field K, every point of $\mathbb{P}^n_Y$ with values in K comes (by restriction to the generic point of Y) from a point of $\mathbb{P}^n_Y$ with values in A. Now, any invertible $\mathcal{O}_Y$-module is trivial, so it follows from Example 23.4.7 that a point of $\mathbb{P}^n_Y$ with values in K is identified with a class of elements $(\xi c_0, \xi c_1, \dots, \xi c_n)$ of K^{n+1}, where $\xi \neq 0$ and the c_i are elements of K which generate the unit ideal of K. By multiplying the c_i with an element of A, we can suppose that the c_i belong to A, and generate the unit ideal of A. But then (Example 23.4.7) the system $(c_0, \dots, c_n)$ defines a point of $\mathbb{P}^n_Y$ with values in A, whence our assertion.

Remark 23.7.4. The criteria Proposition 23.7.5 and Theorem 23.7.10 are especially convenient when we consider a Y-scheme X as a functor

$$X(Y') = \mathrm{Hom}_Y(Y', X)$$

where Y' is a Y-scheme. These criteria will allow us, for example, to prove that under certain conditions the "Picard schemas" are proper.

Corollary 23.7.11. *Let Y be a separated integral scheme (resp. a separated integral locally Noetherian scheme) and $f : X \to Y$ be a dominant morphism.*

(a) If f is quasi-compact and universally closed, any valuation ring with fraction field the rational function field $K(X)$ and which dominates a local ring of Y, also dominates a local ring of X.

(b) Conversely, suppose that f is of finite type, and the property of (a) is satisfied for any valuation ring (resp. any discrete valuation ring) with fraction field $K(X)$. Then f is proper.

Proof. Assume the hypotheses of (a) and let $K = K(Y)$, $L = K(X)$, y be a point of Y, A be a valuation ring with L the fraction field and dominate $\mathcal{O}_{Y,y}$. The injection $\mathcal{O}_{Y,y} \to A$ is local, so it defines a morphism

$$h : Y' = \mathrm{Spec}(A) \to \mathrm{Spec}(\mathcal{O}_{Y,y}) \to Y$$

(Proposition 22.2.12) such that $h(a) = y$, where a is the closed point of Y'. Moreover, since $K \subseteq L$, the morphism $\mathrm{Spec}(A) \to \mathrm{Spec}(\mathcal{O}_{Y,y})$ is dominant, so if η is the generic point of Y (which is also that of $\mathrm{Spec}(\mathcal{O}_{Y,y})$), we have $h(b) = \eta$, where b is the generic point of Y'. If ξ is the generic point of X, we have $\kappa(\xi) = \kappa(b) = L$ by hypothesis, so there is a Y-morphism $g : \mathrm{Spec}(L) \to X$ such that $g(b) = \xi$. In view of Theorem 23.7.10, we obtain a Y-morphism $g' : Y' \to X$ such that $g(b) = \xi$. If we set $x = g'(a)$, then A dominates $\mathcal{O}_{X,x}$.

We now prove (b); since the question is local over Y, we can assume that Y is affine (resp. affine and Noetherian). As f is of finite type, we can apply Chow's lemma, so there exists a projective morphism $p : P \to Y$, an immersion $j : X' \to P$, and a projective and surjective

birational morphism $g : X' \to X$ (where X' is integral) such that the diagram

$$\begin{tikzcd} X' \arrow[r, "j"] \arrow[d, "g"'] & P \arrow[d, "\pi"] \\ X \arrow[r, "f"] & Y \end{tikzcd}$$

is commutative. It suffices to prove that j is a closed immersion, because then $f \circ g = p \circ j$ is projective, hence proper, and as g is surjective we conclude that f is proper by Corollary 23.5.18. Let Z be a reduced closed subscheme of P with underlying space $\overline{j(X')}$; as X' is integral, j factors into

$$j : X' \xrightarrow{h} Z \xrightarrow{i} P$$

where $i : Z \to P$ is the canonical injection and $h : X' \to Z$ is a dominant open immersion. Since Z is integral and projective over Y by Proposition 23.5.25, we are then reduced to the case where P is integral, j is dominant and birational, and prove that j is surjective. Now let $z \in P$; $\mathscr{O}_{Z,z}$ is an integral local ring (resp. Noetherian integral) whose fraction field is

$$L = K(P) = K(X') = K(X).$$

We can assume that z is not the generic point of P (since the later is contained in $j(Z)$ as j is dominant), so $\mathscr{O}_{Z,z} \neq L$ and by Theorem 14.1.7 and Proposition 23.7.2, there exists a valuation ring (resp. a discrete valuation ring) A with fraction field L that dominates $\mathscr{O}_{Z,z}$. A fortiori A dominates the local ring $\mathscr{O}_{Y,y}$ where $y = p(z)$, and by hypotheses there is then a point $x \in X$ such that A dominates $\mathscr{O}_{X,x}$. As the morphism g is proper, it satisfies the conditions of (a), so our previous arguments then prove that A also dominates $\mathscr{O}_{X,x'}$, for some $x' \in X'$. Then the local rings $\mathscr{O}_{Z,z}$ and $\mathscr{O}_{Z,j(x')} = \mathscr{O}_{X,x'}$ are related, and by Proposition 22.7.31, as P is separated, we have $z = j(x')$, which completes the proof. □

Corollary 23.7.12. *Let A be an integral domain, $Y = \operatorname{Spec}(A)$, and $f : X \to Y$ be a dominant morphism of integral schemes which is quasi-compact and universally closed. Then $\Gamma(X, \mathscr{O}_X)$ is canonically isomorphic to a subring of the integral closure of A in $K(X)$.*

Proof. Recall that by (7.5.1), $B = \Gamma(X, \mathscr{O}_X)$ is indeitified with the intersection of $\mathscr{O}_{X,x}$ for $x \in X$. If R is a valuation ring of $K(X)$ containing A, then it dominates the local ring $A_{\mathfrak{P}}$ where $\mathfrak{P} = \mathfrak{m}_R \cap B$, and therefore by Corollary 23.7.11 dominates a local ring of X. Then B is contained in R, and the conclusion follows from Theorem 14.1.8. □

Remark 23.7.5. Under the hypothesis of Corollary 23.7.12, if we suppose that $K(X)$ is a finite extension of $K(Y)$, then we can in many cases conclude that $\Gamma(X, \mathscr{O}_X)$ is a finitely generated module over the ring $B = \Gamma(Y, \mathscr{O}_X)$. This is the case for example if B is a Japanese ring. In particular, if $X = \operatorname{Spec}(A)$ and $Y = \operatorname{Spec}(k)$ where k is a algebraically closed field, then the the corresponding homomorphism $k \to A$ is injective by Corollary 10.4.19 and since the integral closure of k in $K(X)$ is equal to k, we conclude that $\Gamma(X, \mathscr{O}_X) = k$.

23.7.4 Algebraic curves

Let k be a field. In this subsection, all schemes are considered to be separated k-schemes of finite type, and any morphism are k-morphism.

Proposition 23.7.13. *Let X be a scheme of finite type over k; let x_i $(1 \leq i \leq n)$ be the generic points of the irreducible components X_i of X, and $K_i = \kappa(x_i)$. Then the following conditions are equivalent:*

(i) For each i, the transcendence degre of K_i over k is equal to 1.

(ii) For any closed point x of X, the local ring $\mathscr{O}_{X,x}$ is of dimension 1.

(iii) The closed irreducible subsets of X distinct from the X_i are closed points of X.

Proof. As X is quasi-compact, any irreducible closed subset F of X contains a closed point (**??**). Let x be a closed point of X; in view of Corollary 22.2.10, there is a correspondence between prime ideals of $\mathscr{O}_{X,x}$ and the irreducible closed subsets of X containing x. The equivalence of (ii) and (iii) then follows. On the other hand, if $\mathfrak{p}_\alpha$ $(1 \leq \alpha \leq r)$ is the minimal prime ideals of the local Noetherian ring $\mathscr{O}_{X,x}$, the local ring $\mathscr{O}_{X,x}/\mathfrak{p}_\alpha$ are integral, whose fraction fields are the K_i such that $x \in X_i$. Moreover, the dimension of a k-algebra of finite type is equal to its transcendental degree over k. Finally, the dimension of $\mathscr{O}_{X,x}$ is the supremum of the $\mathscr{O}_{X,x}/\mathfrak{p}_\alpha$, and a k-algebra of finite type is catenary, so (i) and (ii) are equivalent. □

We note that under the conditions of Proposition 23.7.13, by Proposition 22.6.43 that set X is either empty of finite. We define an algebraic curve over k to be a nonempty scheme X over k satisfying the conditions of Proposition 23.7.13. Equivalently, we will see that this condition is equivalent to that the irreducible components of X has dimension 1. In particular, we note that if X is an algebraic curve over k, the reduced closed subschemes X_i of X with underlying spaces the irreducible components of X are also algebraic curves over k.

Corollary 23.7.14. *Let X be an irreducible algebraic curve. Then the only non-closed point of X is its generic point, the proper closed subsets of X are the finite subsets of X, which are also the non dense subsets of X.*

Proof. If a point $x \in X$ is not closed, then its closure is an irreducible closed subset of X, hence equal to X by Proposition 23.7.13, so x is the generic point of X. A proper closed subset F of X can not contain the generic point of X, so its points are all closed, hence T1, and by Proposition 22.2.30 we conclude that F is finite and discrete. The closure of an infinite subset of X is therefore necessarily equal to X, which proves the last assertion. □

If X is an arbitrary algebraic curve, then by applying Corollary 23.7.14, we conclude that the only non-closed points of X are the generic points of the irreducible components of X.

Corollary 23.7.15. *Let X and Y be irreducible algebraic curves over k and $f : X \to Y$ be a k-morphism. Then for f to be dominant, it is necessary and sufficient that $f^{-1}(y)$ is finite for any $y \in Y$.*

Proof. If f is not dominant, $f(X)$ is necessarily a finite subset of Y by Corollary 23.7.14, so it is not possible that $f^{-1}(y)$ is finite for any $y \in Y$ (since X is an infinite set). Conversely, if f is dominant, for any $y \in Y$ which is not the generic point η of Y, $f^{-1}(y)$ is closed in X since $\{y\}$ is closed in Y (Corollary 23.7.14); on the other hand, by hypotheses, $f^{-1}(y)$ does not contain the generic point of X, so is finite by Corollary 23.7.14. Finally, to see that $f^{-1}(\eta)$ is finite, we note that the morphism f is of finite type by Corollary 22.6.37, so the fiber $f^{-1}(\eta)$ is an irreducible scheme of finite type over $\kappa(\eta)$ with generic point ξ (Proposition 22.6.35). As $\kappa(\xi)$ and $\kappa(\eta)$ are extensions of k of finite type with transcendental degree 1, it follows that $\kappa(\xi)$ is a finite extension of $\kappa(\eta)$, so ξ is closed in $f^{-1}(\eta)$ by Corollary 23.6.5, and $f^{-1}(\eta)$ is therefore reduced to a point ξ. □

Remark 23.7.6. We will see later that a proper morphism $f : X \to Y$ of Noetherian schemes, such that $f^{-1}(y)$ is finite for any $y \in Y$, is necessarily finite. It then follows from Corollary 23.7.14 that such a dominant proper morphism of irreducible algebraic curves is finite.

Corollary 23.7.16. *Let X be an algebraic curve over k. For X to be regular, it is necessary and sufficient that X is normal, or the local ring of its closed points are discrete valuation rings.*

Proof. This comes from conditions (ii) of Proposition 23.7.13. □

Corollary 23.7.17. *Let X be a reduced algebraic curve, $\mathscr{A}$ be a reduced coherent $\mathscr{K}_X$-algebra. Then the integral closure X' of X relative to $\mathscr{A}$ is a normal algebraic curve, and the canonical morphism $X' \to X$ is finite.*

Proof. The fact that $X' \to X$ is finite follows from Remark 23.6.2, and X' is then a normal algebraic scheme over k. Moreover, we note that if X is irreducible with generic point ξ and its integral closure X' has generic point ξ', then $\kappa(\xi') = \kappa(\xi)$ by Corollary 23.6.23, so X' is also an algebraic curve over k. □

Corollary 23.7.18. *For a reduced algebraic curve X to be proper over k (which is called **complete**), it is necessary and sufficient that the normalization X' of X is proper over k.*

Proof. The canonical morphism $f : X' \to X$ is finite by Corollary 23.7.17, hence proper (Corollary 23.6.8) and surjective (Corollary 23.6.23). If $g : X \to \operatorname{Spec}(k)$ is the structural morphism, g and $g \circ f$ are then simultaneously proper, in view of Proposition 23.5.17 and Corollary 23.5.18. □

Proposition 23.7.19. *Let X be a normal algebraic curve over k and Y be a proper algebraic scheme over k. Then any rational k-map $f : X \dashrightarrow Y$ is everywhere defined, hence a morphism.*

Proof. It follows from Corollary 23.7.9 that the set of points $x \in X$ where this rational map is not defined, the dimnesion of $\mathscr{O}_{X,x}$ is ≥ 2, hence is empty. The assertion then follows from Proposition 22.7.10. □

Corollary 23.7.20. *A normal algebraic curve over k is quasi-projective over k.*

Proof. As X is the sum of finitely many integral and normal algerbaic curves (Corollary 23.6.23), we can assume that X is integral (Corollary 23.5.16). As X is quasi-compact, it can be covered by finitely many affine opens U_i ($1 \leq i \leq n$), and as each of this is of finite type over k, there exists an integer n_i and a k-immersion $f_i : U_i \to \mathbb{P}^{n_i}_k$ (Corollary 23.5.14 and Proposition 23.5.15(i)). As U_i is dense in X (recall that X is integral by our assumption), it follows from Proposition 23.7.19 that f_i extends to a k-morphism $g_i : X \to \mathbb{P}^{n_i}_k$, and we obtain a k-morphism $g = (g_1, \ldots, g_n)_k$ from X into the product P of the $\mathbb{P}^{n_i}_k$ over k. Moreover, for each index i, as the restriction of g_i to U_i is an immersion, so is the restriction of g to U_i (Corollary 22.5.16). As the U_i cover X and g is separated by Proposition 22.5.25(v), g is an immersion from X into P by Proposition 22.7.36. The Segre morphism then provides from g an immersion of X into a projective bundle $\mathbb{P}^n_k$, so X is quasi-projective. □

Corollary 23.7.21. *A normal algebraic curve X is isomorphic to a dense open subscheme of a normal and complete algebraic curve $\widehat{X}$, determined up to isomorphisms.*

Proof. If X_1, X_2 are two normal and complete algebraic curves containing X as open dense subscheme, it follows from Proposition 23.7.19 there is an isomorphism of X_1 and X_2, whence the uniqueness of $\widehat{X}$. To prove the existence of $\widehat{X}$, it suffices to remark that we can consider X as a subscheme of a projective bundle $\mathbb{P}^n_k$ (Corollary 23.7.20). Let $\overline{X}$ be the scheme-theoretic closure of X in $\mathbb{P}^n_k$ (Proposition 22.6.68); as X is an open and dense subscheme of $\overline{X}$, the generic points x_i of the irreducible components of X are those of $\overline{X}$, and the residue fields $\kappa(x_i)$ are the same for both schemes, so $\overline{X}$ is an algebraic curve over k, which is reduced (Proposition 22.6.66) and projective over k (Proposition 23.2.50), hence complete by Theorem 23.5.24. We then take $\widehat{X}$ to be the noramlization of $\overline{X}$, which is complete by Corollary 23.7.18. If $h : \widehat{X} \to \overline{X}$ is the canonical morphism, the restriction of h to $h^{-1}(X)$ is an isomorphism since X is normal (Proposition 23.6.21), and as $h^{-1}(X)$ contains the generic point of the irreducible components of $\widehat{X}$ (Corollary 23.6.23), it is therefore dense in $\widehat{X}$, which proves the assertion. □

Remark 23.7.7. We will later see that the conclusion of Corollary 23.7.21 is still valid without assuming the algebraic curve to be normal (or even reduced); we will also see that for an algebraic curve (reduced or not) to be affine, it is necessary and sufficient that its irreducible (reduced) components are not complete.

Corollary 23.7.22. *Let X be an irreducible normal algebraic curve with $L = K(X)$, Y be a complete and integral algebraic curve with $K = K(Y)$. Then there exists a canonical correspondence between dominant k-morphisms $X \to Y$ and k-monomorphisms $K \to L$.*

Proof. By Proposition 23.7.19, the rational k-maps $X \dashleftarrow Y$ are identified with k-morphisms $f : X \to Y$. The morphism f is dominante if and only if $f(x) = y$, where x and y are the generic points of X and Y, respectively. The corollary then follows from Corollary 22.7.6. □

Example 23.7.23. We can precise the result of Corollary 23.7.22 if Y is the projective line $\mathbb{P}^1_k = \operatorname{Proj}(k[T_0, T_1])$, where T_0 and T_1 are indeterminates. This is an integral and separated k-scheme, and the induced subscheme $D_+(T_0)$ of Y is isomorphic to $\operatorname{Spec}(k[T])$, so the generic point of Y is the ideal (0) of $k[T]$ and its rational function field is $k(T)$, which shows that Y is a complete algebraic cuver over k. Moreover, the only graded ideal of $S = k[T_0, T_1]$ containing T_0 and distinct from S_+ is the principal ideal (T_0), so the complement of $D_+(T_0)$ in Y is reduced to a closed point, called the "infinite point" and denoted by ∞.

Corollary 23.7.24. *Let X be an irreducible normal algebraic curve with $K = K(X)$. Then there exists a canonical correspondence between K and the set of morphisms $u : X \to \mathbb{P}^1_k$ which is distinct from the constant morphism with value ∞. For u to be dominant, it is necessary and sufficient that the corresponding element in K is transcendental over k.*

Proof. By Corollary 22.7.6 and Example 23.7.23, the rational maps $X \dashrightarrow \mathbb{P}^1_k$ (hence morphisms $X \to \mathbb{P}^1_k$, in view of Proposition 23.7.19) correspond to points of $\mathbb{P}^1_k$ with values in K. For any element $\xi \in K$, we have a induced homomorphism $k[T_0] \to K$ which maps T_0 to ξ, and therefore a morphism $\operatorname{Spec}(K) \to D_+(T_0)$. By composing with the canonical injection $D_+(T_0) \to \mathbb{P}^1_k$, we obtain a point of $\mathbb{P}^1_k$ with values in K which is not located at ∞, which is completely determined by ξ in view of Proposition 22.2.4. On the other hand, by Corollary 22.2.15, any constant morphism $u : \operatorname{Spec}(K) \to \mathbb{P}^1_k$ with value y factors into

$$u : \operatorname{Spec}(K) \to \operatorname{Spec}(\kappa(y)) \to \mathbb{P}^1_k.$$

Since $y \in D_+(T_0)$, the morphism $\mathrm{Spec}(\kappa(y)) \to \mathbb{P}^1_k$ factors through the canonical injection $D_+(T_0) \to \mathbb{P}^1_k$, and u therefore is obtained by morphism $\mathrm{Spec}(K) \to D_+(T_0)$, which corresponds to an element $\xi \in K$; this proves the first part of the corollary. For the morphism u to be dominant, it is necessary that the morphism $\mathrm{Spec}(K) \to \mathrm{Spec}(k[T_0]) \cong D_+(T_0)$ is dominant, which means the homomorphism $k[T] \to K$ is injective (Corollary 10.4.19), and this is true if and only if ξ is transcendental. □

Remark 23.7.8. With the notations of Corollary 23.7.24, we now determine the image of the morphism $\mathrm{Spec}(K) \to \mathbb{P}^1_k$ induced by an algerbaic element $\xi \in K$ over k. By definition, if $y \in \mathbb{P}^1_k$ is this image, the morphism factors into

$$\mathrm{Spec}(K) \to \mathrm{Spec}(\kappa(y)) \to \mathrm{Spec}(k[T]) \to \mathbb{P}^1_k$$

where we write $\mathrm{Spec}(k[T])$ for $D_+(T_0)$. We first note that any prime ideal in $k[T]$ is maximal, so $\kappa(y) = k[T]/\mathfrak{p}_y$, and the morphism $\mathrm{Spec}(K) \to \mathrm{Spec}(\kappa(y))$ is identified with the canonical injection $k[T]/\mathfrak{p}_y \to K$. By definition, this homomorphism is induced by the homomorphism $k[T] \to K, T \mapsto \xi$, so if $f(T)$ is the irreducible polynomial of ξ over k, we have $\mathfrak{p}_y = (f)$, and y is therefore the point of $\mathrm{Spec}(k[T])$ corresponding to (f). In particular, if $\xi \in k$, then $\mathfrak{p}_y = (T - \xi)$, and if k is an algebraically closed field, we conclude that any element $\xi \in k$ corresponds to a morphism $\mathrm{Spec}(K) \to \mathbb{P}^1_k$ with image ξ (identified with its corresponding maximal ideal $(T - \xi)$), and any element $\xi \in K - k$ corresponds to a dominant morphism $\mathrm{Spec}(K) \to \mathbb{P}^1_k$.

Corollary 23.7.25. *Let X and Y be normal, complete and irreducible algebraic curves, with $K = K(Y)$, $L = K(X)$. Then there exist a bijective correspondense between the set of k-isomorphisms $X \xrightarrow{\sim} Y$ and the set of k-isomorphisms $K \xrightarrow{\sim} L$.*

Corollary 23.7.25 shows that a normal, complete and irreducible algerbaic curves over k is determined by its rational function field K up to an isomorphism. By definition, K is a field of finite type over k with transcendental degree 1 (which is called a algerbaic function field of one variable).

Proposition 23.7.26. *For any extension K of k of finite type and transcendental degree 1, there exists a normal, complete and irreducible algebraic curve X such that $K(X) = K$. The set of local rings of X is identified with the set formed by K and the valuation rings containing k with fraction field K.*

Proof. In fact, K is a finite extension of a purely transcendental extension $k(T)$ of k, which is identified with the rational function field of $Y = \mathbb{P}^1_k$. Let X be the inegral closure of Y relative to K; X is then a normal algebraic curve with field K (Proposition 23.6.22), and it is complete since the morphism $X \to Y$ is finite (Corollary 23.7.17). For $x \in X$, the local ring $\mathscr{O}_{X,x}$ is equals to K if x is the generic of X, and otherwise it is a discrete valuation ring of K. Conversely, let A be a discrete valuation ring with fraction field K; as the morphism $X \to \mathrm{Spec}(k)$ is proper and A dominates k, it also dominates a local ring $\mathscr{O}_{X,x}$ of X by Corollary 23.7.11, and therefore equals to $\mathscr{O}_{X,x}$. □

Remark 23.7.9. It follows from Proposition 23.7.26 and Corollary 23.7.25 that giving a normal, complete and irreducible algebraic curve over k is essentially equivalent to giving a extension K of k of finite type and transcendental degree 1. We note that if k' is an extension of k, $X \otimes_k k'$ is also a complete algebraic curve over k' (Proposition 23.5.17(iii)), but in general it is neither

reduced nor irreducible. However, this will be the case if K is a separable extension of k and if k is algebraically closed in K (which is expressed, in a classical terminology, that K is a "regular extension" of k). But even in this case, it may happen that $X \otimes_k k'$ is not normal.

23.8 Blow up of schemes, projective cones and closures

23.8.1 Blow up of schemes

Let Y be a scheme and $(\mathscr{I}_n)_{n\geq 0}$ be a decreasing sequence of quasi-coherent ideal of $\mathscr{O}_Y$. Suppose that the following conditions are satisfied:

$$\mathscr{I}_0 = \mathscr{O}_Y, \quad \mathscr{I}_n\mathscr{I}_n \subseteq \mathscr{I}_{m+n}$$

where m, n are integers. If this is true, we say that the sequence $(\mathscr{I}_n)_{n\geq 0}$ is **filtered**, or that $(\mathscr{I}_n)_{n\geq 0}$ is a **filtered sequence of quasi-coherent ideals of** $\mathscr{O}_Y$. We note that this hypothesis implies that $\mathscr{I}_1^n \subseteq \mathscr{I}_n$. Put

$$\mathscr{S} = \bigoplus_{n\geq 0} \mathscr{I}_n.$$

It follows the assumption that $\mathscr{S}$ is a quasi-coherent $\mathscr{O}_Y$-algebra, hence defines a Y-scheme $X = \mathrm{Proj}(\mathscr{S})$. If $\mathscr{I}$ is an invertible ideal of $\mathscr{O}_Y$, $\mathscr{I}_n \otimes_{\mathscr{O}_Y} \mathscr{I}^{\otimes n}$ is canonically idealtified with $\mathscr{I}_n\mathscr{I}^n$, and if we replace $\mathscr{I}_n$ by $\mathscr{I}_n\mathscr{I}^n$, then the obtained $\mathscr{O}_Y$-algebra $\mathscr{S}_{(\mathscr{I})}$ satisfies that $X_{(\mathscr{I})} = \mathrm{Proj}(\mathscr{S}_{(\mathscr{I})})$ is canonically isomorphic to X (Proposition 23.3.6).

Suppose that Y is locally integral, so that $\mathscr{K}_Y$ is a quasi-coherent $\mathscr{O}_Y$-algebra (Proposition 22.7.22). We say a sub-$\mathscr{O}_Y$-module $\mathscr{I}$ of $\mathscr{K}_Y$ is a **fractional ideal** of $\mathscr{K}_Y$ if it is of finite type. Given a filtered sequence $(\mathscr{I}_n)_{n\geq 0}$ of quasi-coherent fractional ideal of $\mathscr{K}_Y$, we can then define the quasi-coherent graded $\mathscr{O}_Y$-algebra $\mathscr{S}$ and the corresponding Y-scheme $X = \mathrm{Proj}(\mathscr{S})$. We then see that for an invertible fractional ideal $\mathscr{J}$ of $\mathscr{K}_Y$, there is a canonical isomorphism of X and $X_{(\mathscr{J})}$.

Let Y be a scheme (resp. a locally integral scheme), and $\mathscr{I}$ be a quasi-coherent ideal of $\mathscr{O}_Y$ (resp. a quasi-coherent fractional ideal of $\mathscr{K}_Y$); put $\mathscr{S} = \bigoplus_{n\geq 0} \mathscr{I}^n$. The Y-scheme $X = \mathrm{Proj}(\mathscr{S})$ is said to be the scheme obtained by **blowing up along the ideal** $\mathscr{I}$, or the **blow up** of Y relative to $\mathscr{I}$. If $\mathscr{I}$ is a quasi-coherent ideal of $\mathscr{O}_Y$ and Y' is the closed subscheme defined by $\mathscr{I}$, we also say that X is the Y-scheme obtained by blowing up Y'. By definition, $\mathscr{S}$ is generated by $\mathscr{S}_1 = \mathscr{I}$; if $\mathscr{I}$ is a $\mathscr{O}_Y$-module of finite type, X is then projective over Y. By the hypotheses on $\mathscr{I}$, the $\mathscr{O}_X$-module $\mathscr{O}_X(1)$ is invertible (Proposition 23.3.14) and very ample in view of Corollary 23.4.12 for the structural morphism $j : X \to Y$. We also note that the restriction of f to $f^{-1}(Y - Y')$ is an isomorphism if $\mathscr{I}$ is the quasi-coherent ideal of $\mathscr{O}_Y$ defining Y': in fact, this question is local over Y, so it suffice to suppose $\mathscr{I} = \mathscr{O}_Y$, and this then follows from Remark 23.3.1.

If we replace $\mathscr{I}$ by $\mathscr{I}^d$ for some $d > 0$, the blow up Y-scheme X is then replaced by a Y-scheme canonically isomorphic to X' (Proposition 23.3.6). Simialrly, for any invertible ideal (resp. fractional ideal) $\mathscr{J}$, the blow up scheme $X_{(\mathscr{I})}$ relative to $\mathscr{I}\mathscr{J}$ is canonically isomorphic to X. In particular, if $\mathscr{I}$ is an invertible ideal (resp. fractional ideal), the blow up Y-scheme relative to $\mathscr{I}$ is isomorphic to Y.

Proposition 23.8.1. *Let Y be an integral scheme.*

(i) For any filtered sequence $(\mathscr{I}_n)$ of quasi-coherent fractional ideals of $\mathscr{K}_Y$, the Y-scheme $X = \operatorname{Proj}(\bigoplus_{n\geq 0}\mathscr{I}_n)$ is integral and the structural morphism $f : X \to Y$ is dominant.

(ii) Let $\mathscr{I}$ be a quasi-coherent fractional ideal of $\mathscr{K}_Y$ and X be the blow up Y-scheme relative to $\mathscr{I}$. If $\mathscr{I} \neq 0$, the structural morphism $f : X \to Y$ is surjective and birational.

Proof. In case (i) the quasi-coherent graded $\mathscr{O}_Y$-algebra $\mathscr{S} = \bigoplus_{n\geq 0}\mathscr{I}_n$ is integral since for any $y \in Y$, $\mathscr{O}_{Y,y}$ is an integral domain, so the claim follows from Proposition 23.3.10. For (ii), we obtain from (i) that X is integral; if morever x and y are generic points of X and Y, we have $f(x) = y$, and it is necessary to prove that $\kappa(x) = \kappa(y)$. Now x is also the generic point of the fiber $f^{-1}(y)$; if $\psi : Z \to Y$ is the canonical morphism, where $Z = \operatorname{Spec}(\kappa(y))$, then the scheme $f^{-1}(y)$ is identified with $\operatorname{Proj}(\mathscr{S}')$, where $\mathscr{S}' = \psi^*(\mathscr{S})$ (Proposition 23.3.28). But it is clear that $\mathscr{S}' = \bigoplus_{n\geq 0}(\widetilde{\mathscr{I}_y})^n$, and as $\mathscr{I}$ is a nonzero quasi-coherent fractional ideal of $\mathscr{K}_Y$, $\mathscr{I}_y \neq 0$ (Corollary 22.7.21), so $\mathscr{I}_y = \kappa(y)$ (since y is the generic point of Y, $\mathscr{I}_y$ is a $\kappa(y)$-vector space). The scheme $\operatorname{Proj}(\mathscr{S}')$ is then identified with $\operatorname{Spec}(\kappa(y))$ (Remark 23.3.1), whence the assertion. □

Retain the notations of Proposition 23.8.1. By definition, the injection $\mathscr{I}_{n+1} \to \mathscr{I}_n$ defines for each $k \in \mathbb{Z}$ a injective homomorphism of degree 0 of graded $\mathscr{S}$-modules

$$u_k : \mathscr{S}_+(k+1) \to \mathscr{S}(k). \tag{8.1.1}$$

As $\mathscr{S}_+(k+1)$ and $\mathscr{S}(k+1)$ are eventually isomorphic $\mathscr{S}$-modules, the hommorphism u_k corresponds to a canonical injective homomorphism of $\mathscr{O}_X$-modules (Proposition 23.3.22):

$$\tilde{u}_k : \mathscr{O}_X(k+1) \to \mathscr{O}_X(k). \tag{8.1.2}$$

Recall on the other hand that we have defined a canonical homomorphism

$$\lambda : \mathscr{O}_X(d) \otimes_{\mathscr{O}_X} \mathscr{O}_X(k) \to \mathscr{O}_X(d+k)$$

and as the diagram

$$\begin{tikzcd}
\mathscr{S}(d) \otimes_{\mathscr{S}} \mathscr{S}(k) \otimes_{\mathscr{S}} \mathscr{S}(l) \arrow[r] \arrow[d] & \mathscr{S}(d+k) \otimes_{\mathscr{S}} \mathscr{S}(l) \arrow[d] \\
\mathscr{S}(d) \otimes_{\mathscr{S}} \mathscr{S}(k+l) \arrow[r] & \mathscr{S}(d+k+l)
\end{tikzcd}$$

is commutative, it follows from the functoriality of λ that the homomorphism λ define a quasi-coherent graded $\mathscr{O}_X$-algebra structure on $\mathscr{S}_X = \bigoplus_{n\in\mathbb{Z}}\mathscr{O}_X(n)$. Moreover, the diagram

$$\begin{tikzcd}
\mathscr{S}(d) \otimes_{\mathscr{S}} \mathscr{S}_+(k+1) \arrow[r] \arrow[d, "1\otimes u_k"'] & \mathscr{S}_+(d+k+1) \arrow[d, "u_{k+d}"] \\
\mathscr{S}(d) \otimes_{\mathscr{S}} \mathscr{S}(k) \arrow[r] & \mathscr{S}(d+k)
\end{tikzcd}$$

is commutative; the functoriality of λ shows that we have a commutative diagram

$$\begin{tikzcd}
\mathscr{O}_X(d) \otimes_{\mathscr{O}_X} \mathscr{O}_X(k+1) \arrow[r, "\lambda"] \arrow[d, "1\otimes\tilde{u}_k"'] & \mathscr{O}_X(d+k+1) \arrow[d, "\tilde{u}_{d+h}"] \\
\mathscr{O}_X(d) \otimes_{\mathscr{O}_X} \mathscr{O}_X(k) \arrow[r, "\lambda"] & \mathscr{O}_X(d+k)
\end{tikzcd} \tag{8.1.3}$$

where the horizontal arrows are the canonical homomorphisms. We can then say that the $\tilde{u}_k$ define an injective homomorphism (of degree 0) of graded $\mathcal{S}_X$-modules

$$\tilde{u} : \mathcal{S}_X(1) \to \mathcal{S}_X \tag{8.1.4}$$

Now we consider for each $n \geq 0$ the homomorphism $\tilde{v}_n = \tilde{u}_{n-1} \circ \cdots \tilde{u}_0$, which is an injective homomorphism $\mathcal{O}_X(n) \to \mathcal{O}_X$; we denote its image by $\mathcal{I}_{n,X}$, which is a quasi-coherent ideal $\mathcal{O}_X$ isomorphic to $\mathcal{O}_X(n)$. Moreover, the diagram

$$\begin{tikzcd}
\mathcal{O}_X(m) \otimes_{\mathcal{O}_X} \mathcal{O}_X(n) \arrow[r, "\lambda"] \arrow[d, "\tilde{v}_m \otimes \tilde{v}_n"'] & \mathcal{O}_X(m+n) \arrow[d, "\tilde{v}_{m+n}"] \\
\mathcal{O}_X \arrow[r, "\mathrm{id}"] & \mathcal{O}_X
\end{tikzcd}$$

is commutative for $m, n \geq 0$. We also conclude that $(\mathcal{I}_{n,X})_{n\geq 0}$ is a filtered sequence of quasi-coherent ideals of $\mathcal{O}_X$.

Proposition 23.8.2. *Let Y be a scheme, $\mathcal{I}$ be a quasi-coherent ideal of $\mathcal{O}_Y$, and X be the blow up Y-scheme relative to $\mathcal{I}$. Then for each $n > 0$ we have a canonical isomorphism*

$$\mathcal{O}_X(n) \xrightarrow{\sim} \mathcal{I}^n \mathcal{O}_X = \mathcal{I}_{n,X}$$

and therefore $\mathcal{I}^n \mathcal{O}_X$ is a very ample invertible $\mathcal{O}_X$-module relative to Y for $n > 0$.

Proof. The last assertion is immediate since $\mathcal{O}_X(1)$ is invertible (Proposition 23.3.14) and very ample relative to Y by definition. On the other hand, the image of the homomorphism $v_n : S_+(n) \to S$ is none other than $\mathcal{I}^n \mathcal{S}$, and the first assertion then follows from the exactness of the functor $\widetilde{\mathcal{M}}$ (Proposition 23.3.13) and the formula $\widetilde{\mathcal{I}\mathcal{M}} = \mathcal{I} \cdot \widetilde{\mathcal{M}}$. □

Corollary 23.8.3. *Under the hypotheses of Proposition 23.8.2, if $f : X \to Y$ is the structural morphism and Y' is the closed subscheme of Y defined by $\mathcal{I}$, the closed subscheme $X' = f^{-1}(Y')$ of X is defined by $\mathcal{I}\mathcal{O}_X$ (isomorphic to $\mathcal{O}_X(1)$), so we have an exact sequence*

$$0 \longrightarrow \mathcal{O}_X(1) \longrightarrow \mathcal{O}_X \longrightarrow \mathcal{O}_{X'} \longrightarrow 0$$

Proof. This follows from Proposition 23.8.2 and Proposition 22.4.14(b). □

Under the hypotheses of Proposition 23.8.2, we can specify that structure of $\mathcal{I}_{n,X}$. Note that that the homomorphism

$$\tilde{u}_{-1} : \mathcal{O}_X \to \mathcal{O}_X(-1)$$

corresponds canonically to a section s of $\mathcal{O}_X(-1)$ over X, which is called the canonical section (relative to $\mathcal{I}$). In the diagram (8.1.3), the horizontal homomorphisms are isomorphisms (Corollary 23.3.16), so by replacing d by k and k by -1 in that diagram, we obtain $\tilde{u}_k = 1_k \otimes \tilde{u}_{-1}$ (where 1_k is the identity of $\mathcal{O}_X(k)$), which means the homomorphism $\tilde{u}_k$ is none other than the tensor product by the canonical section k (for any $k \in \mathbb{Z}$). The homomorphism $\tilde{u}$ of (8.1.4) can be interpreted in the same manner, and we then deduce that, for any $n \geq 0$, the homomorphism $\tilde{v}_n : \mathcal{O}_X(n) \to \mathcal{O}_X$ is the tensor product by $s^{\otimes n}$.

Corollary 23.8.4. *With the notations of Corollary 23.8.3, the underlying of X' is the set of $x \in X$ such that $s(x) = 0$, where s is the canonical section of $\mathcal{O}_X(-1)$.*

Proof. In fact, if c_x is a generator for the fiber $(\mathcal{O}_X(1))_x$ at a point x, $s_x \otimes c_x$ is canonically identified with a generator for the fiber $\mathcal{I}_{1,X}$ at the point x, and is therefore invertible if and only if $s_x \notin \mathfrak{m}_x(\mathcal{O}_X(-1))_x$, which means $s(x) \neq 0$. □

Proposition 23.8.5. *Let Y be an integral scheme, $\mathcal{I}$ be a quasi-coherent fractional ideal of $\mathcal{K}_Y$, and X be the blow up Y-scheme relative to $\mathcal{I}$. Then there is an isomorphism $\mathcal{O}_X \xrightarrow{\sim} \mathcal{I}\mathcal{O}_X$, and in particular $\mathcal{I}\mathcal{O}_X$ is a very ample invertible $\mathcal{O}_X$-module relative to Y.*

Proof. The question is local over Y (Corollary 23.4.14), so we can assume that $Y = \operatorname{Spec}(A)$ is affine, where A is an integral domain with fraction field K and $\mathcal{I} = \widetilde{\mathfrak{I}}$, where $\mathfrak{I}$ is a fractional ideal of K. Then there exists an element $a \neq 0$ such that $a\mathfrak{I} \subseteq A$. Put $S = \bigoplus_n \mathfrak{I}^n$; the map $x \mapsto ax$ is an A-isomorphism of $\mathfrak{I}^{n+1} = S(1)_n$ to $a\mathfrak{I}^{n+1} = a\mathfrak{I}S_n \subseteq \mathfrak{I}^n = S_n$, so defines a eventual isomorphism of degree 0 of graded S-modules $S_+(1) \to a\mathfrak{I}S$. But $x \mapsto a^{-1}x$ is an isomorphism of degree 0 of graded S-modules $a\mathfrak{I}S \xrightarrow{\sim} \mathfrak{I}S$, so we obtain an isomorphism $\mathcal{O}_X(1) \xrightarrow{\sim} \mathcal{I}\mathcal{O}_X$. As S is generated by $S_1 = \mathfrak{I}$, $\mathcal{O}_X(1)$ is invertible and very ample, whence the conclusion. □

Proposition 23.8.6. *Let Y be a locally Noetherian scheme, $\mathcal{I}$ ba a quasi-coherent ideal of $\mathcal{O}_Y$, and X be the blow up Y-scheme relative to $\mathcal{I}$. Let $f : X \to Y$ be the structural morphism. If $g : Z \to Y$ is any morphism such that $g^*(\mathcal{I})\mathcal{O}_Z$ is an invertible $\mathcal{O}_Z$-module, then there exists a unique morphism $\tilde{g} : Z \to X$ such that the following diagram is commutative:*

$$\begin{tikzcd} Z \arrow[r, "\tilde{g}"] \arrow[dr, "g"'] & X \arrow[d, "f"] \\ & Y \end{tikzcd}$$

Proof. The question is local over Y, so we can assume that $Y = \operatorname{Spec}(A)$ is affine, where A is Noetherian, and $\mathcal{I} = \widetilde{\mathfrak{I}}$ where $\mathfrak{I}$ is an ideal of A. Then $X = \operatorname{Proj}(S)$ where $S = \bigoplus_{n\geq 0} \mathfrak{I}^n$, and we note that since A is Noetherian, $\mathfrak{I}$ is finitely generated, so S is of finite type over A. Let $a_0, \dots, a_n \in \mathfrak{I}$ be a set of generators for $\mathfrak{I}$, so that we have a surjective homomorphism $\varphi : A[T_0, \dots, T_n] \to S$ which maps T_i to a_i, and this gives a closed immersion $i : X \to \mathbb{P}^n_A$, and we can identify X with its image. If $g : Z \to Y$ is a morphism such that $\mathcal{L} = g^*(\mathcal{I})\mathcal{O}_Z$ is invertible, then the inverse images of the a_i, which are global sections of $\mathcal{I}$, give global sections $s_0, \dots, s_n$ of $\mathcal{L}$ which generate $\mathcal{L}$. Then by Proposition 23.4.3 $r : Z \to P = \mathbb{P}^n_A$ such that $\mathcal{L} \cong r^*(\mathcal{O}_P(1))$ and $s_i = r^{-1}(T_i)$. We now claim that this morphism factors through the closed subscheme X of $\mathbb{P}^n_A$: this follows from the fact that if $F(T_0, \dots, T_n)$ is a homogeneous polynomial of degree d of $\ker \varphi$, then $F(a_0, \dots, a_n) = 0$ in A and so $F(s_0, \dots, s_n) = 0$ in $\Gamma(Z, \mathcal{L}^{\otimes d})$. This gives the desired morphism $\tilde{g} : Z \to X$, and for any such morphism we necessarily have

$$g^*(\mathcal{I})\mathcal{O}_Z = \tilde{g}^*(f^*(\mathcal{I})\mathcal{O}_X)\mathcal{O}_Z = \tilde{g}^*(\mathcal{O}_X(1))\mathcal{O}_Z$$

by Proposition 23.8.2, so we obtain a surjective hommorphism $\tilde{g}^*(\mathcal{O}_X(1)) \to g^*(\mathcal{I})\mathcal{O}_Z = \mathcal{L}$, hence an isomorphism by Corollary 19.4.38. Clearly the sections s_i of $\mathcal{L}$ are the inverse images of the sections T_i of $\mathcal{O}_P(1)$ on $\mathbb{P}^n_A$, so the uniqueness of $\tilde{g}$ follows from Proposition 23.4.3. □

Corollary 23.8.7. *Let $q : Y' \to Y$ be a morphism of locally Noetherian schemes and $\mathscr{I}$ be a quasi-coherent ideal of $\mathscr{O}_Y$. Let X be the blow up Y-scheme relative to $\mathscr{I}$ and X' be the blow up Y'-scheme relative to $\mathscr{J} = q^*(\mathscr{I})\mathscr{O}_Y$. Then there exists a unique morphism $p : X' \to X$ such that the diagram*

$$\begin{tikzcd} X' \arrow[r, "p"] \arrow[d] & X \arrow[d] \\ Y' \arrow[r, "q"] & Y \end{tikzcd} \tag{8.1.5}$$

is commutative. Moreover, if q is a closed immersion, so is p.

Proof. The existence and uniqueness of q follows from Proposition 23.8.6 and Proposition 23.8.2. To show that p is a closed immersion if q is, we trace the definition of the blow up: $X = \mathrm{Proj}(\mathscr{S})$ where $\mathscr{S} = \bigoplus_{n\geq 0} \mathscr{I}^n$ and $X' = \mathrm{Proj}(\mathscr{S}')$ where $\mathscr{S}' = \bigoplus_{n\geq 0} \mathscr{J}^n$. Since Y' is a closed subscheme of Y, we can consider $\mathscr{S}'$ as a sheaf of graded algebras over Y. Then there exists a natrual surjective homomorphism $\mathscr{S} \to \mathscr{S}'$, which gives rise to the closed immersion p. □

In the situation of Corollary 23.8.7, if Y' is a closed subscheme of Y, we call the closed subscheme X' of X the **strict transform** of Y' under the blowing-up $f : X \to Y$.

Example 23.8.8. Let $Y = \mathbb{A}^n_k$ be the affine space over a field k and we consider the blow up of Y at the origin y of Y. Then $Y = \mathrm{Spec}(A)$ where $A = k[X_1, \dots, X_n]$, y corresponds to the ideal $\mathfrak{I} = (X_1, \dots, X_n)$, and $X = \mathrm{Proj}(S)$ where $S = \bigoplus_{n\geq 0} \mathfrak{I}^n$. We can define a surjective homomorphism

$$\varphi : A[Y_0, \dots, Y_n] \to S$$

of graded rings by sending Y_i to X_i as an element of degree 1 in S, which gives a closed immersion of X into $\mathbb{P}^{n-1}_A$. It is not hard to see that the kernel of φ is generated by the homogeneous polynomials $X_iY_j - X_jY_i$, where $i, j = 1, \dots, n$, so this definition is compatible with the definition of the blow up of the affine variety $\mathbb{A}^n_k$.

Now if Y' is a closed subscheme of Y passing through y, then the strict transform X' of Y' is a closed subscheme of X. Hence, provided that Y' is not reduced to the point y, we can recover X' as the closure of $f^{-1}(Y' - \{y\})$, where $f : f^{-1}(Y' - \{y\}) \to Y' - \{y\}$ is an isomorphism. Again this definition is compatible with the definition of blow up of closed subvarieties of $\mathbb{A}^n_k$.

Example 23.8.9. As an example of the general concept of blowing up a coherent sheaf of ideals, we show how to eliminate the points of indeterminacy of a rational map determined by an invertible sheaf. So let A be a ring, X be a Noetherian scheme over A, $\mathscr{L}$ be an invertible sheaf on X, and $s_0, \dots, s_n$ be global sections of $\mathscr{L}$. Let U be the open subset of X where the s_i generate the sheaf $\mathscr{L}$ (that is, the subset where the corresponding homomorphism $\mathscr{O}_X^{n+1} \to \mathscr{L}$ is surjective, cf. Proposition 19.4.6(iii)). Then the invertible sheaf $\mathscr{L}|_U$ on U and the global sections $s_0, \dots, s_n$ determine an A-morphism $\varphi : U \to \mathbb{P}^n_A$, which is also a rational map $X \dashrightarrow \mathbb{P}^n_A$. We will now show how to blow up a certain sheaf of ideals $\mathscr{I}$ on X, whose corresponding closed subsheme Y has support equal to $X - U$ (i.e., the underlying topological space of Y is

$X - U$), so that the morphism φ extends to a morphism $\tilde{\varphi} : \widetilde{X} \to \mathbb{P}^n_A$.

$$\begin{tikzcd} \widetilde{X} \arrow[d, "\pi"'] \arrow[dr, dashed, "\tilde{\varphi}"] & \\ X & \mathbb{P}^n_A \\ U \arrow[u, hook] \arrow[ur, "\varphi"'] & \end{tikzcd}$$

Let $\mathscr{F}$ be the quasi-coherent sub-$\mathscr{O}_X$-module of $\mathscr{L}$ generated by $s_0, \dots, s_n$. We define a coherent ideal $\mathscr{I}$ of $\mathscr{O}_X$ as follows: for any open subset $V \subseteq X$ and an isomorphism $\psi : \mathscr{L}|_V \cong \mathscr{O}_X|_V$, we take $\mathscr{I}|_V = \psi(\mathscr{F}|_V)$. It is clear that $\mathscr{I}_V$ is independent of the choice of ψ, so we get a well-defined coherent ideal $\mathscr{I}$ of $\mathscr{O}_X$. We also note that $\mathscr{I}_x = \mathscr{O}_{X,x}$ if and only if $x \in U$, so the corresponding closed subscheme Y has support $X - U$. Let $\pi : \widetilde{X} \to X$ be the corresponding blow up relative to $\mathscr{I}$. We claim that $\pi^*(\mathscr{I})$ is a coherent ideal of $\mathscr{O}_{\widetilde{X}}$, so is invertible by Proposition 23.8.2. This can be verified on each affine open X_{s_i}. Then the global sections $\pi^*(s_i)$ of $\pi^*(\mathscr{L})$ generate an invertible sub-$\mathscr{O}_{\widetilde{X}}$-module $\mathscr{L}'$ of $\pi^*(\mathscr{L})$. Now $\mathscr{L}'$ and the sections $\pi^*(s_i)$ define a morphism $\tilde{\varphi} : \widetilde{X} \to \mathbb{P}^n_A$ whose restriction on $\pi^{-1}(U)$ corresponds to the morphism φ under the isomorphism $\pi : \pi^{-1}(U) \xrightarrow{\sim} U$.

23.8.2 Homogenization of graded rings

Let S be a graded ring, which we do not suppose to be with positive degrees. We set

$$S^{\geqslant} = \bigoplus_{n \geq 0} S_n, \quad S^{\leqslant} = \bigoplus_{n \leq 0} S_n$$

which are subrings of S, with positive of negative degrees respectively. If f is a homogeneous element of degree d (positive of negative) of S, the localization $S_f = S'$ is endowed with a graded ring structure, where S'_n is the set of elements x/f^k, where $x \in S_{n+kd}$ ($k \geq 0$); we also note that $S_{(f)} = S'_0$, and we denote $S_f^{\geqslant}$ and $S_f^{\geqslant}$ for $S'^{\geqslant}$ and $S'^{\leqslant}$, respectively. This notation is justified by the fact that if $d > 0$, then we have

$$(S^{\geqslant})_f = S_f; \tag{8.2.1}$$

in fact, if $x \in S_{n+kd}$ where $n + kd < 0$, we can write $x/f^k = xf^h/f^{h+k}$ so that $n + (h+k)d > 0$ for $h > 0$ large enough. We then conclude by definition that

$$(S^{\geqslant})_{(f)} = (S_f^{\geqslant})_0 = S_{(f)}. \tag{8.2.2}$$

If M is a graded S-module, we put similarly

$$M^{\geqslant} = \bigoplus_{n \geq 0} M_n, \quad M^{\leqslant} = \bigoplus_{n \leq 0} M_n$$

which are respectively $S^{\geqslant}$-module and $S^{\geqslant}$-module, with intersection the S_0-module M_0. If $f \in S_d$, we also define M_f as the graded S_f-module such that $(M_f)_n$ is the set of elements z/f^k, where $z \in M_{n+kd}$. We denote by $M_{(f)}$ the set of degree 0 elements in M_f, which is an

$S_{(f)}$-module, and we write $M_f^{\geqslant}$ and $M_f^{\leqslant}$ for $(M_f)^{\geqslant}$ and $(M_f)^{\leqslant}$ respectively. If $d > 0$, we also have

$$(M^{\geqslant})_f = M_f, \quad (M^{\geqslant})_{(f)} = (M_f^{\geqslant})_0 = M_{(f)}. \tag{8.2.3}$$

Let z be an indeterminate, which is called the **homogenization variable**. If S is a graded ring, the polynomial algebra

$$\widehat{S} = S[z]$$

is a graded S-algebra, where for f homogeneous we put

$$\deg(fz^n) = n + \deg(f).$$

Lemma 23.8.10. *Let $f \in S_d$ with $d > 0$. We have canonical isomorphisms*

$$\widehat{S}_{(z)} \cong \widehat{S}/(z-1)\widehat{S} \cong S, \tag{8.2.4}$$

$$\widehat{S}_{(f)} \cong S_f^{\leqslant}. \tag{8.2.5}$$

Proof. The first isomorphism of (8.2.4) is already defined in Proposition 23.2.3 and the second one is trivial; the isomorphism $\widehat{S}_{(z)} \cong S$ thus defined then send an element xz^n/z^{n+k} (where $\deg(x) = k$ for $k \geq -n$) to the element x. The homomorphism (8.2.5) is defined by sending xz^n/f^k (where $\deg(x) = kd - n$) to the element x/f^k, of degree $-k$ in $S_f^{\leqslant}$, and it is easy to verify that this is an isomorphism. □

Let M be a graded S-module. It is clear that the S-module

$$\widehat{M} = M \otimes_S \widehat{S} = M \otimes_S S[z]$$

is the direct sum of the S-modules $M \otimes Sz^n$, whence the abelian groups $M_k \otimes Sz^n$. We define over $\widehat{M}$ an $\widehat{S}$-module structure by

$$\deg(x \otimes z^n) = n + \deg(x)$$

for x homogeneous in M.

Lemma 23.8.11. *Let $f \in S_d$ with $d > 0$. We have a canonical isomorphism*

$$\widehat{M}_{(z)} \cong \widehat{M}/(z-1)\widehat{M} \cong M, \tag{8.2.6}$$

$$\widehat{M}_{(f)} \cong M_f^{\leqslant}. \tag{8.2.7}$$

Proof. This can be proved as Lemma 23.8.10 by using the second part of Proposition 23.2.3. □

Let S be a graded ring with positive degrees. Then for each $n \geq 0$, we can consider $S(n) = \bigoplus_{m \geq n} S_m$ as a graded iedal of S (in particular $S(0) = S$ and $S(1) = S_+$). As it is clear that $S(m)S(n) \subseteq S(m+n)$, we can then define a graded ring

$$S^{\natural} = \bigoplus_{n \geq 0} S(n)$$

whence $S_n^\natural = S(n)$. Then $S_0^\natural$ is equal to S considered as a nongraded ring, and $S^\natural$ is therefore an S-algebra. For any homogeneous element $f \in S_d$ with $d > 0$, we denote by $f^\natural$ the element f considered as an element of $S(d) = S_d^\natural$.

Lemma 23.8.12. *Let S be a graded ring with positive degrees, f be a homogeneous element with $d > 0$. We have canonical isomorphisms:*

$$S_f \cong \bigoplus_{n\in\mathbb{Z}} S(n)_{(f)}, \tag{8.2.8}$$

$$(S_f^{\geqslant})_{f/1} \cong S_f, \tag{8.2.9}$$

$$S^\natural_{(f^\natural)} \cong S_f^{\geqslant}. \tag{8.2.10}$$

the first two of which are bi-isomorphisms of graded rings.

Proof. It is immediate that we have $(S_f)_n = (S(n)_f)_0 = S(n)_f$, whence the first isomorphism. On the other hand, as $f/1$ is invertible in S_f, there is a canonical isomorphism $S_f \cong S_f^{\geqslant} = (S_f)_{f/1}$ in view of (8.2.1) applide to S_f. Finally, if $x = \sum_{m\geq n} y_n$ is an element of $S(n)$, where $n = kd$, we can correspond the element $x/(f^\natural)^k$ to the element $\sum_m y_m/f^k$ of $S_f^{\geqslant}$, and we verify that this is an isomorphism. □

If M is a graded S-module, we can similarly put for $n \in \mathbb{Z}$

$$M^\natural = \bigoplus_{n\in\mathbb{Z}} M(n)$$

as $S(m)M(n) \subseteq M(m+n)$. Then $M^\natural$ is a graded $S^\natural$-module, and similarly we have the following:

Lemma 23.8.13. *Let $f \in S_d$ be a homogeneous element with $d > 0$. We have the following bi-homomorphisms*

$$M_f \cong \bigoplus_{n\in\mathbb{Z}} M(n)_{(f)}, \tag{8.2.11}$$

$$(M_f^{\geqslant})_{f/1} \cong M_f, \tag{8.2.12}$$

$$M^\natural_{(f^\natural)} \cong M_f^{\geqslant}. \tag{8.2.13}$$

the first two of which are bi-isomorphisms of graded modules.

Remark 23.8.1. We can think that $S^\natural$ is obtained from S by adding a "phantom" element $\boldsymbol{y}$ of degree -1. The component $S(n)$ can be then considered as the S-module $(S\boldsymbol{y}^n)_0$, which is the set of degree 0 elements in $S\boldsymbol{y}^n$. With this understanding, we can then relate the results of Lemma 23.8.10 and Lemma 23.8.12.

Lemma 23.8.14. *Let S be a graded ring with positive degrees.*

(i) For $S^\natural$ to be an $S_0^\natural$-algebra of finite type (resp. Noetherian), it is necessary and sufficient that S is an S_0-algebra of finite type (resp. Noetherian).

(ii) For $S_{n+1}^\natural = S_1^\natural S_n^\natural$ for $n \geq n_0$, it is necessary and sufficient that $S_{n+1} = S_1 S_n$ for $n \geq n_0$.

(iii) For $S_n^\natural = (S_1^\natural)^n$ for $n \geq n_0$, it is necessary and sufficient that $S_n = S_1^n$ for $n \geq n_0$.

(iv) If (f_α) is a set of homogeneous elements of S_+ such that the radical in S_+ of the ideal of S_+ generated by the f_α is equal to S_+, then $S_+^\natural$ is the radical in $S_+^\natural$ of the ideal of $S_+^\natural$ generated by the $f_\alpha^\natural$.

Proof. If $S^\natural$ is an $S_0^\natural$-algebra of finite type, $S_+ = S_1^\natural$ is a finitely generated module over $S = S_0^\natural$ by Proposition 11.1.33, so S is an S_0-algebra of finite type by Corollary 11.1.34. If $S^\natural$ is a Noetherian ring, so is the ring $S_0^\natural = S$ by Corollary 11.1.34. Conversely, if S is an S_0-algebra of finite type, then by Proposition 11.1.36 there exists $d > 0$ and $n_0 > 0$ such that $S_{n+d} = S_h S_n$ for any $n \geq n_0$; we can clearly suppose that $n_0 \geq d$. Moreover, the S_n are finitely generated S_0-modules (Corollary 11.1.34(c)), so if $n \geq n_0 + d$, we have $S_n^\natural = S_n S_{n-d}^\natural = S_d^\natural S_{n-d}^\natural$; and if $n < n_0 + d$, we have

$$S_n^\natural = S_n + \cdots + S_{n_0+d-1} + S_d E + S_d^2 E + \cdots$$

where $E = S_{n_0} + \cdots + S_{n_0+d-1}$. For $1 \leq n \leq n_0$, let G_n be the union of the generators of the S_0-module S_i where $n \leq i \leq n_0 + d - 1$, considered as subsets of $S(n)$. For $n_0 + 1 \leq n \leq n_0 + d - 1$, similarly let G_n be the union of the generators of the S_0-module S_i where $n \leq i \leq n_0 + d - 1$ and of $S_d E$, considered as subsets of $S(n)$. Then it is clear that we have $S_n^\natural = S_0^\natural G_n$ for $1 \leq n \leq n_0 + d - 1$, and therefore the union G of the G_n for $1 \leq n \leq n_0 + d - 1$ is a system of generators of the $S_0^\natural$-algebra $S^\natural$. We then conclude that if $S = S_0^\natural$ is Noehterian, then so is $S^\natural$.

It is clear that if $S_{n+1} = S_1 S_n$ for $n \geq n_0$, then we have $S_{n+1}^\natural = S_1 S_n^\natural$, and a fortiori $S_{n+1}^\natural = S_1^\natural S_n^\natural$ for $n \geq n_0$. Conversely, the latter relation means that

$$S_{n+1} + S_{n+2} + \cdots = (S_1 + S_2 + \cdots)(S_n + S_{n+1} + \cdots);$$

by comparing the degree $n + 1$ component of both sides, we conclude that $S_{n+1} = S_1 S_n$. This proves the assertion (ii).

If $S_n = S_1^n$ for $n \geq n_0$, we have $S_n^\natural = \bigoplus_{m \geq n} S_1^m$, and as $S_1^\natural$ contains $\bigoplus_{m \geq 1} S_1^m$, we then have $S_n^\natural \subseteq (S_1^\natural)^n$ for $n \geq n_0$. Conversely, the degree n component of $(S_1^\natural)^n = (S_1 + S_2 + \cdots)^n$ considered as elements of S is equal to S_1^n; so the relation $S_n^\natural = (S_1^\natural)^n$ implies $S_n = S_1^n$.

Finally, to prove (iv), it suffices to show that if an element $g \in S_{k+d}$ is considered as an element of $S_k^\natural$ ($k > 0$, $d \geq 0$), then there exists an integer $n > 0$ such that in $S_{kn}^\natural$, g^n is a linear combination of the $f_\alpha^\natural$ with coefficients in $S^\natural$. By hypothesis, there exists an integer n_0 such that for $n \geq n_0$, we have $g^n = \sum_\alpha c_{\alpha n} f_\alpha$ in S, where the indices α appearing in this formula are independent of n. Moreover, we can evidently suppose that the $c_{\alpha n}$ are homogeneous, with

$$\deg(c_{\alpha n}) = n(k + d) - \deg(f_\alpha)$$

in S. Let n_0 be large enough such that we have $kn_0 > deg(f_\alpha)$ for the f_α appearing in the formula of g^n; for any α, let $c'_{\alpha n}$ be the element $c_{\alpha n}$ considered as an element of degree $kn - \deg(f_\alpha)$ in $S^\natural$. We then have $g^n = \sum_\alpha c'_{\alpha m} f_\alpha^\natural$ in $S^\natural$, which proves our assertion. □

Consider the graded S_0-algebra

$$S^\natural \otimes_S S_0 = S^\natural / S_+ S^\natural = \bigoplus_{n \geq 0} S(n)/S_+ S(n).$$

As S_n is a quotient S_0-module of $S(n)/S_+S(n)$, we have a canonical hommorphism of graded S_0-algebras

$$S^\natural \otimes_S S_0 \to S \tag{8.2.14}$$

which is evidently surjective, and corresponds to a canonical closed immersion

$$\mathrm{Proj}(S) \to \mathrm{Proj}(S^\natural \otimes_S S_0) \tag{8.2.15}$$

Proposition 23.8.15. *The canonical morphism (8.2.15) is bijective. For the homomorphism (8.2.14) to be eventually bijective, it is necessary and sufficient that there exists an integer n_0 such that $S_{n+1} = S_1S_n$ for $n \geq n_0$. If this is satisfied, then the morphism (8.2.15) is an isomorphism, and the converse of this is also true if S is Noetherian.*

Proof. To prove the first assertion, it suffices (Corollary 23.2.45) to prove that the kernel $\mathfrak{I}$ of the homomorphism (8.2.14) is formed by nilpotent elements. Now if $f \in S(n)$ is an element whose class mod $S_+S(n)$ belongs to this kernel, then $f \in S(n+1)$ (by the definition of (8.2.14)); the element f^{n+1}, considered as an element of $S(n(n+1))$, then belongs to $S_+S(n(n+1))$, if we write it as $f \cdot f^n$. Then the class of f^{n+1} mod $S_+S(n(n+1))$ is zero, which proves our assertion.

As the hypothesis $S_{n+1} = S_1S_n$ for $n \geq n_0$ is equivalent to $S^\natural_{n+1} = S^\natural_1 S^\natural_n$ for $n \geq n_0$ (Lemma 23.8.14(ii)), these hypotheses are equivalent to that (8.2.14) is eventually injective, hence eventually bijective, and then (8.2.15) is an isomorphism by Proposition 23.3.6(a). Conversely, assume that S is Noetherian, hence so is $S^\natural$ and $S^\natural \otimes_S S_0$ (Lemma 23.8.14(i)). If (8.2.15) is an isomorphism, the sheaf $\widetilde{\mathscr{I}}$ over $\mathrm{Proj}(S^\natural \otimes_S S_0)$ is zero (Proposition 23.3.30(a)); as $S^\natural \otimes_S S_0$ is Noetherian, we then conclude from Proposition 23.2.36(b) that $\mathfrak{I}$ is eventually null, so $S^\natural_{n+1} = S^\natural_1 S^\natural_n$ for $n \geq n_0$. □

Consider now the canonical injection $(S_+)^n \to S(n)$, which defines an injective homomorphism of degree 0 of graded rings

$$\bigoplus_{n\geq 0}(S_+)^n \to S^\natural. \tag{8.2.16}$$

Proposition 23.8.16. *For the homomorphism (8.2.16) to be an eventual isomorphism, it is necessary and sufficient that there exists an integer n_0 such that $S_n = S_1^n$ for $n \geq n_0$. If this is the case, the corresponding morphism*

$$\mathrm{Proj}(S^\natural) \to \mathrm{Proj}(\bigoplus_{n\geq 0}(S_+)^n) \tag{8.2.17}$$

is everywhere defined and an isomorphism, and the converse is also true if S is Noetherian.

Proof. The first two conditions are equivalent in view of Lemma 23.8.14(iii). The third assertion follows from Lemma 23.8.14(i), (iii) and Lemma 23.8.17. □

Lemma 23.8.17. *Let S be a graded ring with positive degrees which is a S_0-algebra of finite type. If the morphism corresponding to the canonical injection $S' = \bigoplus_{n\geq 0} S_1^n \to S$ is everywhere defined and an isomorphism, then there exists $n_0 > 0$ such that $S_n = S_1^n$ for $n \geq n_0$.*

Proof. In fact, let f_i $(1 \leq i \leq r)$ be a system of generators for the S_0-module S_1. Then the hypotheses implies that the $D_+(f_i)$ cover $\mathrm{Proj}(S)$. Let $(g_j)_{1\leq j\leq n}$ be a system of homogeneous elements of S_+, with $n_j = \deg(g_j)$, which together with the f_i form a system of generators of the ideal S_+, or a system of generators of S as an S_0-algebra. The elements $g_j/f_i^{n_j}$ of the ring $S_{(f_i)}$ then by hypotheses belong to the subring $S'_{(f_i)}$, so there exists an integer k such that $S_1^k g_j \subseteq (S_1)^{k+n_j}$ for any j. We then conclude by recurrence on r that $S_1^k g_j^r \subseteq S'$ for any $r \geq 1$, and by the choice of the g_j, we then have $S_1^k S \subseteq S'$. On the other hand there exists for any j an integer m_j such that $g_j^{m_j}$ belongs to the ideal of S generated by the f_i (Corollary 23.2.11), so $g_j^{m_j} \in S_1 S$, and $g_j^{m_j k} \in S_1^k S \subseteq S'$. Therefore there exists an integer $m_0 \geq k$ such that $g_j^m \in S_1^{mn_j}$ for $m \geq m_0$. Now if d is the largest of the n_j, the number $n_0 = dm_0 + k$ then satisfies the requirement. In fact, an element of S_n, for $n \geq n_0$, is a sum of elements of $S_1^\alpha u$, where u is a product of powers of g_j; if $\alpha \geq k$, it follows from the choice of k that $S_1^\alpha u \subseteq S_1^n$; in the contrary case, at least one of the exponent of g_j is $\geq m_0$, so $u \in S_1^\beta v$ where $\beta \geq m_0 \geq k$ and v is a product of powers of g_j, so we are reduced to the previous case, and $S_1^\alpha u \subseteq S_1^n$. This completes the proof. □

Remark 23.8.2. The condition $S_n = S_1^n$ for $n \geq n_0$ clearly implies that $S_{n+1} = S_1 S_n$ for $n \geq n_0$, but the converse is not ture, even we assume that S is Noetherian. For example, let K be a field, $A = K[\boldsymbol{x}]$, $B = K[\boldsymbol{y}]/\boldsymbol{y}^2 K[\boldsymbol{y}]$, where $\boldsymbol{x}, \boldsymbol{y}$ are two indeterminates, with $\deg(\boldsymbol{x}) = 1$ and $\deg(\boldsymbol{y}) = 2$, and let $S = A \otimes_K B$, so that S is a graded algebra over K having a basis formed by the elements $\boldsymbol{x}^n$ and $\boldsymbol{x}^n\boldsymbol{y}$. It is immediate that $S_{n+1} = S_1 S_n$ for $n \geq 2$, but $S_1^n = K\boldsymbol{x}^n$ while $S_n = K\boldsymbol{x}^n + K\boldsymbol{x}^{n-2}\boldsymbol{y}$ for $n \geq 2$.

23.8.3 Projective cones

Let Y be a scheme; in this subsection, we only consider Y-schemes and Y-morphisms. Let $\mathcal{S}$ be a quasi-coherent graded $\mathcal{O}_Y$-algebra with positive degrees, which we suppose that $\mathcal{S}_0 = \mathcal{O}_Y$. According to the notations of the previous part, we put

$$\widehat{\mathcal{S}} = \mathcal{S}[\boldsymbol{z}] = \mathcal{S} \otimes_{\mathcal{O}_Y} \mathcal{O}_Y[\boldsymbol{z}] \tag{8.3.1}$$

which we consider as a graded $\mathcal{O}_Y$-algebra with positive degrees, so that for any affine open subset U of Y, we have

$$\Gamma(U, \mathcal{S}) = \Gamma(U, \mathcal{S})[\boldsymbol{z}].$$

In the following, we put

$$P = \mathrm{Proj}(\mathcal{S}), \quad C = \mathrm{Spec}(\mathcal{S}), \quad \widehat{C} = \mathrm{Proj}(\widehat{\mathcal{S}})$$

(where in the definition of C, $\mathcal{S}$ is considered as a nongraded $\mathcal{O}_Y$-algebra), and we say that C (resp. $\widehat{C}$) is the **affine cone** (resp. **projective cone**) defined by $\mathcal{S}$; we will also say "cone" instead of "cone affine". By abuse of language, we sat that C (resp. $\widehat{C}$) is the **affine projecting cone** of P (resp. the **projective projecting cone** of P), which P is understood to be given of the form $\mathrm{Proj}(\mathcal{S})$. Finally, we say that $\widehat{C}$ is the projective closure of C, where C is understood to be a scheme of the form $\mathrm{Spec}(\mathcal{S})$.

Lemma 23.8.18. *Let S be a graded ring with positive degrees, $X = \operatorname{Proj}(S)$, and f be a homogeneous element of S with degree $d > 0$. If f is not a divisor of zero in S, X is the smallest closed subscheme of X such that $X_f = D_+(f)$.*

Proof. This question is clearly local on X; for any homogeneous element $g \in S_h$ ($h > 0$), it suffices to prove that X_g is the smallest closed subscheme of X_g which dominates X_{fg}. It follows from the definition and Corollary 10.4.19 that this condition is equivalent to the fact that the canonical homomorphism $S_{(g)} \to S_{(fg)}$ is injective. Now this homomorphism is identified canonically with the homomorphism $S_{(g)} \to (S_{(g)})_{f^h/g^d}$ (Lemma 23.2.1). But as f^h is not a zero divisor of S, f^h/g^e is not a zero divisor in S_g (and a fortiori in $S_{(g)}$), because the relation $(f^h/g^d)(t/g^m) = 0$ with $t \in S$ and $m > 0$ implies the existence of an integer $n > 0$ such that $g^n f^h t = 0$, whence $g^n t = 0$, and therefore $t/g^m = 0$ in S_g. This proves the claim. □

Proposition 23.8.19. *There is a commutative diagram*

$$\begin{tikzcd}
 & \widehat{C} \arrow[dd] & \\
P \arrow[ur, "j"] \arrow[dr] & & C \arrow[ul, "i"'] \arrow[dl, bend left, "\varepsilon"] \\
 & Y &
\end{tikzcd}$$

where ε and j are closed immersions and i is an affine morphism which is an open dominant immersion such that

$$i(C) = \widehat{C} - j(P). \tag{8.3.2}$$

Moreover $\widehat{C}$ is the smallest closed subscheme of $\widehat{C}$ dominating $i(C)$.

Proof. To define i, we consider the open subset $\widehat{C}_z = \operatorname{Spec}(\widehat{\mathcal{S}}/(z-1)\widehat{\mathcal{S}})$ of $\widehat{C}$ (by (8.2.4)), where z is canonically identified with a section of $\widehat{\mathcal{S}}$ over Y. The isomorphism $i : C \xrightarrow{\sim} \widehat{C}_z$ corresponds then to the canonical isomorphism

$$\widehat{\mathcal{S}}/(z-1)\widehat{\mathcal{S}} \cong \mathcal{S}$$

of (8.2.4). The morphism ε corresponds to the augmentation hommorphism $\mathcal{S} \to \mathcal{S}_0 = \mathcal{O}_Y$ with kernel $\mathcal{S}_+$, which is surjective so ε is a closed immersion (Proposition 23.1.25). Finally, j corresponds similar to the surjective homomorphism $\widehat{\mathcal{S}} \to \mathcal{S}$ of degree 0, which is the identity on $\mathcal{S}$ and zero on $z\widehat{\mathcal{S}}$. By Proposition 23.3.30 it is clear that j is everywhere defined and a closed immersion.

To prove the other assertions of the proposition, we can evidently assume that $Y = \operatorname{Spec}(A)$ is affine, $\mathcal{S} = \widetilde{S}$ where S is a graded A-algebra, whence $\widehat{\mathcal{S}} = (\widehat{S})^{\sim}$); the homogeneous elements f of S_+ are then identified with the sections of $\widehat{\mathcal{S}}$ over Y, and the open subset $D_+(f)$ of $\widehat{C}$ is identified with $\widehat{C}_f$ (Proposition 23.2.5); similarly the open subset $D(f)$ of C is identified with C_f. It then follows from Corollary 23.2.11 and the definition of $\widehat{S}$ that the open subset $\widehat{C}_z = i(C)$ together with $\widehat{C}_f$ (where f is homogeneous in S_+) constitute an open covering of $\widehat{C}$. Moreover, we have

$$i^{-1}(\widehat{C}_f) = C_f. \tag{8.3.3}$$

In fact, if we identify $i(C)$ with $\widehat{C}_{\boldsymbol{z}}$, then

$$\widehat{C}_f \cap i(C) = \widehat{C}_f \cap \widehat{C}_{\boldsymbol{z}} = \widehat{C}_{f\boldsymbol{z}} = \operatorname{Spec}(\widehat{S}_{(f\boldsymbol{z})}).$$

Now if $d = \deg(f)$, $\widehat{S}_{(f\boldsymbol{z})}$ is canonically isomorphic to $(\widehat{S}_{(\boldsymbol{z})})_{(f/\boldsymbol{z}^d)}$ (Lemma 23.2.1), and it follows from the definition of the isomorphism (8.2.4) that the image of $(\widehat{S}_{(\boldsymbol{z})})_{(f/\boldsymbol{z}^d)}$ under the corresponding isomorphism is exactly S_f. As $C_f = \operatorname{Spec}(S_f)$, this proves (8.3.3) and also shows that the morphism i is affine. Moreover, the restriction of i to C_f, considered as a morphism into $\widehat{C}_f$, corresponds (Proposition 22.2.4) to the canonical homomorphism $\widehat{S}_{(f)} \to \widehat{S}_{(f\boldsymbol{z})} \cong S_f$. We also note that under the isomorphism (8.2.5), $\widehat{C}_f$ is canonically idnetified with $\operatorname{Spec}(S_f^{\leqslant})$ and the morphism restriction $i|_{C_f} : C_f \to \widehat{C}_f$ corresponds to the canonical injection $S_f^{\leqslant} \to S_f$. The complement of $\widehat{C}_{\boldsymbol{z}}$ in $\widehat{C} = \operatorname{Proj}(\widehat{S})$ is, by definition, the set of graded prime ideals of $\widehat{S}$ containing $\boldsymbol{z}$, which is $j(P)$ from the defintion of j, whence (8.3.2).

To prove the final assertion, we can still assume that Y is affine. With the preceding notations, we note that $\boldsymbol{z}$ is not a zero divisor in $\widehat{S}$, so we can apply Lemma 23.8.18. □

We now identify the affine cone C with the open subscheme $i(C)$ of the projective cone $\widehat{C}$, which is dense in $\widehat{C}$. The closed subscheme of C associated with the closed immersion ε is called the **sommet scheme** of C. We also say that ε, which is a Y-section of C, is the **sommet section** or the **zero section** of C; we can then identify Y with the sommet scheme of C via the morphism ε. The composition $i \circ \varepsilon$ is a Y-section of $\widehat{C}$, which is also a closed immersion (Corollary 22.5.19), corresponding to the canonical surjective homomorphism $\widehat{\mathscr{S}} = \mathscr{S}[\boldsymbol{z}] \to \mathscr{O}_Y[\boldsymbol{z}]$ (cf. Remark 23.3.1), with kernel $\mathscr{S}_+[\boldsymbol{z}] = \widehat{\mathscr{S}}_+$. The closed subscheme of $\widehat{C}$ associated with this closed immersion is called the **sommet scheme** of $\widehat{C}$, which can be identified with Y via $i \circ \varepsilon$, and $i \circ \varepsilon$ is called the **sommet section** of $\widehat{C}$. Finally, the closed subscheme of $\widehat{C}$ associated with j is called the **place of infinity** of C, which is identified with P via j.

The subscheme of C (resp. $\widehat{C}$) induced respectively over the open subsets

$$E = C - \varepsilon(Y), \quad \widehat{E} = \widehat{C} - i(\varepsilon(Y)) \tag{8.3.4}$$

are called respectively (by abuse of language) the **blunt affine cone** (resp. **blunt projective cone**) defined by $\mathscr{S}$. We note that with this terminology, E is not necessarily affine over Y, nor is it projective over Y (cf. Example 23.8.25). If we identify C with $i(C)$, we then have

$$C \cup \widehat{E} = \widehat{C}, \quad C \cap \widehat{E} = E. \tag{8.3.5}$$

so that $\widehat{C}$ can be considered as obtaining by gluing the open subschemes C and $\widehat{E}$ along E; moreover, in view of (8.3.2),

$$E = \widehat{E} - j(P). \tag{8.3.6}$$

If $Y = \operatorname{Spec}(A)$ is affine, we then have (with the notations of Proposition 23.8.19),

$$E = \bigcup C_f, \quad \widehat{E} = \bigcup \widehat{C}_f, \quad C_f = C \cap \widehat{C}_f \tag{8.3.7}$$

where f runs through homogeneous elements of S_+ (or a family of homogeneous elements of

S_+ generating the ideal S_+). The glueing of C and the $\widehat{C}_f$ along the C_f is then determined by the injections $C_f \to C$, $C_f \to \widehat{C}_f$, which correspond to the cannical homomorphisms $S \to S_f$, $S_f^{\leqslant} \to S_f$. On the other hand, we note that $\bigcup \widehat{E}_f$ is the defining domain $G(\varphi)$ of the morphism associated with the canonical injection $\varphi : \mathcal{S} \to \widehat{\mathcal{S}} = \mathcal{S}[z]$, so we obtain a morphism $p : \widehat{E} \to P$.

Proposition 23.8.20. *The associated morphism $p : \widehat{E} \to P$ is an affine and surjective morphism (called the **canonical retraction**) such that*

$$p^{-1}(P_f) = \widehat{C}_f \tag{8.3.8}$$

and we have $p \circ j = 1_P$. Moreover, if Y is affine and $f \in S_1$, then $\widehat{C}_f$ is isomorphic to $P_f \otimes_{\mathbb{Z}} \mathbb{Z}[T]$ (T is an indeterminate).

Proof. To prove the proposition we may assume that Y is affine, so $\mathcal{S} = \widetilde{S}$. For any $f \in S_+$ homogeneous, by (2.5.1) we have (8.3.8) and the restriction $p : \widehat{C}_f \to P_f$ corresponds to the canonical injection $S_{(f)} \to S_f^{\leqslant}$. The formula $p \circ j = 1_P$ and the fact that p is surjective follows from the fact that the composition $\mathcal{S} \to \widehat{\mathcal{S}} \to \mathcal{S}$ is the identity on $\mathcal{S}$. Finally, the last assertion follows from the fact that $S_f^{\leqslant}$ is isomorphic to $S_{(f)}[T]$ (cf. (2.1.1)). □

Corollary 23.8.21. *The restriction $\pi : E \to P$ of p to E is a surjective and affine morphism. If Y is affine and $f \in S_+$ is homogeneous, we have*

$$\pi^{-1}(P_f) = C_f \tag{8.3.9}$$

and the restriction of $\pi|_{C_f} : C_f \to P_f$ corresponds to the cannical injection $S_{(f)} \to S_f$. If $f \in S_1$, then C_f is isomorphic to $P_f \otimes_{\mathbb{Z}} \mathbb{Z}[T, T^{-1}]$ (T is an indeterminant).

Proof. The formula (8.3.9) follows from (8.3.8) and (8.3.3), which also proves the surjectivity of π. We also have seen that the canonical injection $C_f \to \widehat{C}_f$ corresponds to $S_{(f)} \to S_f$, whence the second assertion. Finally, the last assertion is a concequence of the fact that for $f \in S_1$, S_f is isomorphic to $S_{(f)}[T, T^{-1}]$ (cf. (2.1.1)). □

Remark 23.8.3. If Y is affine, the elements of the underlying space of E are the prime ideals $\mathfrak{p}$ (not necessarily graded) of S not containing S_+, in ivew of the definition of the immersion ε. For such a prime ideal $\mathfrak{p}$, the intersections $\mathfrak{p} \cap S_n$ satisfy the conditions of Proposition 11.1.46, so there exists a graded prime ideal $\mathfrak{q}$ of S such that $\mathfrak{q} \cap S_n = \mathfrak{p} \cap S_n$ for any n. The map $\pi : E \to P$ on the underlying topological space is then interpreted by the relation

$$\pi(\mathfrak{p}) = \mathfrak{q}.$$

In fact, to verify this relation, it suffices to consider a homogeneous element f of S_+ such that $\mathfrak{p} \in D(f)$, and we then observe that $\mathfrak{q}_{(f)}$ is the inverse image of $\mathfrak{p}_f$ under the canonical injection $S_{(f)} \to S_f$.

Corollary 23.8.22. *If $\mathcal{S}$ is generated by $\mathcal{S}_1$, the morphism p and π are of finite type. Moreover, for any $x \in P$, the fiber $p^{-1}(x)$ is isomorphic to* $\operatorname{Spec}(\kappa(x)[T])$ *and $\pi^{-1}(x)$ is isomorphic to* $\operatorname{Spec}(\kappa(x)[T, T^{-1}])$.

Proof. This follows from Proposition 23.8.20 and Corollary 23.8.21, since if Y is affine and S is genrated by S_1, then the P_f for $f \in S_1$ form an open covering of P. □

Remark 23.8.4. The blunt affine cone E corresponding to the graded $\mathcal{O}_Y$-algebra $\mathcal{O}_Y[T]$ (where T is an indeterminate) is identified with $G_m = \mathrm{Spec}(\mathcal{O}_Y[T, T^{-1}])$, since it is none other than C_T as we have seen in Proposition 23.8.19. This scheme is canonically endowed with an abelian group Y-scheme structure.

Example 23.8.23. Let k be a field, $k[T_0, \dots, T_n]$ be the polynomial ring, and $\mathfrak{p}$ be a graded prime ideal of $k[T_0, \dots, T_n]$ not containing the irrelevant ideal. Consider the quotient graded ring $S = k[T_0, \dots, T_n]/\mathfrak{p}$, and set

$$P = \mathrm{Proj}(S), \quad C = \mathrm{Spec}(S), \quad \widehat{C} = \mathrm{Spec}(\widehat{S}).$$

In the language of varieties, if $V \subseteq \mathbb{P}^n_k$ is the variety defined by S, C can be viewed as the affine cone obtained by considering the lines connecting the origin with points of V. Moreover, $\widehat{C}$ is the closure of C in $\mathbb{P}^{n+1}_k$ if we embed $\mathbb{A}^{n+1}_k$ into $\mathbb{P}^{n+1}_k$ via the map $(x_0, \dots, x_n) \to [x_0 : \cdots : x_n : 1]$. Also, the morphism $j : P \to \widehat{C}$ corresponds to the injection $[x_0 : \cdots : x_n] \mapsto [x_0 : \cdots : x_n : 0]$. With these, the projective closure $\widehat{C}$ of C in $\mathbb{P}^{n+1}$ is given by the equivalent classes $[x_0 : \cdots : x_n : x_{n+1}]$ in $\mathbb{P}^{n+1}$ such that $[x_0 : \cdots : x_n] \in P$, and we can divide into two cases depending on whether $x_{n+1} \neq 0$:

(a) $(x_0, \dots, x_n) \in C$, $x_{n+1} \neq 0$;

(b) $[x_0 : \cdots : x_n] \in P$, $x_{n+1} = 0$.

Thus we see that the variety $\widehat{C}$ can be viewed as a union of P with C, which justifies the formula (8.3.2). Also, by definition the blunt affine cone E is the subvariety of C obtained by removing the origin of $\mathbb{A}^{n+1}$, and $\widehat{E}$ can be considered as a union of E and P, which is also the projective cone $\widehat{C}$ removing the point $[0 : \cdots : 0 : 1]$ in $\mathbb{P}^{n+1}$. We also remark that if we base change C through the structural morphism $P \to Y$, then the projection $C_{(P)} \to C$ can be viewed as the projection from $\mathbb{A}^{n+1} \times \mathbb{P}^n$ to $\mathbb{P}^n_k$ which maps (x, ξ) to ξ (where the class of $x \in \mathbb{A}^{n+1}_k$ is equal to ξ), and this is the blow up map of $\mathbb{A}^{n+1}_k$ at the origin.

Let Y be a scheme, $\mathscr{E}$ be a quasi-coherent $\mathcal{O}_Y$-module. If $\mathcal{S}$ is the graded $\mathcal{O}_Y$-algebra $\boldsymbol{S}_{\mathcal{O}_Y}(\mathscr{E})$, then $\widehat{\mathcal{S}}$ is identified with $\boldsymbol{S}_{\mathcal{O}_Y}(\mathscr{E} \oplus \mathcal{O}_Y)$. The affine cone $\mathrm{Spec}(\mathcal{S})$ defined by $\mathcal{S}$ is by definition the vector bundle $\boldsymbol{V}(\mathscr{E})$, and $\mathrm{Proj}(\mathcal{S})$ is by definition $\mathbb{P}(\mathscr{E})$, so we see that:

Proposition 23.8.24. *The projective closure of a vector bundle $\boldsymbol{V}(\mathscr{E})$ over Y is canonically isomorphic to $\mathbb{P}(\mathscr{E} \oplus \mathcal{O}_Y)$, and the place of infinity of this is canonically isomorphic to $\mathbb{P}(\mathscr{E})$.*

Example 23.8.25. Put for example $\mathscr{E} = \mathcal{O}_Y^r$ where $r \geq 2$. Then the blunt cones $E, \widehat{E}$ defined by $\mathcal{S}$ are neither affine nor projective over Y if $Y \neq \varnothing$. The second assertion is immediate, since $\widehat{C} = \mathbb{P}(\mathcal{O}_Y^{r+1})$ is projective over Y and the underlying spaces of E and $\widehat{E}$ are not closed in $\widehat{C}$, so the canonical immersions $E \to \widehat{C}$ and $\widehat{E} \to \widehat{C}$ are not projective (Theorem 23.5.24 and Proposition 23.5.25(v)). On the other hand, suppose that $Y = \mathrm{Spec}(A)$ is affine and for example $r = 2$; we have $C = \mathrm{Spec}(A[T_1, T_2])$ and E is the open subscheme $D(T_1) \cup D(T_2)$ of C, and we have seen that this is not affine (Example 22.5.34); a fortiori $\widehat{E}$ is not affine, since E is the open subset of $\widehat{E}$ where the section z is nonzero (8.3.5).

Proposition 23.8.26. *Let $\mathscr{L}$ be an invertible $\mathscr{O}_Y$-module, we have canonical isomorphisms for the blunt cones corresponding to $C = V(\mathscr{L})$:*

$$\operatorname{Spec}(\bigoplus_{n\in\mathbb{Z}} \mathscr{L}^n) \xrightarrow{\sim} E, \quad \boldsymbol{V}(\mathscr{L}^{-1}) \xrightarrow{\sim} \widehat{E}. \tag{8.3.10}$$

Moreover, there exists a canonical isomorphism from the projective closue of $V(\mathscr{L})$ to that of $V(\mathscr{L}^{-1})$, which transform the sommet scheme (resp. the place of infinity) of the first one to the place of infinity (resp. the sommet scheme) of the second one.

Proof. Here we have $\mathscr{S} = \bigoplus_{n\geq 0} \mathscr{L}^{\otimes n}$; the canonical injection $\mathscr{S} \to \bigoplus_{n\in\mathbb{Z}} \mathscr{L}^{\otimes n}$ defines a cannical dominant morphism

$$\operatorname{Spec}(\bigoplus_{n\in\mathbb{Z}} \mathscr{L}^{\otimes n}) \to \boldsymbol{V}(\mathscr{L}) = \operatorname{Spec}(\bigoplus_{n\geq 0} \mathscr{L}^{\otimes n}) \tag{8.3.11}$$

and it suffices to prove that this morphism is an isomorphism from $\operatorname{Spec}(\bigoplus_{n\in\mathbb{Z}} \mathscr{L}^{\otimes n})$ to E. The question is local over Y, so we can suppose that $Y = \operatorname{Spec}(A)$ is affine and $\mathscr{L} = \mathscr{O}_Y$, so $\mathscr{S} = \widetilde{A[T]}$ and $\bigoplus_{n\in\mathbb{Z}} \mathscr{L}^{\otimes n} = \widetilde{A[T, T^{-1}]}$. Now $A[T, T^{-1}]$ is the fraction ring $A[T]_T$ of $A[T]$, so (8.3.11) identify $\operatorname{Spec}(\bigoplus_{n\in\mathbb{Z}} \mathscr{L}^{\otimes n})$ as the open subscheme $D(T)$ of $C = \boldsymbol{V}(\mathscr{L})$, which by definition is E.

The isomorphism $\boldsymbol{V}(\mathscr{L}^{-1}) \cong \widehat{E}$ will on the other hand be a consequence of the last assertion, since $\boldsymbol{V}(\mathscr{L}^{-1})$ is the complement of the place of infinity of its integral closure and $\widehat{E}$ is the complement of the sommet scheme of projective closure of $C = \boldsymbol{V}(\mathscr{E})$. Now these projective closures are respectively $\mathbb{P}(\mathscr{L}^{-1} \oplus \mathscr{O}_Y)$ and $\mathbb{P}(\mathscr{L} \oplus \mathscr{O}_Y)$; but we have

$$\mathscr{L} \oplus \mathscr{O}_Y = \mathscr{L} \oplus (\mathscr{L} \otimes \mathscr{L}^{-1}) = \mathscr{L} \otimes (\mathscr{L}^{-1} \oplus \mathscr{O}_Y),$$

so the existence of the isomorphism follows from Proposition 23.4.1, and it remains to see that this isomorphism exchanges the sommet scheme and the place of infinity. For this we can assume that $Y = \operatorname{Spec}(A)$ is affine, $\mathscr{L} = \widetilde{L}$, with $L = Ac$, $L^{-1} = Ac'$, and the canonical isomorphism $L \otimes L^{-1} \to A$ sends $c \otimes c'$ to 1. Then

$$\boldsymbol{S}(L \oplus A) = A[\boldsymbol{z}] \otimes \bigoplus_{n\geq 0} Ac^{\otimes n}, \quad \boldsymbol{S}(L^{-1} \oplus A) = A[\boldsymbol{z}] \otimes \bigoplus_{n\geq 0} Ac'^{\otimes n},$$

and the isomorphism defined in Proposition 23.4.1 sends $\boldsymbol{z}^h \otimes c'^{\otimes(n-h)}$ to the element $\boldsymbol{z}^{n-h} \otimes c^{\otimes h}$. Now, in $\mathbb{P}(\mathscr{L}^{-1} \oplus \mathscr{O}_Y)$ the place of infinity is the set of points where the section $\boldsymbol{z}$ vanishes, and the sommet section is the set of points where the section c' vanishes. As we have a similary description for $\mathbb{P}(\mathscr{L} \oplus \mathscr{O}_Y)$, our conclusion follows immediately from the preceding explanations. □

23.8.4 Functorial properties

Let Y, Y' be two schemes, $q : Y' \to Y$ be a morphism, $\mathscr{S}$ (resp. $\mathscr{S}'$) be a quasi-coherent $\mathscr{O}_Y$-algebra (resp. $\mathscr{O}_{Y'}$-algebra) with positive degrees. Consider a q-morphism of graded algebras

$$\varphi : \mathscr{S} \to \mathscr{S}'.$$

We have seen that this corresponds canonically to a morphism

$$\Phi = \mathrm{Spec}(\varphi) = \mathrm{Spec}(\mathcal{S}') \to \mathrm{Spec}(\mathcal{S})$$

such that the diagram

$$\begin{tikzcd} C' \arrow[r, "\Phi"] \arrow[d] & C \arrow[d] \\ Y' \arrow[r, "q"] & Y \end{tikzcd} \tag{8.4.1}$$

where $C = \mathrm{Spec}(\mathcal{S})$, $C' = \mathrm{Spec}(\mathcal{S}')$, is commutative. Suppose moreover that $\mathcal{S}_0 = \mathcal{O}_Y$ and $\mathcal{S}'_0 = \mathcal{O}_{Y'}$; let $\varepsilon : Y \to C$ and $\varepsilon' : Y' \to C'$ be the cannical immersions, we then have a commutative diagram

$$\begin{tikzcd} C' \arrow[r, "\Phi"] & C \\ Y' \arrow[r, "q"] \arrow[u, "\varepsilon'"] & Y \arrow[u, "\varepsilon"'] \end{tikzcd} \tag{8.4.2}$$

which corresponds to the diagram

$$\begin{tikzcd} \mathcal{S} \arrow[r, "\varphi"] \arrow[d] & \mathcal{S}' \arrow[d] \\ \mathcal{O}_Y \arrow[r] & \mathcal{O}_{Y'} \end{tikzcd}$$

where the vertical are augmentation homomorphisms, and the commutativity follows from the hypotheses that φ is a homomorphism of graded algebras.

Proposition 23.8.27. *If E (resp. E') is the blunt affine cone defined by $\mathcal{S}$ (resp. $\mathcal{S}'$), we have $\Phi^{-1}(E) \subseteq E'$. Moreover, the morphism $\mathrm{Proj}(\varphi) : G(\varphi) \to \mathrm{Proj}(\mathcal{S})$ is everywhere defined (in other words $G(\varphi) = \mathrm{Proj}(\mathcal{S}')$) if and only if $\Phi^{-1}(E) = E'$.*

Proof. The first assertion followsfrom (8.4.2), since $E = C - \varepsilon(Y)$ and $E' = C' - \varepsilon'(Y')$. To prove the second assertion, we can assume that $Y = \mathrm{Spec}(A)$ and $Y' = \mathrm{Spec}(A')$ are affine, $\mathcal{S} = \widetilde{S}$, $\mathcal{S}' = \widetilde{S}'$. For f homogeneous in S_+, if we put $f' = \varphi(f)$, we have $\Phi^{-1}(C_f) = C'_{f'}$ (2.5.1); to say that $G(\varphi) = \mathrm{Proj}(S')$ signifies that in S'_+ the radical of the ideal generated by the $f' = \varphi(f)$ is equal to S'_+ (Corollary 23.2.11), and this is equivalent to that the $C'_{f'}$ cover E' (8.3.7). □

The q-morphism φ extends canonically to a q-morphism of graded algebras

$$\hat{\varphi} : \widehat{\mathcal{S}} \to \widehat{\mathcal{S}'}$$

which satisfies $\hat{\varphi}(z) = z$. We then deduce a morphism

$$\hat{\Phi} = \mathrm{Proj}(\hat{\varphi}) : G(\hat{\varphi}) \to \widehat{C} = \mathrm{Proj}(\widehat{\mathcal{S}})$$

such that the diagram

$$\begin{tikzcd} G(\hat{\varphi}) \arrow[r, "\hat{\Phi}"] \arrow[d] & \widehat{C} \arrow[d] \\ Y' \arrow[r, "q"] & Y \end{tikzcd}$$

is commutative. It then follows from the definition that if we denote by $i : C \to \widehat{C}$ and

$i' : C' \to \widehat{C}'$ are the canonical immersions, we have $i'(C') \subseteq G(\hat{\varphi})$ and the diagram

$$\begin{tikzcd} G(\hat{\varphi}) \arrow[r, "\hat{\Phi}"] & \widehat{C} \\ C' \arrow[u, "i'"] \arrow[r, "\Phi"] & C \arrow[u, "i"'] \end{tikzcd} \tag{8.4.3}$$

is commutative. Finally, if we put $P = \mathrm{Proj}(\mathscr{S})$, $P' = \mathrm{Proj}(\mathscr{S}')$, and if $j : P \to \widehat{C}$, $j' : P' \to \widehat{C}'$ are the canonical closed immersions, we have $j'(G(\varphi)) \subseteq G(\hat{\varphi})$ and the diagram

$$\begin{tikzcd} G(\hat{\varphi}) \arrow[r, "\hat{\Phi}"] & \widehat{C} \\ G(\varphi) \arrow[u, "j"] \arrow[r, "\mathrm{Proj}(\varphi)"] & P \arrow[u, "j"'] \end{tikzcd} \tag{8.4.4}$$

is commutative.

Proposition 23.8.28. *If $\widehat{E}$ (resp. $\widehat{E}'$) is the blunt projective cone defined by $\mathscr{S}$ (resp. $\mathscr{S}'$), we have $\hat{\Phi}^{-1}(\widehat{E}) \subseteq \widehat{E}'$. Moreover, if $p : \widehat{E} \to P$ and $p' : \widehat{E}' \to P'$ are the canonical retractions, we have $p'(\hat{\Phi}^{-1}(\widehat{E})) \subseteq G(\varphi)$, and the diagram*

$$\begin{tikzcd} \hat{\Phi}^{-1}(\widehat{E}) \arrow[r, "\hat{\Phi}"] \arrow[d, "p'"'] & E \arrow[d, "p"] \\ G(\varphi) \arrow[r, "\mathrm{Proj}(\varphi)"] & P \end{tikzcd}$$

is commutative. If $\mathrm{Proj}(\varphi)$ is everywhere defined, so is $\hat{\Phi}$ and we have $\hat{\Phi}^{-1}(\widehat{E}) = \widehat{E}'$.

Proof. The first assertion follows from the commutative diagrams (8.4.1) and (8.4.3), and the next two follow from the definition of the canonical retraction, the definition of $\hat{\varphi}$, and the fact that $\widehat{E}$ is the defining domain of the morphism induced by the canonical injection $\mathscr{S} \to \widehat{\mathscr{S}}$. On the other hand, to see that $\hat{\Phi}$ is everywhere defined if $\mathrm{Proj}(\varphi)$ is, we can assume that $Y = \mathrm{Spec}(A)$, $Y' = \mathrm{Spec}(A')$ are affine, $\mathscr{S} = \widetilde{S}$, $\mathscr{S}' = \widetilde{S}'$; the hypothesis is that if f runs through homogeneous elements of S_+, the ideal in S'_+ generated by the $\varphi(f)$ has radical in S'_+ equal to S'_+. We then conclude that the radical of the ideal genrated by z and the $\varphi(f)$ in $(S'[z])_+$ is equal to $(S'[z])_+$, whence our assertion. This proves similarly that $\widehat{E}'$ is the union of the $\widehat{C}'_{(\varphi(f))'}$ which is equal to $\hat{\Phi}^{-1}(\widehat{E})$. □

Corollary 23.8.29. *If Φ is everywhere defined, the inverse image under $\hat{\Phi}$ of underlying space of the place of infinity (resp. the sommet scheme) of $\widehat{C}'$ is the underlying space of the place of infinity (resp. the sommet scheme) of $\widehat{C}$.*

Proof. This follows from Proposition 23.8.28 and Proposition 23.8.27, in ivew of the relations (8.3.4) and (8.3.4). □

23.8.5 Blunt cones over a homogeneous specturm

Let Y be a scheme, $\mathscr{S}$ be a quasi-coherent $\mathscr{O}_Y$-algebra with positive degrees such that $\mathscr{S}_0 = \mathscr{O}_Y$, and $X = \mathrm{Proj}(\mathscr{S})$. We now apply the previous results to the structure morphism $q : X \to Y$.

Let

$$\mathcal{S}_X = \bigoplus_{n\in\mathbb{Z}} \mathcal{O}_X(n) \tag{8.5.1}$$

which is a quasi-coherent $\mathcal{O}_X$-algebra, the multiplication γ being defined by the canonical homomorphisms

$$\mathcal{O}_X(m) \otimes \mathcal{O}_X(n) \to \mathcal{O}_X(m+n)$$

which satisfies the associativity in view of Proposition 23.3.15. Let $\mathcal{S}'$ be the quasi-coherent sub-algebra

$$\mathcal{S}_X^{\geqslant} = \bigoplus_{n\geq 0} \mathcal{O}_X(n)$$

of $\mathcal{S}_X$, with positive degrees. For each $n \in \mathbb{Z}$, we have a canonical q-morphisms $\alpha_n : \mathcal{S}_n \to \mathcal{O}_X(n)$ defined in (3.3.1), which together give a homomorphism

$$\alpha : \mathcal{S} \to \bigoplus_{n\geq 0} q_*(\mathcal{O}_X(n)).$$

By composing with the canonical homomorphism $\bigoplus_{n\geq 0} q_*(\mathcal{O}_X(n)) \to q_*(\mathcal{S}_X^{\geqslant})$, this gives a q-homomorphism $\mathcal{S} \to \mathcal{S}_X^{\geqslant}$, still denoted by α. We set

$$C_X = \operatorname{Spec}(\mathcal{S}_X^{\geqslant}), \quad \widehat{C}_X = \operatorname{Proj}(\mathcal{S}_X^{\geqslant}[z]), \quad P_X = \operatorname{Proj}(\mathcal{S}_X^{\geqslant})$$

and denote by E_X and $\widehat{E}_X$ the corresponding blunt cones. We then have the canonical morphisms

$$\begin{tikzcd}
 & \widehat{C}_X \arrow[dd, "\varepsilon_X"] & \\
P_X \arrow[ur, "j_X"] \arrow[dr] & & C_X \arrow[ul, "i_X"'] \arrow[dl, bend left] \\
 & X \arrow[ur, bend left] &
\end{tikzcd}$$

and $p_X : \widehat{E}_X \to P_X$, $\pi_X : E_X \to P_X$.

Proposition 23.8.30. *The structural morphism $\psi : P_X \to X$ is an isomorphism, and the morphism* $\operatorname{Proj}(\alpha)$ *is everywhere defined and equals to ψ. The morphism* $\operatorname{Proj}(\hat{\alpha}) : \widehat{C}_X \to \widehat{C}$ *is everywhere defined and its restriction to $\widehat{E}_X$ and E_X are isomorphisms into $\widehat{E}$ and E, respectively. Finally, if we identify P_X and X via ψ, the morphisms p_X and π_X are identified with the structural morphisms of the X-schemes $\widehat{E}_X$ and E_X.*

Proof. We can clearly assume that $Y = \operatorname{Spec}(A)$ is affine and $\mathcal{S} = \widetilde{S}$; then X is the union of the affine opens X_f, where $f \in S_+$ is homogeneous, the ring of X_f being $S_{(f)}$. It follows from the isomorphism (8.2.8) that

$$\Gamma(X_f, \mathcal{S}_X^{\geqslant}) = S_f^{\geqslant}. \tag{8.5.2}$$

We then have $\psi^{-1}(X_f) = \operatorname{Proj}(S_f^{\geqslant})$. But if $f \in S_d$ with $d > 0$, $\operatorname{Proj}(S_f^{\geqslant})$ is canonically isomorphic to $\operatorname{Proj}((S_f^{\geqslant})^{(d)})$ by Remark 23.3.2, and $(S_f^{\geqslant})^{(d)} = (S^{(d)})_f^{\geqslant}$ is identified with $S_{(f)}[T]$ by the map $T \mapsto$

$f/1$ (cf. (2.1.1)), so we conclude from Remark 23.3.1 that the structural morphism $\psi^{-1}(X_f) \to X_f$ is an isomorphism, whence the first assertion. To prove the second one, we first note that $\mathrm{Proj}(\alpha)$ is everywhere defined by Lemma 23.8.14. Since $\psi^{-1}(X_f) = (\psi^{-1}(X_f))_{f/1}$, it follows from (2.5.1) that the image of $\psi^{-1}(X_f)$ under $\mathrm{Proj}(\alpha)$ is contained in X_f, and the restriction of $\mathrm{Proj}(\alpha)$ to $\psi^{-1}(X_f)$, considered as a morphism into $X_f = \mathrm{Spec}(S_{(f)})$, is identified with ψ. Finally, the formula (8.3.8) and (8.2.5) show that $p_X^{-1}(\psi^{-1}(X_f)) = \mathrm{Spec}((S_f^{\geqslant})_{f/1}^{\leqslant})$, and this open subset is, by Proposition 23.8.28 and formula (8.3.8), the inverse image of $p^{-1}(X_f) = \mathrm{Spec}(S_f^{\leqslant})$ under $\mathrm{Proj}(\hat{\alpha})$. By the isomorphism (8.2.5), the restriction of $\mathrm{Proj}(\hat{\alpha})$ to $p_X^{-1}(\psi^{-1}(X_f))$ corresponds to the isomorphism $S_f^{\leqslant} \cong (S_f^{\geqslant})_{f/1}^{\leqslant}$, whence the third assertion. The last assertion is clear by definition. □

We note that by (8.4.3) the restriction of $\mathrm{Proj}(\hat{\alpha})$ to C_X is equal to $\mathrm{Spec}(\alpha)$.

Corollary 23.8.31. *Considered as X-schemes, $\widehat{E}_X$ is canonically isomorphic to $\mathrm{Spec}(\mathscr{S}_X^{\leqslant})$, E_X is canonically isomorphic to $\mathrm{Spec}(\mathscr{S}_X)$, and C_X is canonically isomorphic to $\mathrm{Spec}(\mathscr{S}_X^{\geqslant})$.*

Proof. As we have seen that p_X and π_X are affine, it suffices to verify the corollary if $Y = \mathrm{Spec}(A)$ is affine and $\mathscr{S} = \widetilde{S}$. The first assertion follows from the canonical isomorphism $(S_f^{\geqslant})_{f/1}^{\leqslant} \cong S_f^{\leqslant}$, which are compatible with passage from f to fg (f, g homogeneous in S_+). Similarly, the formula (8.3.9), applied to π_X, shows that $\pi_X^{-1}(\psi^{-1}(X_f)) = \mathrm{Spec}((S_f^{\geqslant})_{f/1})$ for f homogeneous in S_+, and the second assertion then follows from the canonical isomorphism $(S_f^{\geqslant})_{f/1} \cong S_f$. □

We can then say that $\widehat{C}_X$, considered as an X-scheme, is obtained by glueing the affine X-schemes $C_X = \mathrm{Spec}(\mathscr{S}_X^{\geqslant})$ and $\widehat{E}_X = \mathrm{Spec}(\mathscr{S}_X^{\leqslant})$ along their intersection $E_X = \mathrm{Spec}(\mathscr{S}_X)$.

Corollary 23.8.32. *Suppose that $\mathscr{O}_X(1)$ is an invertible $\mathscr{O}_X$-module and that $\mathscr{S}_X \cong \bigoplus_{n\in\mathbb{Z}}(\mathscr{O}_X(1))^{\otimes n}$ (for example if $\mathscr{S}$ is generated by $\mathscr{S}_1$). Then the blunt projective cone $\widehat{E}$ is identified with the rank one vector bundle $\boldsymbol{V}(\mathscr{O}_X(-1))$ over X, and the bulnk affine cone E is isomorphic to the open subscheme induced over the complement of the zero section in this vector bundle. With these indentifications, the canonical retraction $\widehat{E} \to X$ is identified with the structural morphism of the X-scheme $\boldsymbol{V}(\mathscr{O}_X(-1))$. Finally, there exists a canonical Y-morphism $\boldsymbol{V}(\mathscr{O}_X(1)) \to C$, whose restriction to the complement of the zero section of $\boldsymbol{V}(\mathscr{O}_X(1))$ is an isomorphism from this complement to the blunt affine cone E.*

Proof. In fact, if $\mathscr{L} = \mathscr{O}_X(1)$, then $\mathscr{S}_X^{\geqslant}$ is identified with $\boldsymbol{S}_{\mathscr{O}_X}(\mathscr{L})$ and $\mathscr{S}_X^{\leqslant}$ is identified with $\boldsymbol{S}_{\mathscr{O}_X}(\mathscr{L}^{-1})$, so $\widehat{E}_X$ is identified with $\boldsymbol{V}(\mathscr{L}^{-1})$ in view of Corollary 23.8.31 and C_X is identified with $\boldsymbol{V}(\mathscr{L})$. The morphism $\boldsymbol{V}(\mathscr{L}) \to C$ is the restriction of $\mathrm{Proj}(\hat{\alpha})$, and the assertion of the corollary is a particular case of Proposition 23.8.30. □

We note that the inverse image of the sommet scheme of C under the morphism $\boldsymbol{V}(\mathscr{O}_X(1)) \to C$ is the zero section of $\boldsymbol{V}(\mathscr{O}_X(1))$ (Corollary 23.8.29). But in general the corresponding subschemes of C and of $\boldsymbol{V}(\mathscr{O}_X(1))$ are not isomorphic.

23.8.6 Blow up of projective cones

With the notations of the previous subsection, we have a commutative diagram

$$\begin{tikzcd} \widehat{C}_X \arrow[r, "r"] & \widehat{C} \\ X \arrow[u, "i_X\circ\varepsilon_X"] \arrow[r, "q"] & Y \arrow[u, "i\circ\varepsilon"'] \end{tikzcd}$$

where $r = \mathrm{Proj}(\hat{\alpha})$. Moreover, the restriction of r to the complement $\widehat{C}_X - i_X(\varepsilon_X(X))$ of the sommet section is an isomorphism to $\widehat{C} - i(\varepsilon(Y))$ of the sommet section in view of Proposition 23.8.30. If we suppose for simplicity that Y is affine, $\mathcal{S}$ is of finite type and generated by $\mathcal{S}_1$, X is projective over Y and $\widehat{C}_X$ is projective over X, so $\widehat{C}_X$ is projective over Y (Proposition 23.5.25(ii)), and a fortiori over $\widehat{C}$ (Proposition 23.5.25(v)). We thus have a projective Y-morphism $r : \widehat{C}_X \to \widehat{C}$ (hence restricts to a projective Y-morphism $C_X \to C$) which contract X to Y and induces an isomorphism when restricted to the complement of X and of Y. We therefore have a relation between C_X and C, analogous to that which takes place between a blow up scheme and its initial scheme. We will effectively show that we can identify C_X with the homogeneous spectrum of a graded $\mathcal{O}_C$-algebra.

For each $n \geq 0$, we consider the quasi-coherent ideal

$$\mathcal{S}(n) = \bigoplus_{m\geq n} \mathcal{S}_m$$

of the graded $\mathcal{O}_Y$-algebra of $\mathcal{S}$. It is clear that $(\mathcal{S}(n))_{n\geq 0}$ is a filtered sequence of ideals of $\mathcal{S}$. Consider the $\mathcal{O}_C$-module associated with $\mathcal{S}(n)$, which is a quasi-coherent ideal of $\mathcal{O}_C = \widetilde{\mathcal{S}}$:

$$\mathcal{I}_n = \widetilde{\mathcal{S}(n)}.$$

Then $(\mathcal{I}_n)$ is also a filtered sequence of quasi-coherent $\mathcal{O}_C$-ideals, so we can consider the quasi-coherent graded $\mathcal{O}_C$-algebra

$$\mathcal{S}^\natural = \bigoplus_{n\geq 0} \mathcal{I}_n = \Big(\bigoplus_{n\geq 0} \mathcal{S}(n)\Big)^{\sim}.$$

Proposition 23.8.33. *There exists a canonical C-isomorphism*

$$h : C_X \to \mathrm{Proj}(\mathcal{S}^\natural). \tag{8.6.1}$$

Proof. Suppose first that $Y = \mathrm{Spec}(A)$ is affine, so $\mathcal{S} = \widetilde{S}$ where S is a graded A-algebra with positive degrees and $C = \mathrm{Spec}(S)$. We then have $\mathcal{S}^\natural = \widetilde{(S^\natural)}$. To define the morphism h, consider an element $f \in S_d$ $(d > 0)$ and the corresponding element $f^\natural \in S^\natural$; the S-isomorphism (8.2.10) defines a C-isomorphism

$$\mathrm{Spec}(S_f^{\geqslant}) \xrightarrow{\sim} \mathrm{Spec}(S^\natural_{(f^\natural)}). \tag{8.6.2}$$

But with the notations of Proposition 23.8.30, if $\varphi : C_X \to X$ is the structural morphism, it follows from (8.5.2) that $\varphi^{-1}(X_f) = \mathrm{Spec}(S_f^{\geqslant})$. We have on the other hand $D_+(f^\natural) = \mathrm{Spec}(S^\natural_{(f^\natural)})$,

so that (8.6.2) define an isomorphism $v^{-1}(X_f) \to D_+(f^\natural)$. Moreover, if $g \in S_e$ with $e > 0$, the diagram

$$\begin{tikzcd} \varphi^{-1}(X_{fg}) \arrow[r, "\sim"] \arrow[d] & D_+(f^\natural g^\natural) \arrow[d] \\ \varphi^{-1}(X_f) \arrow[r, "\sim"] & D_+(f^\natural) \end{tikzcd}$$

is commutative, which is clear from the definition of (8.2.10). By definition S_+ is generated by these homogeneous elements F, so it follows from Lemma 23.8.14(iv) that the $D_+(f^\natural)$ form a covering of $\operatorname{Proj}(S^\natural)$ and the $\varphi^{-1}(X_f)$ form a covering of C_X, if X_f form a covering of X. These together gives a isomorphism $h : C_X \to \operatorname{Proj}(\mathscr{S}^\natural)$.

To prove the proposition in the general case, it suffices to see that if U, U' are two affine opens of Y such that $U' \subseteq U$, with rings A and A', and if $\mathscr{S}|_U = \widetilde{S}$, $\mathscr{S}|_{U'} = \widetilde{S}'$, the diagram

$$\begin{tikzcd} C_{U'} \arrow[r] \arrow[d] & \operatorname{Proj}(S^\natural) \arrow[d] \\ C_U \arrow[r] & \operatorname{Proj}(S^\natural) \end{tikzcd} \tag{8.6.3}$$

is commutative. But S' is canonically identified with $S \otimes_A A'$, so $S'^\natural$ is identified with $S^\natural \otimes_S S' = S^\natural \otimes_A A'$ and we then have $\operatorname{Proj}(S'^\natural) = \operatorname{Proj}(S^\natural) \times_U U'$ (Proposition 23.2.48). Similarly, if $X = \operatorname{Proj}(S)$ and $X' = \operatorname{Proj}(S')$, we have $X' = X \times_U U'$ and $\mathscr{S}_{X'} = \mathscr{S}_X \otimes_{\mathscr{O}_U} \mathscr{O}_{U'}$ (Corollary 23.3.29), which means $\mathscr{S}_{X'} = j^*(\mathscr{S}_X)$, where $j : X' \to X$ is the projection. By Corollary 23.1.28 we then have $C_{U'} = C_U \times_X X' = C_U \times_U U'$, and the commutativity of (8.6.3) is immediate. □

Remark 23.8.5. The end of the reasoning of Proposition 23.8.33 is immediately generalized in the following way.: let $g : Y' \to Y$ be a morphism, $\mathscr{S}' = g^*(\mathscr{S})$, $X' = \operatorname{Proj}(\mathscr{S}')$; we then have a commutative diagram

$$\begin{tikzcd} C_{X'} \arrow[r] \arrow[d] & \operatorname{Proj}(\mathscr{S}'^\natural) \arrow[d] \\ C_X \arrow[r] & \operatorname{Proj}(\mathscr{S}^\natural) \end{tikzcd} \tag{8.6.4}$$

On the other hand, let $\varphi : \mathscr{S}'' \to \mathscr{S}$ be a homomorphism of graded $\mathscr{O}_Y$-algebras such that the induced morphism $\Phi = \operatorname{Proj}(\varphi) : X \to X''$ is everywhere defined, where $X'' = \operatorname{Proj}(\mathscr{S}'')$. We have an Y-morphism $v : C \to C''$ (where $C'' = \operatorname{Spec}(\mathscr{S}'')$) such that $\mathscr{A}(v) = \varphi$, and as φ is a graded homomorphism, we deduce from φ a v-morphism $\psi : \mathscr{S}''^\natural \to \mathscr{S}^\natural$ (Proposition 23.1.16). Moreover, it follows from Lemma 23.8.14(iv) and the hypotheses on φ that $\Psi = \operatorname{Proj}(\psi)$ is everywhere defined. Finally, in view of (3.4.5), we have a canonical Φ-morphism $\mathscr{S}_{X''} \to \mathscr{S}_X$, whence a morphism $w : C_{X''} \to C_X$. The diagram

$$\begin{tikzcd} C_{X''} \arrow[r, "\sim"] \arrow[d, "w"] & \operatorname{Proj}(\mathscr{S}^\natural) \arrow[d, "\Psi"] \\ C_X \arrow[r, "\sim"] & \operatorname{Proj}(\mathscr{S}^\natural) \end{tikzcd}$$

is commutative, as can be verified in the case where Y is affine.

Remark 23.8.6. Recall that $(\mathscr{I}_n)_{n\geq 0}$ is a filtered sequence where $\mathscr{I}_n = \mathscr{S}(n)$, so we have $\mathscr{I}_1^n \subseteq$

$\mathscr{I}_n \subseteq \mathscr{I}_1$ for any $n > 0$. Now by definition, $\mathscr{I}_1 = \widetilde{\mathscr{S}_+}$, so $\mathscr{I}_1$ defines in C the closed subscheme $\varepsilon(Y)$ (Proposition 23.1.25 and Proposition 23.8.19). We then conclude that for any $n > 0$, the support of $\mathscr{O}_C/\mathscr{I}_n$ is contained in the underlying space of tge sommet scheme $\varepsilon(Y)$. In the inverse image of the blunt affine cone E, the structural morphism $\operatorname{Proj}(\mathscr{S}^\natural) \to C$ reduces to an isomorphism (as it follows from Proposition 23.8.33 and Proposition 23.8.30). Moreover, if we canonically identify C as a dense open subset of $\widehat{C}$, we can evidently extend the ideal $\mathscr{I}_n$ of $\mathscr{O}_C$ to an ideal $\mathscr{J}_n$ of $\mathscr{O}_{\widehat{C}}$, such that it coincides with $\mathscr{O}_{\widehat{C}}$ on the open subset $\widehat{E}$ of $\widehat{C}$. If we put $\mathscr{T} = \bigoplus_{n\geq 0} \mathscr{J}_n$, which is a graded $\mathscr{O}_{\widehat{C}}$-algebra, we can then extend the isomorphism (8.6.1) into a $\widehat{C}$-isomorphism

$$\widehat{C}_X \xrightarrow{\sim} \operatorname{Proj}(\mathscr{T}). \tag{8.6.5}$$

In fact, over $\widehat{E}$, it follows from the definition of $\mathscr{J}$ that $\operatorname{Proj}(\mathscr{T})$ is identified with $\widehat{E}$, and we therefore define the isomorphism (8.6.5) so that it coincides with the canonical isomorphism $\widehat{E}_X \to \widehat{E}$ on $\widehat{E}$ (Proposition 23.8.30); it is then clear that this isomorphism and (8.6.1) coincides over $\widehat{E}$.

Corollary 23.8.34. *Suppose that there exists $n_0 > 0$ such that $\mathscr{S}_{n+1} = \mathscr{S}_1\mathscr{S}_n$ for $n \geq n_0$. Then the sommet scheme of C_X (isomorphic to X) is the inverse image of the sommet scheme of C (isomorphic to Y) under the canonical morphism $r = \operatorname{Proj}(\alpha) : C_X \to C$. The converse of this is true if moreover Y is Noetherian and $\mathscr{S}$ is of finite type.*

Proof. The first assertion is local over Y, so we can assume that $Y = \operatorname{Spec}(A)$ is affine, $\mathscr{S} = \widetilde{S}$ where S is a graded A-algebra with positive degrees. This then follows from Proposition 23.8.15, because we have

$$\operatorname{Proj}(S^\natural \otimes_S S_0) = \operatorname{Proj}(S^\natural \otimes_S (S/S_+)) = C_X \times_C \varepsilon(Y)$$

(in view of the identification (8.6.1) and Proposition 23.2.48), which is also the inverse image of $\varepsilon(Y)$ in C_X under the morphism $r : C_X \to C$. The converse of this also follows from Proposition 23.8.15 if Y is Noetherian and affine and S is of finite type. If Y is Noetherian (not necessarily affine) and $\mathscr{S}$ is of finite type, there exists a finite convering of Y by Noetherian affine covers U_i, and we then deduce that for each i, there is an integer n_i such that $\mathscr{S}_{n+1}|_{U_i} = (\mathscr{S}_1|_U)(\mathscr{S}_n|_U)$ for $n \geq n_i$; the largest integer n_0 of the n_i then satisfies the requirement. □

We now consider the C-scheme $\widetilde{C}$ with is obtained by blowing up the affine cone C along the sommet scheme $\varepsilon(Y)$. By definiton this is $\operatorname{Proj}(\bigoplus_{n\geq 0}(\mathscr{S}_+)^n)$; the canonical injection

$$\iota : \bigoplus_{n\geq 0}(\mathscr{S}_+)^n \to \mathscr{S}^\natural$$

defines (by the identification of (8.6.1)) a canonical dominant C-morphism $\operatorname{Proj}(\iota) : G(\iota) \to \widetilde{C}$, where $G(\iota)$ is an open subset of C_X. We note that it is possible that $G(\iota) \neq C_X$; for example, $Y = \operatorname{Spec}(k)$ where k is a field, $\mathscr{S} = \widetilde{S}$ where $S = k[\boldsymbol{y}]$ and $\boldsymbol{y}$ is an indeterminate of degree 2. If R_n is the set $(S_+)^n$, considered as a subset of $S(n) = S_n^\natural$, then $S_+^\natural$ is not equal to the radical in $S_+^\natural$ of the ideal generated by the R_n.

Corollary 23.8.35. *Suppose that there exists $n_0 > 0$ such that $\mathscr{S}_n = \mathscr{S}_1^n$ for $n \geq n_0$. Then the canonical morphism $\operatorname{Proj}(\iota) : G(\iota) \to \widetilde{C}$ is everywhere defined and an isomorphism from C_X to $\widetilde{C}$. The converse of this is also ture if moreover Y is Noetherian and $\mathscr{S}$ is of finite type.*

Proof. This assertion is local over Y, and therefore follows from Proposition 23.8.16. The converse of this is also true if Y is Noetherian and $\mathcal{S}$ is of finite type, as can be shown similarly to Corollary 23.8.34. □

Remark 23.8.7. As the condition of Corollary 23.8.35 implies that of Corollary 23.8.34, we see that if this condition is verified, not only C_X is identified with the scheme obtained by blowing up C along the sommet scheme (isomorphic to Y), but also the sommet scheme of C_X (isomorphic to X) is identified with the inverse image of the sommet scheme of C in C_X. Moreover, the hypothesis of Corollary 23.8.35 implies that over $X = \mathrm{Proj}(\mathcal{S})$, the $\mathcal{O}_X$-modules $\mathcal{O}_X(n)$ are invertible (Proposition 23.3.14) and we have $\mathcal{O}_X(n) = \mathcal{L}^{\otimes n}$, where $\mathcal{L} = \mathcal{O}_X(1)$ (Corollary 23.3.16). By definition C_X is then the vector bundle $\boldsymbol{V}(\mathcal{L})$ over X, and the sommet scheme is the zero section of this vector bundle.

23.8.7 Ample sheaves and contractions

Let Y be a scheme, $f : X \to Y$ be a quasi-compact and quasi-separated morphism $\mathcal{L}$ be an ample inveritble $\mathcal{O}_X$-module realtive to f. Consider the graded $\mathcal{O}_Y$-algebra with positive degrees

$$\mathcal{S} = \mathcal{O}_Y \oplus \bigoplus_{n\geq 1} f_*(\mathcal{L}^{\otimes n})$$

which is quasi-coherent by Proposition 22.6.54. We have a canonical homomorphism of graded $\mathcal{O}_X$-algebras

$$\sigma : f^*(\mathcal{S}) \to \bigoplus_{n\geq 0} \mathcal{L}^{\otimes n}$$

which, for each $n \geq 1$, coincides with the canonical homomorphism $\sigma_n : f^*(f_*(\mathcal{L}^{\otimes n})) \to \mathcal{L}^{\otimes n}$, and for $n = 0$ is the identify on $\mathcal{O}_X$. The hypothesis that $\mathcal{L}$ is f-ample implies that (Proposition 23.4.34 and Proposition 23.3.22) the corresponding Y-morphism

$$r = r_{\mathcal{L},\sigma} : X \to P = \mathrm{Proj}(\mathcal{S})$$

is everywhere defined and a dominant open immersion, and we have $\mathcal{L}^{\otimes n} = r^*(\mathcal{O}_P(n))$ for $n \in \mathbb{Z}$.

Proposition 23.8.36. *Let $C = \mathrm{Spec}(\mathcal{S})$ the affine cone defined by $\mathcal{S}$. If $\mathcal{L}$ is f-ample, there exists a canonical Y-morphism*

$$g : V = \boldsymbol{V}(\mathcal{L}) \to C \tag{8.7.1}$$

such that the diagram

$$\begin{tikzcd} X \arrow[r, "j"] \arrow[d, "f"'] & \boldsymbol{V}(\mathcal{L}) \arrow[r, "\pi"] \arrow[d, "g"] & X \arrow[d, "f"] \\ Y \arrow[r, "\varepsilon"] & C \arrow[r, "\psi"] & Y \end{tikzcd} \tag{8.7.2}$$

is commutative, where ψ and π are structural morphisms, j and ε are the canonical immersions which maps X and Y respectively to the zero section of $\boldsymbol{V}(\mathcal{L})$ and the sommet scheme of C. Moreover, the

restriction of g to $\boldsymbol{V}(\mathscr{L}) - j(X)$ is an open immersion

$$\boldsymbol{V}(\mathscr{L}) - j(X) \to E = C - \varepsilon(Y)$$

into the blunt affine cone E corresponding to $\mathscr{S}$.

23.8.8 Quasi-coherent sheaves over the projective cone

Let Y be a scheme, $\mathscr{S}$ be a quasi-coherent graded $\mathscr{O}_Y$-algebra, $X = \operatorname{Proj}(\mathscr{S})$, $C = \operatorname{Spec}(\mathscr{S})$ and $\widehat{C} = \operatorname{Proj}(\widehat{\mathscr{S}})$. Let $\mathscr{M}$ be a quasi-coherent graded $\mathscr{S}$-module; to avoid any possible confusion, we denote by $\widetilde{\mathscr{M}}$ the quasi-coherent $\mathscr{O}_C$-module associated with $\mathscr{M}$ if $\mathscr{M}$ is considered as a *non-graded* $\mathscr{S}$-module, and by $\mathscr{P}roj_0(\mathscr{M})$ the quasi-coherent $\mathscr{O}_X$-module associated with $\mathscr{M}$, where $\mathscr{M}$ is considered as a graded $\mathscr{S}$-module. We also set

$$\mathscr{M}_X = \mathscr{P}roj(\mathscr{M}) = \bigoplus_{n\in\mathbb{Z}} \mathscr{P}roj_0(\mathscr{M}(n));$$

with the quasi-coherent $\mathscr{O}_X$-algebra being defined by (8.5.1), $\mathscr{P}roj(\mathscr{M})$ is endowed a quasi-coherent graded $\mathscr{S}_X$-module structure, via the canonical homomorphisms

$$\mathscr{O}_X(m) \otimes_{\mathscr{O}_X} \mathscr{P}roj_0(\mathscr{M}(n)) \to \mathscr{P}roj_0(\mathscr{S}(m) \otimes_{\mathscr{S}} \mathscr{M}(n)) \to \operatorname{Proj}_0(\mathscr{M}(m+n))$$

which satisfies the axioms of modules in view of the commutative diagram (2.3.2). If $Y = \operatorname{Spec}(A)$ is affine, $\mathscr{S} = \widetilde{S}$ and $\mathscr{M} = \widetilde{M}$, where S is a graded A-algebra and M is a graded S-module, then for any homogeneous element $f \in S_+$, we have

$$\Gamma(X_f, \mathscr{P}roj(\mathscr{M})) = M_f$$

in view of the definition and (8.2.11).

Now consider the quasi-coherent graded $\widehat{\mathscr{S}}$-module

$$\widehat{\mathscr{M}} = \mathscr{M} \otimes_{\mathscr{S}} \widehat{\mathscr{S}}$$

(where $\widehat{\mathscr{S}} = \mathscr{S}[T] = \mathscr{S} \otimes_{\mathbb{Z}} \mathbb{Z}[T]$); we then deduce a quasi-coherent graded $\mathscr{O}_{\widehat{C}}$-module $\mathscr{P}roj_0(\widehat{\mathscr{M}})$ (recall that $\widehat{C} = \operatorname{Proj}(\widehat{\mathscr{S}})$), which we also denote by

$$\mathscr{M}^{\square} = \mathscr{P}roj_0(\widehat{\mathscr{M}}).$$

It is clear that $\mathscr{M}^{\square}$ is an exact functor on $\mathscr{M}$ and commutes with inductive limits and direct sums.

Proposition 23.8.37. *With the notations of Proposition 23.8.19 and Proposition 23.8.20, we have canonical homomorphisms*

$$i^*(\mathscr{M}^{\square}) \xrightarrow{\sim} \widetilde{\mathscr{M}}, \tag{8.8.1}$$

$$j^*(\mathscr{M}^{\square}) \to \mathscr{P}roj_0(\mathscr{M}), \tag{8.8.2}$$

$$p^*(\mathscr{P}roj_0(\mathscr{M})) \to \mathscr{M}^{\square}|_{\widehat{E}} \tag{8.8.3}$$

Moreover, the homomorphism (8.8.2) is an isomorphism if $\mathscr{S}$ is generated by $\mathscr{S}_1$.

Proof. In fact, $i^*(\mathscr{M}^\square)$ is canonically identified with $(\widehat{\mathscr{M}}/(z-1)\widehat{\mathscr{M}})^\sim$ over $\operatorname{Spec}(\widehat{\mathscr{S}}/(z-1)\widehat{\mathscr{S}})$ in view of Proposition 23.3.12 and the definition of i. The first isomorphism of (8.8.1) is then deduced from Proposition 23.1.16 and the canonical isomorphism $\widehat{\mathscr{M}}/(z-1)\widehat{\mathscr{M}} \cong \mathscr{M}$. On the other hand, the canonical immersion $j : X \to \widehat{C}$ corresponds to the canonical homomorphism $\widehat{\mathscr{S}} \to \mathscr{S}$ with kernel $z\widehat{\mathscr{S}}$, so the second isomorphism is a particular case of the canonical homomorphism of Proposition 23.3.27, using the fact that $\widehat{\mathscr{M}} \otimes_{\widehat{S}} \mathscr{S} = \mathscr{M}$. Finally, the homomorphism of (8.8.3) is a particular case of the homomorphisms $v^\sharp$ defined in (3.4.4). If $Y = \operatorname{Spec}(A)$ is affine, $\mathscr{S} = \widetilde{S}$, $\mathscr{M} = \widetilde{M}$, then we see from Proposition 23.2.47 that the restriction of (8.8.3) to $p^{-1}(X_f) = \widehat{C}_f$ (for $f \in S_+$ homogeneous) corresponds to the canonical homomorphism

$$M_{(f)} \otimes_{S_{(f)}} S_f^{\leqslant} \to M_f^{\leqslant}$$

in view of (8.2.5) and (8.2.7). The last assertion also follows from Proposition 23.3.27. □

By abuse of language, we say that $\mathscr{M}^\square$ is the projective closure of the $\mathscr{O}_C$-module $\widetilde{\mathscr{M}}$, where $\mathscr{M}$ is understood to be a graded $\mathscr{S}$-module.

Let us consider a morphism $q : Y' \to Y$ and a q-homomorphism $\varphi : \mathscr{S} \to \mathscr{S}'$. It then follows from (1.4.2) that for any quasi-coherent graded $\mathscr{S}$-module $\mathscr{M}$, we have a canonical isomorphism

$$\Phi^*(\widetilde{\mathscr{M}}) \xrightarrow{\sim} (q^*(\mathscr{M}) \otimes_{q^*(\mathscr{S})} \mathscr{S}')^\sim$$

of $\mathscr{O}_C$-modules, where $\Phi = \operatorname{Spec}(\varphi)$. On the other hand, if $w = \operatorname{Proj}(\varphi)$ and $\hat{\Phi} = \operatorname{Proj}(\hat{\varphi})$, (3.4.3) gives a canonical w-homomorphism

$$\mathscr{P}roj_0(\mathscr{M}) \to (\mathscr{P}roj_0(q^*(\mathscr{M}) \otimes_{q^*(\mathscr{S})} \mathscr{S}'))|_{G(\varphi)} \tag{8.8.4}$$

and also a canonical $\hat{\Phi}$-morphism

$$\mathscr{P}roj_0(\widehat{\mathscr{M}}) \to (\mathscr{P}roj_0(q^*(\widehat{\mathscr{M}}) \otimes_{q^*(\widehat{\mathscr{S}})} \widehat{\mathscr{S}}'))|_{G(\hat{\varphi})}. \tag{8.8.5}$$

Now we consider the situation of the structural morphism $q : X \to Y$, where $X = \operatorname{Proj}(\mathscr{S})$, with the canonical q-homomorphism $\alpha : \mathscr{S} \to \mathscr{S}_X^{\geqslant}$. We then have a canonical isomorphism

$$q^*(\mathscr{M}) \otimes_{q^*(\mathscr{S})} \mathscr{S}_X^{\geqslant} \xrightarrow{\sim} \mathscr{M}_X^{\geqslant} \tag{8.8.6}$$

where $\mathscr{M}_X^{\geqslant} = \bigoplus_{n\geq 0} \mathscr{P}roj_0(\mathscr{M}(n))$. To see this, we can assume that $Y = \operatorname{Spec}(A)$ is affine, $\mathscr{S} = \widetilde{S}$ and $\mathscr{M} = \widetilde{M}$, and define the isomorphism (8.8.6) in each affine open X_f (f is homogeneous in S_+), and verify the compatibility when passing to a homogeneous multiple of f. Now, the restriction of the left side of (8.8.6) to X_f is $\widetilde{M}' = ((M \otimes_A S_{(f)}) \otimes_{S\otimes_A S_{(f)}} S_f^{\geqslant})^\sim$ by (8.5.2). As we have a canonical isomorphism $M \otimes_A S_{(f)} \cong M \otimes_S (S \otimes_A S_{(f)})$, we conclude that $\widetilde{M}' \cong (M \otimes_S S_f^{\geqslant})^\sim$, and this is canonically isomorphic to the restriction of $\mathscr{M}_X^{\geqslant}$ by (8.2.8). The compatibility of this isomorphism with restrictions is clear.

By replace $\mathscr{M}$ by $\widehat{\mathscr{M}}$, $\mathscr{S}$ by $\widehat{\mathscr{S}}$ and $\mathscr{S}_X$ by $(\mathscr{S}_X^{\geqslant})^\frown$ in the preceding arguments, we obtain similarly a canonical isomorphism

$$q^*(\widehat{\mathscr{M}}) \otimes_{q^*(\widehat{\mathscr{S}})} (\mathscr{S}_X^{\geqslant})^\frown \xrightarrow{\sim} (\mathscr{M}_X^{\geqslant})^\frown \tag{8.8.7}$$

If we recall Proposition 23.8.30 that the structural morphism $\psi : \mathrm{Proj}(\mathscr{S}_X^{\geqslant}) \to X$ is an isomorphism, we then deduce a canonical ψ-isomorphism

$$\mathscr{P}roj_0(\mathscr{M}) \xrightarrow{\sim} \mathscr{P}roj_0(\mathscr{M}_X^{\geqslant}) \tag{8.8.8}$$

as a particular case of (8.8.4). In fact, we observe that, in the notations of Proposition 23.8.30, that this reduces to the fact that canonical homomorphism $M_{(f)} \otimes_{S_{(f)}} (S_f^{\geqslant})^{(d)} \to (M_f^{\geqslant})^{(d)}$ is an isomorphism if $f \in S_d$ is homogeneous, which is immediate.

The isomorphism (8.8.7) permits us, by apply (8.8.5) to the canonical morphism $r = \mathrm{Proj}(\hat{\alpha}) : \widehat{C}_X \to \widehat{C}$, to obtain a canonical r-homomorphism

$$\mathscr{M}^{\square} \to (\mathscr{M}_X^{\geqslant})^{\square}. \tag{8.8.9}$$

Now recall that the restrictions of r to the blunt cones $\widehat{E}_X$ and E_X are isomorphisms onto $\widehat{E}$ and E, respectively.

Proposition 23.8.38. *The restriction of the canonical r-homomorphism (8.8.9) to $\widehat{E}_X$ and to E_X are isomorphisms*

$$\mathscr{M}^{\square}|_{\widehat{E}} \xrightarrow{\sim} (\mathscr{M}_X^{\geqslant})^{\square}|_{\widehat{E}_X}, \tag{8.8.10}$$

$$\mathscr{M}^{\square}|_{E} \xrightarrow{\sim} (\mathscr{M}_X^{\geqslant})^{\square}|_{E_X}. \tag{8.8.11}$$

Proof. We can assume that $Y = \mathrm{Spec}(A)$ is affine as in the proof of Proposition 23.8.30; with the notations there, we must show that the canonical homomorphism

$$\widehat{M}_{(f)} \otimes_{\widehat{S}_{(f)}} (S_f^{\geqslant})\widehat{\ }_{(f/1)} \to (M \otimes_S S_f^{\geqslant})\widehat{\ }_{(f/1)}$$

is an isomorphism. But in view of (8.2.5) and (8.2.7), the left side is canonically identified with $M_f^{\geqslant} \otimes_{S_f^{\geqslant}} (S_f^{\geqslant})_{f/1}^{\leqslant}$, hence with $M_f^{\geqslant}$ in view of (8.2.9); the right side is identified with $(M_f^{\geqslant})_{f/1}^{\leqslant}$, hence also to $M_f^{\geqslant}$ by (8.2.12), whence our assertion about (8.8.10). The isomorphism (8.8.11) then follows from (8.8.10) and (8.8.1). □

Corollary 23.8.39. *With the notations of Corollary 23.8.31, the restriction of $(\mathscr{M}_X^{\geqslant})^{\square}$ to $\widehat{E}_X$ is identified with $\widetilde{\mathscr{M}_X^{\leqslant}}$ and its restriction to E_X is identified with $\widetilde{\mathscr{M}_X}$.*

Proof. We can clearly reduce to the affine case, and this follows from the idnetification of $(M_f^{\geqslant})_{f/1}^{\leqslant}$ with $M_f^{\leqslant}$ and $(M_f^{\geqslant})_{f/1}$ with M_f (cf. (8.2.12)). □

Proposition 23.8.40. *Under the hypotheses of Corollary 23.8.32, the canonical homomorphism (8.8.3) is an isomorphism.*

Proof. In view of the fact that the structural morphism $\mathrm{Proj}(\mathscr{S}_X^{\geqslant}) \to X$ is an isomorphism and the isomorphisms (8.8.8) and (8.8.10), we only need to prove that the canonical homomorphism $p_X^*(\mathscr{P}roj_0(\mathscr{M}_X^{\geqslant})) \to (\mathscr{M}_X^{\geqslant})^{\square}|_{E_X}$ is an isomorphism, which means that we can assume that $\mathscr{S}_1$ is an invertible $\mathscr{O}_Y$-module and $\mathscr{S}$ is generated by $\mathscr{S}_1$. With the notations of Proposition 23.8.37, we then have, for $f \in S_1$, $S_f^{\leqslant} = S_{(f)}[1/f]$ and the canonical isomorphism $M_{(f)} \otimes_{S_{(f)}} S_f^{\leqslant} \to M_f^{\leqslant}$ is an isomorphism by the definition of $M_f^{\geqslant}$. □

We now consider the quasi-coherent $\mathscr{S}$-module $\mathscr{M}(n) = \bigoplus_{m \geq n} \mathscr{M}_m$ and the quasi-coherent graded $\mathscr{S}^\natural$-module

$$\mathscr{M}^\natural = \Big(\bigoplus_{n \geq 0} \mathscr{M}(n) \Big)^{\widetilde{}}.$$

By Proposition 23.8.33 we have a canonical C-isomorphism $h : C_X \xrightarrow{\sim} \mathrm{Proj}(\mathscr{S}^\natural)$.

Proposition 23.8.41. *There exists a canonical h-isomorphism*

$$\mathscr{P}roj_0(\mathscr{M}^\natural) \xrightarrow{\sim} \widetilde{\mathscr{M}_X}. \tag{8.8.12}$$

Proof. This can be proved as Proposition 23.8.33, by using the bi-isomorphism (8.2.13) here instead of (8.2.10). □

Chapter 24

Cohomology of coherent sheaves over schemes

24.1 Cohomology of affine schemes

24.1.1 Čech cohomology and Koszul complex

Let X be a quasi-compact and quasi-separated scheme and $\mathscr{F}$ be a quasi-coherent $\mathscr{O}_X$-module. Let $A = \Gamma(X, \mathscr{O}_X)$, $M = \Gamma(X, \mathscr{F})$, $\boldsymbol{f} = (f_i)_{1\leq i\leq r}$ be a family of elements of A, and $U_i = X_{f_i}$ be the open subset of X. Let $U = \bigcup_{i=1}^r U_i$ and $\mathfrak{U} = (U_i)$ be the covering of U. For any sequence $(i_0, i_1, \dots, i_p) \in I^{p+1}$ with $I = \{1, \dots, r\}$, we set

$$U_{i_0\dots i_p} = \bigcap_{j=0}^{p} U_{i_j} = X_{f_{i_0}\cdots f_{i_p}}.$$

By Corollary 22.6.15, we have $\Gamma(U_{i_0\dots i_p}, \mathscr{F}) = M_{f_{i_0}\cdots f_{i_p}}$, where $M = \Gamma(X, \mathscr{F})$. Note that the localization module $M_{f_{i_0}\cdots f_{i_p}}$ is identified with the limit of the inductive system $\{M^n_{i_0\dots i_p}\}_{n\geq 0}$, where $M^n_{i_0\dots i_p} = M$ and the homomorphism $\varphi_{nm} : M^m_{i_0\dots i_p} \to M^n_{i_0\dots i_p}$ is given by multiplication by $(f_{i_0}\dots f_{i_p})^{n-m}$ for $m \leq n$.

For any $n \geq 0$, let $C^{p+1}_n(M)$ be the set of alternating maps from I^{p+1} to M, and consider the inductive system formed by these A-modules and the homomorphisms induced by φ_{nm}. If $C^p(\mathfrak{U}, \mathscr{F})$ is the group of alternating Čech p-cochains relative to the covering $\mathfrak{U}$ with coefficients in $\mathscr{F}$, then we see that

$$C^p(\mathfrak{U}, \mathscr{F}) = \varinjlim_n C^{p+1}_n(M).$$

On the other hand, from the definition of $C^{p+1}_n(M)$ it is easy to see that it is canonically identified with the Koszul complex $K^{p+1}(\boldsymbol{f}^n, M)$, and the homomorphism φ_{nm} is identified with the map

$$\varphi_{\boldsymbol{f}^{n-m}} : K^\bullet(\boldsymbol{f}^n, M) \to K^\bullet(\boldsymbol{f}^m, M)$$

induced by the map $(x_1, \dots, x_r) \mapsto (f_1^{n-m}x_1, \dots, f_r^{n-m}x_r)$ on A^r. We then have, for any $p \geq 0$, a functorial isomorphism

$$C^p(\mathfrak{U}, \mathscr{F}) \xrightarrow{\sim} C^{p+1}(\mathfrak{f}, M), \tag{1.1.1}$$

where $\mathfrak{f}$ is the ideal generated by $\boldsymbol{f}$. Moreover, the definition of the differentials of $C^p(\mathfrak{U}, \mathscr{F})$ and $C_n^p(M)$ show that the isomorphism (1.1.1) is in fact a morphism of complexes.

Proposition 24.1.1. *If X is a quasi-compact and quasi-separated scheme, there exists a canonical functorial isomorphism*

$$H^p(\mathfrak{U}, \mathscr{F}) \xrightarrow{\sim} H^{p+1}(\mathfrak{f}, M) \quad \textit{for} \quad p \geq 1, \tag{1.1.2}$$

where $\mathfrak{f}$ is the ideal generated by $\boldsymbol{f}$. Moreover, we have a functorial exact sequence

$$0 \longrightarrow H^0(\mathfrak{f}, M) \longrightarrow M \longrightarrow H^0(\mathfrak{U}, \mathscr{F}) \longrightarrow H^1(\mathfrak{f}, M) \longrightarrow 0 \tag{1.1.3}$$

Proof. The relation (1.1.2) is in fact a concequence of (1.1.1). On the other hand, we have $C^0(\mathfrak{U}, \mathscr{F}) = C^1(\mathfrak{f}, M)$, so $H^0(\mathfrak{U}, \mathscr{F})$ is identified with a subgroup of 1-cocycles of $C^1(\mathfrak{f}, M)$. As $C^0(\mathfrak{f}, M) = M$, the exact sequence (1.1.3) follows from the definition of $H^0(\mathfrak{f}, M)$ and $H^1(\mathfrak{f}, M)$. □

Corollary 24.1.2. *Suppose that the X_{f_i} are quasi-compact and there exists $g_i \in \Gamma(U, \mathscr{F})$ such that $\sum_i g_i(f_i|_U) = 1|_U$. Then for any quasi-coherent $(\mathscr{O}_X|_U)$-module $\mathscr{G}$, we have $H^p(\mathfrak{U}, \mathscr{G}) = 0$ for $p > 0$. If moreover $U = X$, then the canonical homomorphism $M \to H^0(\mathfrak{U}, \mathscr{F})$ in (1.1.3) is bijective.*

Proof. By hypothesis $U_i = X_{f_i}$ is quasi-compact, so U is quasi-compact, and we can assume that $U = X$. Then the hypothesis implies that $\mathfrak{f} = A$, so by Corollary 8.5.2 we have $H^p(\mathfrak{f}, M) = 0$ for $p \geq 1$, and the corollary follows from (1.1.2) and (1.1.3). □

Remark 24.1.1. Let X be an affine scheme, so that the $U_i = X_{f_i} = D(f_i)$ are affine opens, and so is each $U_{i_0 \ldots i_p}$ (but U is not necessarily affine). In this case, the functors $\Gamma(X, \mathscr{F})$ and $\Gamma(U_{i_0 \ldots i_p}, \mathscr{F})$ are exact by Theorem 23.5.10. If we have an exact sequence $0 \to \mathscr{F}' \to \mathscr{F} \to \mathscr{F}'' \to 0$ of quasi-coherent $\mathscr{O}_X$-modules, the sequence of complexes

$$0 \longrightarrow C^\bullet(\mathfrak{U}, \mathscr{F}') \longrightarrow C^\bullet(\mathfrak{U}, \mathscr{F}) \longrightarrow C^\bullet(\mathfrak{U}, \mathscr{F}'') \longrightarrow 0$$

is exact, so we obtain a long exact sequence of coholomogy groups

$$\cdots \longrightarrow H^p(\mathfrak{U}, \mathscr{F}') \longrightarrow H^p(\mathfrak{U}, \mathscr{F}) \longrightarrow H^p(\mathfrak{U}, \mathscr{F}'') \xrightarrow{\delta} H^{p+1}(\mathfrak{U}, \mathscr{F}') \longrightarrow 0$$

On the other hand, if we put $M' = \Gamma(X, \mathscr{F}')$, $M'' = \Gamma(X, \mathscr{F}'')$, $M = \Gamma(X, \mathscr{F})$, then the sequence $0 \to M' \to M \to M' \to 0$ is exact; as $C^\bullet(\mathfrak{f}, M)$ is an exact functor on M, we then get a long exact sequence on cohomology

$$\cdots \longrightarrow H^p(\mathfrak{f}, M') \longrightarrow H^p(\mathfrak{f}, M) \longrightarrow H^p(\mathfrak{f}, M'') \xrightarrow{\delta} H^{p+1}(\mathfrak{f}, M') \longrightarrow 0$$

Now as the diagram

$$\begin{tikzcd}
0 \arrow[r] & C^\bullet(\mathfrak{U}, \mathscr{F}') \arrow[r] \arrow[d] & C^\bullet(\mathfrak{U}, \mathscr{F}) \arrow[r] \arrow[d] & C^\bullet(\mathfrak{U}, \mathscr{F}'') \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & C^\bullet(\mathfrak{f}, M') \arrow[r] & C^\bullet(\mathfrak{f}, M) \arrow[r] & C^\bullet(\mathfrak{f}, M'') \arrow[r] & 0
\end{tikzcd}$$

is commutative, we conclude that the diagram

$$\begin{tikzcd} H^p(\mathfrak{U}, \mathscr{F}'') \arrow[r, "\delta"] \arrow[d] & H^{p+1}(\mathfrak{U}, \mathscr{F}') \arrow[d] \\ H^{p+1}(\mathfrak{f}, M'') \arrow[r, "\delta"] & H^{p+2}(\mathfrak{f}, M') \end{tikzcd} \tag{1.1.4}$$

is commutative for any $p > 0$.

24.1.2 Cohomology of affine schemes

Theorem 24.1.3. *Let X be an affine scheme. For any quasi-coherent $\mathscr{O}_X$-module $\mathscr{F}$, we have $H^p(X, \mathscr{F}) = 0$ for $p > 0$.*

Proof. Let $\mathfrak{U}$ be a finite covering of X by affine opens $X_{f_i} = D(f_i)$ $(1 \leq i \leq r)$; then the ideal generated by f_i is equal to $A = \Gamma(X, \mathscr{O}_X)$. We then conclude from Corollary 24.1.2 that we have $H^p(\mathfrak{U}, \mathscr{F}) = 0$ for any $p > 0$. As affine opens for a basis for X, we then conclude from the definition of the Čech cohomology that $\check{H}^p(X, \mathscr{F}) = 0$ for any $p > 0$. But this is also applicable on X_f for $f \in A$, so $\check{H}^p(X_f, \mathscr{F}) = 0$ for $p > 0$; as $X_f \cap X_g = X_{fg}$, we then conclude from Leray's vanishing theorem that $H^p(X, \mathscr{F}) = 0$ for $p > 0$. □

Corollary 24.1.4. *Let $f : X \to Y$ be an affine morphism. Then for any quasi-coherent $\mathscr{O}_X$-module $\mathscr{F}$, we have $R^p f_*(\mathscr{F}) = 0$ for $p > 0$.*

Proof. By definition $R^p f_*(\mathscr{F})$ is defined to be the sheaf associated with the presheaf $U \mapsto H^p(f^{-1}(U), \mathscr{F})$, where U runs through open subsets of Y. Now the affine opens U form a basis for Y, and for such U, $f^{-1}(U)$ is affine, so $H^p(f^{-1}(U), \mathscr{F}) = 0$ by Theorem 24.1.3, so we conclude that $R^p f_*(\mathscr{F}) = 0$. □

Corollary 24.1.5. *Let $f : X \to Y$ be an affine morphism. Then for any quasi-coherent $\mathscr{O}_X$-module $\mathscr{F}$, the canonical homomorphism $H^p(Y, f_*(\mathscr{F})) \to H^p(X, \mathscr{F})$ is bijective for any p.*

Proof. It suffices to prove that the edge-homomorphisms

$$E_2^{p,0} = H^p(Y, f_*(\mathscr{F})) \to H^p(X, \mathscr{F})$$

of the Leray spectral sequence is bijective. But the E_2 page of this sequence is given by

$$E_2^{p,q} = (R^p\Gamma \circ R^q f_*)(\mathscr{F}) = H^p(Y, R^q f_*(\mathscr{F})),$$

so it follows from Corollary 24.1.4 that $E_2^{p,q} = 0$ for $q > 0$, and this sequence collapses at E_2 page, whence our assertion. □

Corollary 24.1.6. *Let $f : X \to Y$ be an affine morphism, $g : Y \to Z$ be a morphism. Then for any quasi-coherent $\mathscr{O}_X$-module $\mathscr{F}$, the canonical homomorphism $R^p g_*(f_*(\mathscr{F})) \to F^p(g \circ f)_*(\mathscr{F})$ is bijective for any p.*

Proof. It suffices to remark that, by Corollary 24.1.5, for any affine open W of Z, the canonical homomorphism $H^p(g^{-1}(W), f_*(\mathscr{F})) \to H^p(f^{-1}(g^{-1}(W)), \mathscr{F})$ is bijective; this homomorphism of presheaves then defines a canonical homomorphism $R^p g_*(f_*(\mathscr{F})) \to R^p(g \circ f)_*(\mathscr{F})$ which is bijective. □

24.1.3 Application to cohomology of schemes

Proposition 24.1.7. *Let X be a separated scheme, $\mathfrak{U} = (U_\alpha)$ be a covering of X by affine opens. For any quasi-coherent $\mathscr{O}_X$-module $\mathscr{F}$, the cohomology module $H^\bullet(X, \mathscr{F})$ and $H^\bullet(\mathfrak{U}, \mathscr{F})$ (over $\Gamma(X, \mathscr{O}_X)$) are canonically isomorphic.*

Proof. In fact, as X is separated, any finite intersection V of open sets in the covering $\mathfrak{U}$ is affine (Proposition 22.5.30), so $H^p(V, \mathscr{F}) = 0$ for $q > 0$ in view of Theorem 24.1.3. The proposition then follows from Leray's vanishing theorem. □

Remark 24.1.2. We note that the conclusion of Proposition 24.1.7 is still valid if the finite intersections of U_α are affine, even if X is not necessarily separated.

Corollary 24.1.8. *Let X be a quasi-compact and separated scheme, $A = \Gamma(X, \mathscr{O}_X)$, $\boldsymbol{f} = (f_i)_{1\leq i\leq r}$ be a sequence of elements of A such that the X_{f_i} are affine. Then for any quasi-coherent $\mathscr{O}_X$-module $\mathscr{F}$, we have a canonical functorial isomorphism*

$$H^p(U, \mathscr{F}) \xrightarrow{\sim} H^{p+1}(\mathfrak{f}, M) \quad \textit{for} \quad p > 0 \tag{1.3.1}$$

where $\mathfrak{f}$ is the ideal generated by $\boldsymbol{f}$. Moreover, we have a functorial exact sequence

$$0 \longrightarrow H^0(\mathfrak{f}, M) \longrightarrow M \longrightarrow H^0(U, \mathscr{F}) \longrightarrow H^1(\mathfrak{f}, M) \longrightarrow 0 \tag{1.3.2}$$

If X is an affine scheme, it then follows from Remark 24.1.1 and Proposition 24.1.7 that for any $q \geq 0$, the diagram

$$\begin{tikzcd} H^p(U, \mathscr{F}'') \arrow[r, "\delta"] \arrow[d] & H^{p+1}(U, \mathscr{F}') \arrow[d] \\ H^{p+1}(\mathfrak{f}, M'') \arrow[r, "\delta"] & H^{p+2}(\mathfrak{f}, M') \end{tikzcd} \tag{1.3.3}$$

corresponding to an exact sequence $0 \to \mathscr{F}' \to \mathscr{F} \to \mathscr{F}'' \to 0$ of quasi-coherent $\mathscr{O}_X$-modules, is commutative.

Proposition 24.1.9. *Let X be a quasi-compact and separated X scheme, $\mathscr{L}$ be an invertible $\mathscr{O}_X$-module, and consider the graded ring $A_* = \Gamma_*(\mathscr{L})$. Then $H^\bullet(\mathscr{F}, \mathscr{L}) = \bigoplus_{n\in\mathbb{Z}} H^\bullet(X, \mathscr{F} \otimes \mathscr{L}^{\otimes n})$ is a graded A_*-module, and for any $f \in (A_*)_n$, we have a canonical isomorphism*

$$H^\bullet(X_f, \mathscr{F}) \xrightarrow{\sim} (H^\bullet(\mathscr{F}, \mathscr{L}))_{(f)} \tag{1.3.4}$$

of $(A_*)_{(f)}$-modules.

Proof. As X is quasi-compact and separated, we can compute the cohomology of $\mathscr{O}_X$-module $\mathscr{F} \otimes \mathscr{L}^{\otimes n}$ using the same finite covering $\mathfrak{U} = (U_i)$ by open affine subsets such that $\mathscr{L}|_{U_i}$ is isomorphic to $\mathscr{O}_X|_{U_i}$ for each i (Proposition 24.1.7). Also, since each $U_i \cap X_f$ is open and affine, we can also compute $H^\bullet(X_f, \mathscr{F}\otimes\mathscr{L}^{\otimes n})$ using the covering $\mathfrak{U}|_{X_f} = (U_i \cap X_f)$. Now for any $f \in A_n$, it is immediate that the multiplication by f defines a homomorphism $C^\bullet(\mathfrak{U}, \mathscr{F} \otimes \mathscr{L}^{\otimes m}) \to C^\bullet(\mathfrak{U}, \mathscr{F} \otimes \mathscr{L}^{\otimes(m+n)})$, whence a homomorphism $H^\bullet(\mathfrak{U}, \mathscr{F} \otimes \mathscr{L}^{\otimes m}) \to H^\bullet(\mathfrak{U}, \mathscr{F} \otimes \mathscr{L}^{\otimes(m+n)})$. On the other hand, by Corollary 22.6.16 and Corollary 22.1.6 (ii), any $f \in A_n$ gives an isomorphism of $(A_*)_{(f)}$-modules

$$C^\bullet(\mathfrak{U}|_{X_f}, \mathscr{F}) \xrightarrow{\sim} (C^\bullet(\mathfrak{U}, \bigoplus_{n\in\mathbb{Z}} \mathscr{F} \otimes \mathscr{L}^{\otimes n}))_{(f)}.$$

By passing to cohomologies, we then deduce the desired isomorphism (1.3.4), using the fact that $M \mapsto M_{(f)}$ is an exact functor on the category of graded modules. □

Corollary 24.1.10. *If $A = \Gamma(X, \mathcal{O}_X)$, then for any $f \in A$ we have a canonical isomorphism $H^\bullet(X_f, \mathcal{F}) \xrightarrow{\sim} (H^\bullet(X, \mathcal{F}))_f$ of A_f-module.*

Corollary 24.1.11. *Let X be a quasi-compact and separated scheme and $f \in \Gamma(X, \mathcal{O}_X)$.*

(a) If X_f is affine, then for any quasi-coherent $\mathcal{O}_X$-module $\mathcal{F}$ and any $\xi \in H^i(X, \mathcal{F})$ with $i > 0$, there exists an integer $n > 0$ such that $f^n \xi = 0$.

(b) Conversely, suppose that X_f is quasi-compact and for any quasi-coherent ideal $\mathcal{I}$ and any $\zeta \in H^1(X, \mathcal{I})$, there exists $n > 0$ such that $f^n \zeta = 0$. Then X_f is affine.

Proof. First, if X_f is affine then $H^i(X_f, \mathcal{F}) = 0$ for $i > 0$, so (a) follows from the isomorphism of Corollary 24.1.10. Conversely, in case (b), in view of Serre's criterion, it suffices to prove that for any quasi-coherent ideal $\mathcal{K}$ of $\mathcal{O}_X|_{X_f}$, we have $H^1(X_f, \mathcal{K}) = 0$. Now as X_f is a quasi-compact open subset of the quasi-compact scheme X, by Theorem 22.6.60 there exists a quasi-coherent ideal $\mathcal{I}$ of $\mathcal{O}_X$ such that $\mathcal{K} = \mathcal{I}|_{X_f}$. By Corollary 24.1.10 we have $H^1(X_f, \mathcal{K}) = (H^1(X, \mathcal{I}))_f$, and the hypothesis then implies our claim. □

Lemma 24.1.12 (Induction principle). *Let X be a quasi-compact and quasi-separated scheme and $\mathcal{P}$ be a property for quasi-compact open subsets of X. Assume that the following conditions are satisfied:*

(a) $\mathcal{P}$ holds for affine opens of X,

(b) if U is a quasi-compact open subset of X, V is an affine open of X, and $\mathcal{P}$ holds for U, V, $U \cap V$, then $\mathcal{P}$ holds for $U \cup V$.

Then $\mathcal{P}$ holds for every quasi-compact open subset of X, and in particular holds for X.

Proof. We first prove that $\mathcal{P}$ holds for separated quasi-compact open subset $W \subseteq X$. For this, note that W can be written as a union $W = U_1 \cup \cdots \cup U_n$ of affine opens and we can applying induction on n with $U = U_1 \cup \cdots \cup U_n$ and $V = U_n$. This is allowed because $U \cap V = (U_1 \cap U_n) \cup \cdots \cup (U_{n-1} \cap U_n)$ is again a union of $n-1$ affine open subschemes. Now for any quasi-compact open subset $W \subseteq X$, we can induct on the number of affine opens needed to cover W using the same trick as before and using that the quasi-compact open $U_i \cap U_n$ is separated as an open subscheme of the affine scheme U_n. □

Proposition 24.1.13. *Let $f : X \to Y$ be a quasi-compact and quasi-separated morphism. Then for any quasi-coherent $\mathcal{O}_X$-module $\mathcal{F}$, $R^p f_*(\mathcal{F})$ is quasi-coherent for $p \geq 0$.*

Proof. Since taking restriction commutes with higher direct images, we may assume that Y is affine. Then X is quasi-compact and quasi-separated. For a quasi-compact open subset $U \subseteq X$ and $f_U = f|_U$, we let $\mathcal{P}(U)$ be the property that $R^p(f_U)_*(\mathcal{F})$ is quasi-coherent for all quasi-coherent modules $\mathcal{F}$ on U and $o \geq 0$. It then suffices to prove that the conditions of Lemma 24.1.12 hold. If U is affine, then the morphism f_U is affine, so by Corollary 23.5.11 we have $R^p(f_U)_*(\mathcal{F}) = 0$ for $p > 0$, and $f_*(\mathcal{F})$ is quasi-coherent by Proposition 22.6.54. Now let $U \subseteq X$ be a quasi-compact open subset, $V \subseteq X$ be an affine open subset, and assume that

property $\mathcal{P}$ holds for U, V and $U \cap V$. Then for any quasi-coherent $\mathcal{O}_X|_{U\cup V}$-module $\mathcal{F}$, we have the relative Mayer-Vietoris sequence

$$0 \to (f_{U\cup V})_*(\mathcal{F}) \to (f_U)_*(\mathcal{F}|_U) \oplus (f_V)_*(\mathcal{F}|_V) \to (f_{U\cap V})_*(\mathcal{F}|_{U\cap V}) \to R^1(f_{U\cup V})_*(\mathcal{F}) \to \cdots$$

It then follows from our assumption and Corollary 22.1.6 that $R^p(f_{U\cup V})_*(\mathcal{F})$ is quasi-coherent for $p \geq 0$, so the assertion follows by applying Lemma 24.1.12. □

Proposition 24.1.14. *Let $f : X \to Y$ be a quasi-compact and separated morphism. Then for any quasi-coherent $\mathcal{O}_X$-module $\mathcal{F}$ and any affine open $V \subseteq Y$, the canonical homomorphism $H^p(f^{-1}(V), \mathcal{F}) \to \Gamma(V, R^p f_*(\mathcal{F}))$ is an isomorphism for $p \geq 0$.*

Corollary 24.1.15. *Under the hypothesis of Proposition 24.1.13, suppose that Y is quasi-compact. Then there exists an integer $n > 0$ such that for any quasi-coherent $\mathcal{O}_X$-module, we have $R^p f_*(\mathcal{F}) = 0$ for $p > n$. If Y is affine, then we can choose n so that there exists a covering of X by n affine opens.*

Proof. Since Y is a union of affine opens, it suffices to prove the second assertion, in view of Proposition 24.1.14. Now if $\mathfrak{U}$ is a covering of X by n affine opens, then $H^p(\mathfrak{U}, \mathcal{F}) = 0$ for $p > n$, since the cochains can be taken to be alternating. The conclusion then follows from Proposition 24.1.7. □

Corollary 24.1.16. *Under the hypothesis of Proposition 24.1.13, suppose that $Y = \mathrm{Spec}(A)$ is affine. Then for any quasi-coherent $\mathcal{O}_X$-module $\mathcal{F}$ and any $f \in A$, we have*

$$\Gamma(Y_f, R^p f_*(\mathcal{F})) = (\Gamma(Y, R^p f_*(\mathcal{F})))_f$$

Proof. This follows from Proposition 24.1.13 and Corollary 22.6.15. □

Proposition 24.1.17. *Let $f : X \to Y$ be a quasi-compact and separated morphism, $g : Y \to Z$ be an affine morphism. For any quasi-coherent $\mathcal{O}_X$-module $\mathcal{F}$, the canonical homomorphism $R^p(g \circ f)_*(\mathcal{F}) \to g_*(R^p f_*(\mathcal{F}))$ is bijective for $p \geq 0$.*

Proof. For any affine open $W \subseteq Z$, $g^{-1}(W)$ is an affine open of Y, so the conclusion follows from Proposition 24.1.14. □

Proposition 24.1.18. *Let $f : X \to Y$ be a separated morphism of finite type and $g : Y' \to Y$ be a flat morphism. Let $f' = f_{(Y')} : X' = X_{(Y')} \to Y'$, and consider the commutative diagram*

$$\begin{tikzcd} X' \arrow[r, "g'"] \arrow[d, "f'"'] & X \arrow[d, "f"] \\ Y' \arrow[r, "g"] & Y \end{tikzcd}$$

Then for any quasi-coherent $\mathcal{O}_X$-module $\mathcal{F}$, $R^p f'_*(\mathcal{F}')$ is canonically isomorphic to $R^p f_*(\mathcal{F}) \otimes_{\mathcal{O}_Y} \mathcal{O}_{Y'} = g^*(R^p f_*(\mathcal{F}))$ for $p \geq 0$ (where $\mathcal{F}' = g'^*(\mathcal{F}) = \mathcal{F} \otimes_{\mathcal{O}_Y} \mathcal{O}_{Y'}$).

Proof. The canonical homomorphism $\rho : \mathcal{F} \to g'_*(g'^*(\mathcal{F}))$ defines a homomorphism

$$R^p f_*(\mathcal{F}) \to R^p f_*(g'_*(g'^*(\mathcal{F}))). \tag{1.3.5}$$

On the other hand, we also have the canonical homomorphisms

$$R^p f_*(g'_*(\mathscr{F}')) \to R^p h_*(\mathscr{F}') \to g_*(R^p f'_*(\mathscr{F}')), \tag{1.3.6}$$

where $h = f \circ g' = g \circ f'$. Composing (1.3.5) with (1.3.6), we get a homomorphism

$$\psi : R^p f_*(\mathscr{F}) \to g_*(R^p f'_*(\mathscr{F}))$$

and finaly a induced canonical homomorphism (without using the hypothesis on g)

$$\psi^\sharp : g^*(R^p f_*(\mathscr{F})) \to R^p f'_*(\mathscr{F}'). \tag{1.3.7}$$

We need to prove that $\psi^\sharp$ is an isomorphism if g is flat. It is clear that the question is local over Y and Y', so we may assume that $Y = \operatorname{Spec}(A)$, $Y' = \operatorname{Spec}(B)$, and g corresponds to a ring homomorphism $\varphi : A \to B$. Then it follows from Proposition 24.1.14 and the definition of the homomorphism (1.3.6) that ψ corresponds to the composition homomorphism

$$H^p(X, \mathscr{F}) \xrightarrow{\rho_p} H^p(X, g'_*(g'^*(\mathscr{F}))) \xrightarrow{\theta_p} H^p(X', g'_*(g'^*(g'^*(\mathscr{F})))) \xrightarrow{\sigma_p} H^p(X', g'^*(\mathscr{F}))$$

where ρ_p and σ_p correspond to the canonical homomorphism ρ and σ, and θ_p is the φ-morphism of (**??**) relative to the $\mathscr{O}_X$-module $g'_*(g'^*(\mathscr{F}))$. By the functoriality of θ_p, we have a commutative diagram

$$\begin{tikzcd}
H^p(X, \mathscr{F}) \arrow[r, "\rho_p"] \arrow[d] & H^p(X, g'_*(g'^*(\mathscr{F}))) \arrow[d] \\
H^p(X', v'^*(\mathscr{F})) \arrow[r, "g'^*(\rho_p)"] & H^p(X', g'_*(g'^*(g'^*(\mathscr{F}))))
\end{tikzcd}$$

and as by definition $g'^*(\rho)$ is the inverse of σ, we see that the composition homomorphism considered above is none other than θ_p. The homomorphism $\psi^\sharp$ is therefore the B-homomorphism $H^p(X, \mathscr{F}) \otimes_A B \to H^p(X', \mathscr{F}')$. As f is of finite type, X can be covered by finitely many affine opens $\mathfrak{U} = (U_i)$. Since g is an affine morphism, so is g' (Proposition 23.1.31), and the $U'_i = g'^{-1}(U_i)$ therefore form an open affine covering $\mathfrak{U}'$ of X'. We then conclude from (**??**) that the diagram

$$\begin{tikzcd}
H^p(\mathfrak{U}, \mathscr{F}) \arrow[r, "\theta_p"] \arrow[d] & H^p(\mathfrak{U}', \mathscr{F}') \arrow[d] \\
H^p(X, \mathscr{F}) \arrow[r, "\theta_p"] & H^p(X', \mathscr{F}')
\end{tikzcd}$$

is commutative, and the the columns are isomorphisms since X and X' are separated (Proposition 24.1.7). It then suffices to prove that the φ-morphism $\theta_p : H^p(\mathfrak{U}, \mathscr{F}) \to H^p(\mathfrak{U}', \mathscr{F}')$ is such that the associated B-homomorphism

$$H^p(\mathfrak{U}, \mathscr{F}) \otimes_A B \to H^p(\mathfrak{U}', \mathscr{F}')$$

is an isomorphism. Now in view of Proposition 22.1.13, we see the canonical map $C^p(\mathfrak{U}, \mathscr{F}) \otimes_A B \to C^p(\mathfrak{U}', \mathscr{F}')$ is bijective. As B is a flat A-module, it follows that the canonical map $H^p(\mathfrak{U}, \mathscr{F}) \otimes_A B \to H^p(\mathfrak{U}', \mathscr{F}')$ is an isomorphism. □

Corollary 24.1.19. *Let A be a ring, X be an A-scheme of finite type, and B be a faithfully flat A-algebra.*

Then for X to be affine, it is necesary and sufficient that $X \otimes_A B$ is affine.

Proof. The condition is clearly necessary. Conversely, as X is separated over A and the morphism $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is flat, it follows from Proposition 24.1.7 that we have

$$H^i(X \otimes_A B, \mathscr{F} \otimes_A B) = H^i(X, \mathscr{F}) \otimes_A B$$

for $i \geq 0$ and any quasi-coherent $\mathscr{O}_X$-module $\mathscr{F}$. As $X \otimes_A B$ is affine, we see that $H^i(X \otimes_A B, \mathscr{F} \otimes_A B) = 0$ for $i > 0$, so $H^i(X, \mathscr{F}) = 0$ for $i > 0$ since B is faithfully flat over A. As X is quasi-compact, the conclusion then follows from Serre's criterion. □

24.2 Coholomogical study of projective morphisms

24.2.1 Cohomology associated with an invertible sheaf

Let X be a scheme, $\mathscr{L}$ be an invertible $\mathscr{O}_X$-module, and consider the graded ring

$$S = \Gamma_*(X, \mathscr{L}) = \bigoplus_{n \in \mathbb{Z}} \Gamma(X, \mathscr{L}^{\otimes n}).$$

Let $\boldsymbol{f} = (f_i)_{1 \leq i \leq r}$ be a family of homogeneous elements of S, where $f_i \in S_{d_i}$. Put $U_i = X_{f_i}$, $U = \bigcup_i U_i$, and let $\mathfrak{U} = (U_i)$ be the covering of U. For any quasi-coherent $\mathscr{O}_X$-module $\mathscr{F}$ of X, we set

$$H^\bullet(\mathfrak{U}, \mathscr{F}(*)) := \bigoplus_{n \in \mathbb{Z}} H^\bullet(\mathfrak{U}, \mathscr{F} \otimes \mathscr{L}^{\otimes n}), \quad H^\bullet(U, \mathscr{F}(*)) := \bigoplus_{n \in \mathbb{Z}} H^\bullet(U, \mathscr{F} \otimes \mathscr{L}^{\otimes n}). \tag{2.1.1}$$

We note that the abelian groups in (2.1.1) are bigraded: for $m, n \in \mathbb{Z}$ we set

$$(H^\bullet(\mathfrak{U}, \mathscr{F}(*)))_{mn} = H^m(\mathfrak{U}, \mathscr{F} \otimes \mathscr{L}^n), \quad (H^\bullet(U, \mathscr{F}(*)))_{mn} = H^m(U, \mathscr{F} \otimes \mathscr{L}^n).$$

For any fixed $m \in \mathbb{Z}$, it is clear that $H^m(\mathfrak{U}, \mathscr{F}(*))$ and $H^m(U, \mathscr{F}(*))$ are graded S-modules. We now consider the graded S-module

$$M = \Gamma_*(\mathscr{L}, \mathscr{F}) = H^0(X, \mathscr{F}(*)) = \bigoplus_{n \in \mathbb{Z}} \Gamma(X, \mathscr{F} \otimes \mathscr{L}^{\otimes n}).$$

If X is quasi-compact and quasi-separated, then it follows from Theorem 22.6.14 that for any sequence $(i_0, i_1, \ldots, i_p)$, we have a canonical isomorphism

$$\Gamma(U_{i_0 \ldots i_p}, \mathscr{F}(*)) = H^0(U_{i_0 \ldots i_p}, \mathscr{F}(*)) = M_{f_{i_0} \cdots f_{i_p}}.$$

Recall that $M_{f_{i_0} \cdots f_{i_p}}$ is idnetified with $\varinjlim_n M^n_{i_0 \ldots i_p}$, and this identification is an isomorphism of graded S-modules, if we define the degree of an element $z \in \varinjlim_n M^n_{i_0 \ldots i_p}$ to be the number $m - n(d_{i_0} + \cdots + d_{i_p})$ if z is the image of a homogeneous element $x \in M^n_{i_0 \ldots i_p} = M$ of degree m (from the definition of the transition homomorphisms $\varphi_{kj} : M^{(j)}_{i_0 \ldots i_p} \to M^{(k)}_{i_0 \ldots i_p}$, it follows that this definition does not depend on the choice of x). Let $C^p_n(M)$ be the set of alternating maps $I^{p+1} \to M$ (for any n), then we can similarly define a graded S-module structure on

$\varinjlim_n C_n^p(M)$. Now the canonical isomorphism

$$C^p(\mathfrak{U}, \mathscr{F}(*)) = \varinjlim_n C_n^p(M)$$

is then an isomorphism of graded S-modules. By Proposition 24.1.1, we have isomorphism of graded S-modules

$$C^p(\mathfrak{U}, \mathscr{F}(*)) = C^{p+1}(\mathfrak{f}, M) = \varinjlim_n K^{p+1}(\boldsymbol{f}^n, M)$$

where the degree of an element in $\varinjlim K^{p+1}(\boldsymbol{f}^n, M)$ is defined similarly. It is easy to see that the isomorphisms above are compatible with differential maps, so from Proposition 24.1.1 we conclude the following:

Proposition 24.2.1. *Let X be a quasi-compact and quasi-separated scheme. Then there exists a canonical isomorphism of graded S-modules*

$$H^p(\mathfrak{U}, \mathscr{F}(*)) \xrightarrow{\sim} H^{p+1}(\mathfrak{f}, M) \quad \textit{for} \quad p \geq 1, \tag{2.1.2}$$

where $\mathfrak{f}$ is the ideal generated by $\boldsymbol{f}$. Moreover, we have a functorial exact sequence

$$0 \longrightarrow H^0(\mathfrak{f}, M) \longrightarrow M \longrightarrow H^0(\mathfrak{U}, \mathscr{F}(*)) \longrightarrow H^1(\mathfrak{f}, M) \longrightarrow 0 \tag{2.1.3}$$

of homomorphisms of degree 0.

Corollary 24.2.2. *If X is quasi-compact and separated and $U_i = X_{f_i}$ are affine, then there exists a canonical isomorphism of degree* 0*:*

$$H^p(U, \mathscr{F}(*)) \xrightarrow{\sim} H^{p+1}(\mathfrak{f}, M) \quad \textit{for} \quad p > 0.$$

and we have a functorial exact sequence

$$0 \longrightarrow H^0(\mathfrak{f}, M) \longrightarrow M \longrightarrow H^0(\mathfrak{U}, \mathscr{F}(*)) \longrightarrow H^1(\mathfrak{f}, M) \longrightarrow 0$$

of homomorphisms of degree 0.

Corollary 24.2.3. *Let S be a graded ring with positive degrees, $(f_i)_{1\leq i\leq r}$ be homogeneous elements of S_+ with $f_i \in S_{d_i}$, and M be a graded S-module. Let $X = \mathrm{Proj}(S)$, $U_i = D_+(f_i)$, and $\mathscr{L} = \mathscr{O}_X(1)$, then there exists a canonical isomorphism of degree* 0*:*

$$H^p(U, \widetilde{M}(*)) \xrightarrow{\sim} H^{p+1}(\mathfrak{f}, M) \quad \textit{for} \quad p > 0.$$

and we have a functorial exact sequence

$$0 \longrightarrow H^0(\mathfrak{f}, M) \longrightarrow M \longrightarrow H^0(\mathfrak{U}, \widetilde{M}(*)) \longrightarrow H^1(\mathfrak{f}, M) \longrightarrow 0$$

of homomorphisms of degree 0.

Proof. In fact, we have $\Gamma(U_{i_0\ldots i_p}, \widetilde{M(n)}) = (M_{f_{i_0}\cdots f_{i_p}})_n$, so $\Gamma(U_{i_0\ldots i_p}, \widetilde{M}(*)) = M_{f_{i_0}\cdots f_{i_p}}$. The conclusion then follows from Corollary 24.2.2 since X is quasi-compact and separated. □

Remark 24.2.1. Corollary 24.2.3 is intersting if S is an A-algebra generated by S_1 where A is Noetherian. In fact, in this case any quasi-coherent $\mathscr{O}_X$-module $\mathscr{F}$ is of the form $\widetilde{M}$ by Theorem 23.2.39.

Remark 24.2.2. Under the hypothesis of Corollary 24.2.3, the functor $\Gamma(U_{i_0\dots i_p}, \widetilde{M}(*)) = M_{f_{i_0}\cdots f_{i_p}}$ is exact on M, and as in Remark 24.1.1, if $0 \to M' \to M \to M'' \to 0$ is an exact sequence of graded S-modules, we have a commutative diagram for $p \geq 0$:

$$\begin{tikzcd} H^p(U, \widetilde{M}''(*)) \arrow[r, "\partial"] \arrow[d] & H^{p+1}(U, \widetilde{M}') \arrow[d] \\ H^{p+1}(\mathfrak{f}, M'') \arrow[r, "\partial"] & H^{p+2}(\mathfrak{f}, M') \end{tikzcd}$$

We now apply Corollary 24.2.3 to $S = A[T_0, \dots, T_r]$, where A is a ring and T_i are indeterminantes. Let $M = S$ and $f_i = T_i$, we are then reduced to compute $H^\bullet(\mathfrak{m}, S)$, where $\boldsymbol{T} = (T_i)_{0\leq i\leq r}$ and $\mathfrak{m}$ is the maximal ideal of S generated by $T_0, \dots, T_r$.

Lemma 24.2.4. *If $S = A[T_0, \dots, T_r]$ and $\boldsymbol{T} = (T_i)_{0\leq i\leq r}$, then*

$$H^i(\boldsymbol{T}^n, S) = \begin{cases} 0 & i \neq r+1, \\ S/\mathfrak{m}^n & i = r+1. \end{cases} \tag{2.1.4}$$

Proof. This is an immediate from the fact that the sequence $\boldsymbol{T}$ is regular. □

By passing to inductive limits over n, we see that $H^i(\mathfrak{m}, S) = 0$ for $i \neq r+1$. If $i = r+1$, then the inductive system is formed by $S/\mathfrak{m}^n$ and $\varphi_{nm} : S/\mathfrak{m}^n \to S/\mathfrak{m}^m$ for $0 \leq n \leq m$ is the multiplication by $(T_0 \cdots T_r)^{n-m}$. For any sequence $\alpha = (\alpha_0, \dots, \alpha_r)$ and integer $n \geq \sup_i\{\alpha_i\}$, we define

$$\xi_\alpha^n = T_0^{n-\alpha_0} \cdots T_r^{n-\alpha_r} \mod \mathfrak{m}^n.$$

Then $\varphi_{nm}(\xi_\alpha^n) = \xi_\alpha^m$, so the ξ_I^n form an element ξ_I in the inductive limit $H^{r+1}(\mathfrak{m}, S)$.

Corollary 24.2.5. *With the notations of Lemma 24.2.4, we have $H^i(\mathfrak{m}, S) = 0$ for $i \neq r+1$, and $H^{r+1}(\mathfrak{m}, S)$ is a free A-module with basis formed by the elements ξ_α with $\alpha_i > 0$ for each i.*

Proof. In fact, for each $n \geq 0$, the elements ξ_α^n for $0 < \alpha_i \leq n$ form a basis of the A-module $S/\mathfrak{m}^n$, so the corollary follows from (2.1.4). □

Proposition 24.2.6. *Let A be a ring, $r > 0$ be an integer, and $X = \mathbb{P}^r_A$.*

(a) We have $H^i(X, \mathscr{O}_X(*)) = 0$ for $i \neq 0, r$.

(b) The canonical homomorphism $\alpha : S \to H^0(X, \mathscr{O}_X(*))$ is an isomorphism.

(c) The A-module $H^r(X, \mathscr{O}_X(*))$ is free with basis formed by the elements ξ_α with $\alpha_i > 0$ for each i. Moreover, ξ_α is of degree $-|\alpha| = -(\alpha_0 + \cdots + \alpha_r)$, and $T_i \cdot \xi_\alpha = \xi_{\alpha_0,\dots,\alpha_i-1,\dots,\alpha_r}$.

Proof. By Corollary 24.2.5 we have $H^i(\mathfrak{m}, S) = 0$ for $i \neq r+1$, so the assertion in (a) follows from (2.1.2). From the exact sequence (2.1.3), it is easy to see that $S \cong H^0(X, \mathscr{O}_X(*))$, and the isomorphism is given by the canonical homomorphism α. The last assertion also follows from (2.1.2) and Corollary 24.2.5. □

Corollary 24.2.7. *The values (i, n) such that $H^i(X, \mathcal{O}_X(n)) \neq 0$ are the following: $i = 0$ and $n \geq 0$, or $i = r$ and $n \leq -(r+1)$.*

Proof. We note that if $A \neq 0$ then $H^i(X, \mathcal{O}_X(n)) \neq 0$ by the listed values of (i, n). □

Corollary 24.2.8. *The A-modules $H^i(X, \mathcal{O}_X(n))$ are free of finite rank. If $i > 0$, then they are zero for $n > 0$.*

Proposition 24.2.9. *Let Y be a scheme, $\mathscr{E}$ be a locally free $\mathcal{O}_Y$-module of rank $r+1$, and $X = \mathbb{P}(\mathscr{E})$ be the projective bundle defined by $\mathscr{E}$. Let $f : X \to Y$ be the structural morphism, then the values (n, i) such that $R^i f_*(\mathcal{O}_X(n)) \neq 0$ are the following: $i = 0$ and $n \geq 0$, or $i = r$ and $n \leq -(r+1)$. Moreover, the canonical homomorphism*

$$\alpha : \boldsymbol{S}_{\mathcal{O}_Y}(\mathscr{E}) \to \Gamma_*(\mathcal{O}_X) = R^0 f_*(\mathcal{O}_X(*)) = \bigoplus_{n \in \mathbb{Z}} f_*(\mathcal{O}_X(n))$$

is an isomorphism.

Proof. This question is local over Y, so we can assume that $Y = \operatorname{Spec}(A)$ is affine and $\mathscr{E} = \widetilde{E}$, where $E = A^{r+1}$. We can then apply Proposition 24.2.6, in view of Proposition 24.1.14. □

24.2.2 The coherence theorem for projective morphisms

Proposition 24.2.10. *Let A be a Noetherian ring and S be a graded A-algebra with positive degrees that is generated by $r+1$ elements of S_1. Let $X = \operatorname{Proj}(S)$, and consider a coherent $\mathcal{O}_X$-module $\mathscr{F}$.*

(a) The A-module $H^p(X, \mathscr{F})$ is finitely generated.

(b) We have $H^p(X, \mathscr{F}) = 0$ for $p > r$.

(c) There exists an integer n_0 such that for $n \geq n_0$, we have $H^p(X, \mathscr{F}(n))$ for $p > 0$.

(d) There exists an integer n_0 such that for $n \geq n_0$, $\mathscr{F}(n)$ is generated by global sections.

Proof. Note that X can be identified with a closed subscheme of $P = \mathbb{P}^r_A$ (Proposition 23.2.50). Moreover, if $j : X \to P$ is the canonical injection, $j_*(\mathscr{F})$ is a coherent $\mathcal{O}_P$-module and we have $j_*(\mathscr{F}(n)) = (j_*(\mathscr{F}))(n)$ (Corollary 23.3.24 and Proposition 23.3.27). In view of **??**, we only need to consider the case where $X = \mathbb{P}^r_A$ and $S = A[T_0, \ldots, T_r]$. Now X can be covered by $r+1$ affine opens $D_+(T_i)$, so (b) follows from Proposition 24.1.14 and Corollary 24.1.15. We also note that (d) is proved in Corollary 23.3.25.

We now prove (a) and (c). By Proposition 24.2.6, these assertions hold for $\mathscr{F} = \mathcal{O}_X(m)$, hence for direct sums of finitely many $\mathcal{O}_X$-module of the form $\mathcal{O}_X(m_j)$. On the other hand, (a) and (c) are trivial for $p > r$ in view of (b). We now proceed by descendent induction on p. Since $\mathscr{F}$ is coherent, it is a quotient of direct sume of finitely many sheaves $\mathcal{O}_X(m_j)$ (Corollary 23.2.42). That is, we have an exact sequence $0 \to \mathscr{R} \to \mathscr{E} \to \mathscr{F} \to 0$ where $\mathscr{R}$ is coherent and $\mathscr{E}$ satisfies (a) and (c). Since tensoring with $\mathcal{O}_X(n)$ is exact, we obtain an exact sequence

$$H^{p-1}(X, \mathscr{E}(n)) \longrightarrow H^{p-1}(X, \mathscr{F}(n)) \longrightarrow H^p(X, \mathscr{R}(n)).$$

As $\mathscr{E}(n)$ is a direct sum of $\mathcal{O}_X(m_j + n)$, we see $H^{p-1}(X, \mathscr{E}(n))$ is finitely generated by Corollary 24.2.8, and so is $H^p(X, \mathscr{R}(n))$ by induction hypothesis. As A is Noetherian, we then conclude that $H^{p-1}(X, \mathscr{F}(n))$ is finitely generated for any $n \in \mathbb{Z}$, and in particular for $n = 0$. On

the other hand, by induction hypothesis there exists an integer n_0 such that for $n \geq n_0$ we have $H^p(X, \mathscr{R}(n)) = 0$, and we can choose n_0 such that $H^{p-1}(X, \mathscr{E}(n)) = 0$ for $n \geq n_0$, since $\mathscr{E}$ satisfies (c). Therefore we see that $H^{p-1}(X, \mathscr{F}(n)) = 0$ for $n \geq n_0$, which completes the proof. □

Theorem 24.2.11 (Serre). *Let Y be a Noetherian scheme, $f : X \to Y$ be a projective morphism, and $\mathscr{L}$ be an invertible $\mathscr{O}_X$-module that is ample for f. For any coherent $\mathscr{O}_X$-module $\mathscr{F}$, set $\mathscr{F}(n) = \mathscr{F} \otimes_{\mathscr{O}_X} \mathscr{L}^{\otimes n}$.*

(a) The $\mathscr{O}_Y$-module $R^p f_*(\mathscr{F})$ is coherent for $p \geq 0$.

(b) There exists an integer n_0 such that for $n \geq n_0$, we have $R^p f_*(\mathscr{F}(n)) > 0$ for $p > 0$.

(c) There exists an integer n_0 such that for $n \geq n_0$, the canonical homomorphism $f^*(f_*(\mathscr{F}(n))) \to \mathscr{F}(n)$ is surjective.

Proof. We note that the theorem is unchanged if we replace $\mathscr{L}$ by $\mathscr{L}^{\otimes d}$ for $d > 0$. In fact, we then have $\mathscr{F}(n) = (\mathscr{F} \otimes \mathscr{L}^{\otimes r}) \otimes \mathscr{L}^{\otimes kd}$ for $k > 0$ and $0 \leq r < d$, and by hypothesis for any r there is an integer n_r such that for $k \geq n_r$, the properties (b) and (c) holds for $\mathscr{F} \otimes \mathscr{L}^{\otimes r}$. Let n_0 be the supremum of dn_r, then assertion (b) and (c) hold for $n \geq n_0$. In view of Proposition 23.4.42, we may assume that $\mathscr{L}$ is very ample relative to f, so there exists a dominant open immersion $i : X \to P$, where $P = \mathrm{Proj}(\mathscr{S})$ for a quasi-coherent graded $\mathscr{O}_Y$-algebra $\mathscr{S}$ with positive degrees that is finitely generated by $\mathscr{S}_1$; moreover, $\mathscr{L} \cong i^*(\mathscr{O}_P(1))$. Since f is proper, the morphism i is also proper by Corollary 23.5.18, so it is an isomorphism $X \cong P$. We can therefore assme that $X = \mathrm{Proj}(\mathscr{S})$ and $\mathscr{L} = \mathscr{O}_X(1)$, and the theorem then follows from Proposition 24.2.10. □

Corollary 24.2.12. *Under the hypothesis of Theorem 24.2.11, let $0 \to \mathscr{F} \to \mathscr{G} \to \mathscr{H} \to 0$ be an exact sequence of coherent $\mathscr{O}_X$-modules. Then there exists an integer n_0 such that for $n \geq n_0$, the sequence*

$$0 \longrightarrow f_*(\mathscr{F}(n)) \longrightarrow f_*(\mathscr{G}(n)) \longrightarrow f_*(\mathscr{H}(n))$$

is exact.

Proof. This follows from the long exact sequence of f_* and property (b) of Theorem 24.2.11. □

Corollary 24.2.13. *Let Y be a Noetherian scheme, $f : X \to Y$ be a morphism of finite type, and $\mathscr{L}$ be an invertible $\mathscr{O}_X$-module that is ample for f. Let $0 \to \mathscr{F} \to \mathscr{G} \to \mathscr{H} \to 0$ be an exact sequence of coherent $\mathscr{O}_X$-modules such that the supports of $\mathscr{F}$ and $\mathscr{H}$ are proper over Y. Then there exists an integer n_0 such that for $n \geq n_0$, the sequence*

$$0 \longrightarrow f_*(\mathscr{F}(n)) \longrightarrow f_*(\mathscr{G}(n)) \longrightarrow f_*(\mathscr{H}(n))$$

is exact.

Proof. The same reasoning of Theorem 24.2.11 show that we can assume that $\mathscr{L}$ is very ample relative to f, so we can identify X as an open subscheme of $Z = \mathrm{Proj}(\mathscr{S})$, where $\mathscr{S}$ is a quasi-coherent graded $\mathscr{O}_Y$-algebra with positive degrees, such that $\mathscr{S}$ is finitely generated by $\mathscr{S}_1$, and $\mathscr{L} = i^*(\mathscr{O}_Z(1))$, where $i : X \to P$ is the caonical immersion. Now as $\mathrm{supp}(\mathscr{G})$ is closed in X and contained in $\mathrm{supp}(\mathscr{F}) \cap \mathrm{supp}(\mathscr{H})$, it is proper over Y; the supports of $\mathscr{F}, \mathscr{G}, \mathscr{H}$ are then closed in Z. The sheaves $\mathscr{F}' = i_*(\mathscr{F})$, $\mathscr{G}' = i_*(\mathscr{G})$, and $\mathscr{H}' = i_*(\mathscr{H})$ are then coherent $\mathscr{O}_Z$-modules, and the sequence $0 \to \mathscr{F}' \to \mathscr{G}' \to \mathscr{H}' \to 0$ is exact. Moreover, if $g : Z \to Y$ is the structral

morphism, then $f = g \circ i$, and it is clear that $\mathscr{F}'(n) = i_*(\mathscr{F}(n))$ and similarly for $\mathscr{G}'$, $\mathscr{H}'$. The conclusion then follows from Corollary 24.2.12. □

Remark 24.2.3. The assertion (a) of Theorem 24.2.11 is still valid if we only assume that Y is locally Noetherian. In fact, this property is local over Y, and the hypotheses inTheorem 24.2.11 imply that for any affine open $U \subseteq Y$, the restriction f to $f^{-1}(U)$ is projective and $\mathscr{L}|_{f^{-1}(U)}$ is ample for this restriction.

Remark 24.2.4. The assertion (a) of Theorem 24.2.11 is still valid, as we have seen, when we only assumes that X is a quasi-compact and quasi-separated scheme and $f : X \to Y$ is a quasi-compact and quasi-separated morphism (Proposition 23.4.39). However, note that assertion (b) is not true if we suppose that Y is the spectrum of a field k and that f is quasi-projective. For example, let $X' = \operatorname{Spec}(k[T_0, \dots, T_r])$ and X be the union of the affine opens $D(T_i)$ (so that X can be considered as the space $\mathbb{A}^r_k$ with the origin removed). As the immersion $X \to X'$ is quasi-compact, the structural morphism $f : X \to Y$ is quasi-affine, so $\mathscr{O}_X$ is very ample relative to f (Proposition 23.5.1). But the ring $\Gamma(X, \mathscr{O}_X)$ is identified with the intersection of $K[T_0, \dots, T_r]_{T_i}$ for $0 \leq i \leq r$ (Eq. (7.5.1)), which is $K[T_0, \dots, T_r]$, so it follows from (1.3.1) that we have $H^r(X, \mathscr{O}_X^{\otimes n}) = H^r(X, \mathscr{O}_X) = A \neq 0$ for any $n \in \mathbb{Z}$.

Theorem 24.2.14. *Let Y be a Noetherian scheme and $\mathscr{S}$ be a quasi-coherent $\mathscr{O}_Y$-algebra of finite type. Let $f : X \to Y$ be a projective morphism, $\mathscr{S}' = f^*(\mathscr{S})$, $\mathscr{M}$ be a quasi-coherent $\mathscr{S}'$-module of finite type.*

(a) For any $p \geq 0$, $R^p f_*(\mathscr{M})$ is an $\mathscr{S}$-module of finite type.

(b) Let $\mathscr{L}$ be an f-ample $\mathscr{O}_X$-module, and put $\mathscr{M}(n) = \mathscr{M} \otimes \mathscr{L}^{\otimes n}$. Then there exists an integer n_0 such that for $n \geq n_0$, we have $R^p f_*(\mathscr{M}(n)) = 0$ for $p > 0$, and the canonical homomorphism $f^*(f_*(\mathscr{M}(n))) \to \mathscr{M}(n)$ is surjective.

24.2.3 Applications to associated sheaves of graded modules

Theorem 24.2.15. *Let Y be a Noetherian scheme, $\mathscr{S}$ be a quasi-coherent $\mathscr{O}_Y$-algebra of finite type with positive degrees, $X = \operatorname{Proj}(\mathscr{S})$, and $q : X \to Y$ be the structural morphism. Let $\mathscr{M}$ be a quasi-coherent graded $\mathscr{S}$-module that is eventually finite. Then there exists an integer n_0 such that for $n \geq n_0$, the canonical homomorphism of (**??**)*

$$\alpha_n : \mathscr{M}_n \to q_*(\mathscr{P}roj_0(\mathscr{M}(n))) = q_*((\mathscr{P}roj(\mathscr{M}))_n)$$

is bijective. In other words, the canonical homomorphism $\alpha : \mathscr{M} \to \Gamma_*(\mathscr{P}roj(\mathscr{M}))$ is an eventual isomorphisms.

Proof. By Proposition 23.2.36, we can assume that $\mathscr{M}$ is an $\mathscr{S}$-module of finite type. As Y is quasi-compact, by Proposition 23.3.7 there exists an integer $d > 0$ such that $\mathscr{S}^{(d)}$ is generated by $\mathscr{S}_d$, which is of finite type. Now $\mathscr{M}$ is the direct sum of $\mathscr{M}^{(d,k)}$ for $0 \leq k < d$, and each $\mathscr{M}^{(d,k)}$ is quasi-coherent $\mathscr{S}^{(d)}$-module of finite type (Proposition 11.1.35), so it suffices to prove that the canonical homomorphism $\alpha : \mathscr{M}^{(d,k)} \to \Gamma_*((\mathscr{P}roj(\mathscr{M}))^{(d,k)})$ is an eventual isomorphism. In view of **??** (and the diagram (**??**)), we can therefore assume that $\mathscr{S}$ is finitely generated by $\mathscr{S}_1$. As Y is Noetherian, the same reasoning as in Proposition 24.2.10 shows that we can further assume that $Y = \operatorname{Spec}(A)$, $\mathscr{S} = \widetilde{S}$, $\mathscr{M} = \widetilde{M}$, where A is a Noetherian ring, S_1 is a finitely generated A-module, and M is a finitely generated S-module.

We also note that it suffices to prove the assertion for $M = S$. In fact, in the general case, we have an exact sequence $R \to L \to M \to 0$, where L and R are direct sums of graded modules of the form $S(m)$. If the assertion is proved for $M = S$, then it also holds for $M = S(m)$, hence for L and R. Consider the commutative diagram

$$\begin{tikzcd}
\widetilde{R}_n \arrow[r] \arrow[d, "\alpha_n"] & \widetilde{L}_n \arrow[r] \arrow[d, "\alpha_n"] & \widetilde{M}_n \arrow[r] \arrow[d, "\alpha_n"] & 0 \\
q_*(\widetilde{R}(n)) \arrow[r] & q_*(\widetilde{L}(n)) \arrow[r] & q_*(\widetilde{M}(n)) \arrow[r] & 0
\end{tikzcd}$$

The first and second vertical arrows are isomorphisms for $n \gg 0$, so by five lemma we conclude that the middle one is also an isomorphism for sufficiently large n, whence our assertion.

This being done, we are left to prove the theorem for $M = S$; for this, we first suppose that $S = A_0[T_0, \dots, T_r]$ (where T_i are indeterminates). In this case, the assertion follows from Proposition 24.2.6(b). In the general case, S is identified with a quotient of a ring $S' = A[T_0, \dots, T_n]$ by a graded ideal, so X is a closed subscheme of $X' = \mathbb{P}^r_A$. If $j : X \to X'$ is the canonical injection, then $j_*(\widetilde{S}(n))$ is equal to the $\mathscr{O}_{X'}$-module $(\mathscr{P}roj(\widetilde{S}))(n)$ where S is considered as a graded S'-module (Proposition 23.2.46). As $j_*(\widetilde{S}(n))$ is a eventually finite $\mathscr{O}_{X'}$-module, the canonical homomorphism $\alpha_n : S_n \to \Gamma(X', j_*(\widetilde{S}(n)))$ is bijective for $n \gg 0$, and this proves our assertion since $\Gamma(X', j_*(\widetilde{S}(n))) = \Gamma(X, \widetilde{S}(n))$. □

Corollary 24.2.16. *Under the hypotheses of Theorem 24.2.15, let $\mathscr{S}_X = \bigoplus_{n\in\mathbb{Z}} \mathscr{O}_X(n)$, and $\mathscr{F}$ be a quasi-coherent graded $\mathscr{S}_X$-module of finite type. Then $\Gamma_*(\mathscr{F})$ is eventually finite.*

Proof. We see that in the proof of Theorem 24.2.15, X is isomorphic to $\mathrm{Proj}(\mathscr{S}^{(d)})$ which is of finite type over Y. It then follows from **??** that $\mathscr{F}$ is isomorphic to a graded $\mathscr{S}_X$-module of the form $\mathscr{P}roj_0(\mathscr{M})$, where $\mathscr{M}$ is a quasi-coherent $\mathscr{S}$-module of finite type. In view of Theorem 24.2.15, we see $\Gamma_*(\mathscr{F})$ is eventually isomorphic to $\mathscr{M}$, so is eventually finite. □

Remark 24.2.5. Let Y be a Noetherian scheme, $\mathscr{S}$ be a graded $\mathscr{O}_Y$-alegbra satisfying the conditions of Theorem 24.2.15, and $X = \mathrm{Proj}(\mathscr{S})$. Let $\mathscr{K}_{\mathscr{S}}$ be the abelian category of quais-coherent graded $\mathscr{S}$-modules that are eventually finite, and $\mathscr{K}'_{\mathscr{S}}$ be the subcategory of $\mathscr{K}_{\mathscr{S}}$ consists of quais-coherent graded $\mathscr{S}$-modules that are eventually null. Finally, let $\mathscr{K}_X$ be the category of quasi-coherent graded $\mathscr{S}_X$-module of finite type (which amounts to saying, since $\mathscr{S}_X$ is periodic by **??** and **??**, that each $\mathscr{F}_i$ is a coherent $\mathscr{P}_X$-module). Then in view of **??**, **??** and Theorem 24.2.15, the functors $\mathscr{M} \mapsto \mathscr{P}roj(\mathscr{M})$ and $\mathscr{F} \mapsto \Gamma_*(\mathscr{F})$ define an equivalence from the quotient category $\mathcal{K}_{\mathscr{S}}/\mathcal{K}'_{\mathscr{S}}$ to the category $\mathcal{K}_X$. If $\mathscr{S}$ is generated by $\mathscr{S}_1$, we can also replace $mathscrK_X$ by the category of coherent $\mathscr{O}_X$-modules.

Proposition 24.2.17. *Let Y be a Noetherian scheme.*

(a) Let $\mathscr{S}$ be a quasi-coherent graded $\mathscr{O}_Y$-algebra of finite type with positive degrees, $X = \mathrm{Proj}(\mathscr{S})$, and $\mathscr{S}_X = \mathscr{P}roj(\mathscr{S}) = \bigoplus_{n\in\mathbb{Z}} \mathscr{O}_X(n)$. Then $\mathscr{S}_X$ is a periodic graded $\mathscr{O}_X$-algebra whose homogeneous components $(\mathscr{S}_X)_n = \mathscr{O}_X(n)$ are coherent $\mathscr{O}_X$-modules. If $d > 0$ is a period of $\mathscr{S}_X$, then $(\mathscr{S}_X)_d = \mathscr{O}_X(d)$ is an invertible $\mathscr{O}_X$-module that is Y-ample. Moreover, the canonical homomorphism $\alpha : \mathscr{S} \to \Gamma_*(\mathscr{S}_X)$ is a eventual isomorphism.

(b) Conversely, let $q : X \to Y$ be a projective morphism, and $\mathscr{S}'$ be a graded $\mathscr{O}_X$-algebra whose homogeneous components $\mathscr{S}'_n$ are coherent $\mathscr{O}_X$-modules, and that admits a period $d > 0$ such

that $\mathcal{S}'_d$ is an invertible $\mathcal{O}_X$-module that is Y-ample. Then $\mathcal{S} = \bigoplus_{n\geq 0} q_*(\mathcal{S}'_n)$ is a quasi-coherent graded $\mathcal{O}_Y$-algebra of finite type with positive degrees, and there exists a Y-isomorphism $i : X \cong \mathrm{Proj}(\mathcal{S})$ such that $i^*(\mathscr{P}roj(\mathcal{S}))$ is isomorphic to $\mathcal{S}'$.

Proposition 24.2.18. *Let Y be a Noetherian scheme, $q : X \to Y$ be a projective morphism, and $\mathscr{L}$ be an invertible $\mathcal{O}_X$-module that is very ample for q. Then $\mathcal{S} = \bigoplus_{n\geq 0} q_*(\mathscr{L}^{\otimes n})$ is a quasi-coherent $\mathcal{O}_Y$-algebra of finite type such that $\mathcal{S}_n = \mathcal{S}_1^n$ for $n \gg 0$, and there exists an Y-isomorphism $r : X \cong P = \mathrm{Proj}(\mathcal{S})$ such that $\mathcal{S} \cong r^*(\mathcal{O}_P(1))$.*

Proposition 24.2.19. *Let Y be a Noetherian integral scheme, X be an integral scheme, and $f : X \to Y$ be a projective birational morphism. Then there exists a coherent fractional ideal $\mathcal{I} \subseteq \mathcal{K}_Y$ such that X is Y-isomorphic to blow up Y-scheme relative to $\mathcal{I}$. Moreover, there exists an open subset $U \subseteq Y$ such that the restriction $f : f^{-1}(U) \to U$ is an isomorphic, and $\mathcal{I}|_U$ is invertible.*

Proof. By Proposition 23.5.13, there exists an invertible $\mathcal{O}_X$-module $\mathscr{L}$ that is very ample for f, so we can apply Proposition 24.2.18, hence identify X with $\mathrm{Proj}(\mathcal{S})$, where $\mathcal{S} = \bigoplus_{n\geq 0} f_*(\mathscr{L}^{\otimes n})$. We also see that each $f_*(\mathscr{L}^{\otimes n})$ is a torsion-free $\mathcal{O}_Y$-module (Proposition 22.7.26), so $\mathcal{S}$ is canonically identified with a sub-$\mathcal{O}_Y$-module of $\mathcal{S} \otimes_{\mathcal{O}_Y} \mathcal{K}_Y$. By Corollary 22.7.20 this sheaf is simple, so is completely determined when we know its restriction to any non-empty open set, for example to a open nonempty $U' \subseteq U$ (here $U \subseteq Y$ is an open subset such that f is an isomorphic on $f^{-1}(U)$) such that $\mathscr{L}|_{f^{-1}(U')}$ is isomorphic to $\mathcal{O}_X|_{f^{-1}(U')}$. As by hypotheses $f_*(\mathscr{L}^{\otimes n})|_{U'}$ is then isomorphic to $\mathcal{O}_Y|_{U'}$, we conclude that $\mathcal{S} \otimes \mathcal{K}_Y$ is an $\mathcal{K}_Y$-module isomorphic to $\mathcal{K}_Y[T]$, where T is an indeterminate, and $\mathcal{S}$ is eventually isomorphic to the sub-$\mathcal{O}_Y$-module generated by the canonical image of $f_*(\mathscr{L})$ in $\mathcal{S} \otimes_{\mathcal{O}_Y} \mathcal{K}_Y$ (Proposition 24.2.18). But if we identify $\mathcal{S} \otimes_{\mathcal{O}_Y} \mathcal{K}_Y$ with $\mathcal{K}_Y[T]$, then the image of $f_*(\mathscr{L})$ is identified with $\mathcal{I} \cdot T$, where $\mathcal{I}$ is a coherent sub-$\mathcal{O}_Y$-module of $\mathcal{K}_Y$ (Theorem 24.2.11), and its restriction to U' is isomorphic to $\mathcal{O}_Y|_{U'}$. We therefore conclude that $\mathcal{I}|_U$ is invertible and $\mathcal{S}$ is eventually isomorphic to $\bigoplus_{n\geq 0} \mathcal{I}^n$, whence our assertion. □

Corollary 24.2.20. *Under the hypothesis of Proposition 24.2.19, suppose that for any nontrivial coherent sub-$\mathcal{O}_Y$-module $\mathcal{I}$ of $\mathcal{K}_Y$, there exists an invertible $\mathcal{O}_Y$-module $\mathscr{L}$ such that*

$$\Gamma(Y, \mathscr{L} \otimes_{\mathcal{O}_Y} \mathscr{H}om_{\mathcal{O}_Y}(\mathcal{I}, \mathcal{O}_Y)) \neq 0.$$

Then, in the situation of Proposition 24.2.19, we can suppose that $\mathcal{I}$ is an ideal of $\mathcal{O}_Y$. This additional condition is always verified if there exists an ample $\mathcal{O}_Y$-module.

Proof. We first note that

$$\mathscr{L} \otimes_{\mathcal{O}_Y} \mathscr{H}om_{\mathcal{O}_Y}(\mathcal{I}, \mathcal{O}_Y) = \mathscr{H}om_{\mathcal{O}_Y}(\mathscr{L}^{-1}, \mathscr{H}om_{\mathcal{O}_Y}(\mathcal{I}, \mathcal{O}_Y)) = \mathscr{H}om_{\mathcal{O}_Y}(\mathcal{I} \otimes_{\mathcal{O}_Y} \mathscr{L}^{-1}, \mathcal{O}_Y)$$

so the hypothesis signifies that there is a nonzero homomorphism $u : \mathcal{I} \otimes \mathscr{L}^{-1} \to \mathcal{O}_Y$. Now for any $y \in Y$, $(\mathcal{I} \otimes \mathscr{L}^{-1})_y$ is identified with a sub-$\mathcal{O}_{Y,y}$-module of the fraction field $\mathcal{K}_{Y,y}$ of $\mathcal{O}_{Y,y}$, so u_y is necessarily injective, and u is therefore an isomorphism from $\mathcal{I} \otimes \mathscr{L}^{-1}$ onto an ideal $\mathcal{I}'$ of $\mathcal{O}_Y$. As the blow up Y-scheme relative to $\mathcal{I}$ and $\mathcal{I} \otimes \mathscr{L}^{-1}$ are isomorphic (Remark 23.3.2), this proves the corollary. The last remark is a direct concequence of Proposition 23.4.25. □

Corollary 24.2.21. *Let X and Y be integral schemes that are projective over a field k, and let $f : X \to Y$ be a birational k-morphism. Then X is k-isomorphic to a blow up Y-scheme relative to a closed subschem Y' (not necessarily reduced) of Y.*

Proof. In fact, f is projective by Proposition 23.5.25, and as Y is projective over k, the condition of Corollary 24.2.20 is satisfied. It then suffices to consider the closed subscheme of Y defined by the coherent ideal $\mathscr{I}$. □

24.2.4 Euler characteristic and Hilbert polynomial

Let A be an Artinian ring, X be a projective scheme over $Y = \mathrm{Spec}(A)$. For any coherent $\mathscr{O}_X$-module $\mathscr{F}$, the cohomology module $H^i(X, \mathscr{F})$ is finitely generated (Theorem 24.2.11), hence is of finite length. We also see that $H^i(X, \mathscr{F}) = 0$ for $i \gg 0$, so the integer

$$\chi_A(\mathscr{F}) = \sum_{i=0}^{\infty} (-1)^i \ell_A(H^i(X, \mathscr{F}))$$

is defined for any coherent $\mathscr{O}_X$-module. If A is local Artinian, then we say that $\chi_A(\mathscr{F})$ is the Euler characteristic of $\mathscr{F}$ (over the ring A). For $\mathscr{F} = \mathscr{O}_X$, the integer $\chi_A(\mathscr{O}_X)$ is called the **arithmetic genus** of X (over A).

It is clear that the map χ_A is additive on the category of coherent $\mathscr{O}_X$-modules. That is, for an exact sequence $0 \to \mathscr{F}' \to \mathscr{F} \to \mathscr{F}'' \to 0$, we have

$$\chi_A(\mathscr{F}) = \chi_A(\mathscr{F}') + \chi_A(\mathscr{F}'').$$

Theorem 24.2.22. *Let A be a local Artinian ring, X be a projective scheme over $Y = \mathrm{Spec}(A)$, $\mathscr{L}$ be a very ample $\mathscr{O}_X$-module relative to Y, and $\mathscr{F}$ be a coherent $\mathscr{O}_X$-module. For $n \in \mathbb{Z}$, we set $\mathscr{F}(n) = \mathscr{F} \otimes_{\mathscr{O}_X} \mathscr{L}^{\otimes n}$.*

(a) There exists a polynomial $P \in \mathbb{Q}[T]$ such that $\chi_A(\mathscr{F}(n)) = P(n)$ for $n \in \mathbb{Z}$ (the polynomial P is called the Hilbert polynomial of $\mathscr{F}$ over A).

(b) For $n \gg 0$, we have $\chi_A(\mathscr{F}(n)) = \ell_A(\Gamma(X, \mathscr{F}(n)))$.

(c) The leading coefficient of $\chi_A(\mathscr{F}(n))$ is positive.

Example 24.2.23. Let k be a field, $r > 0$ be an integer, and $X = \mathbb{P}^r_k$. Then we have $\chi_A(\mathscr{O}_X(n)) = \binom{n+r}{r}$ for $n \in \mathbb{Z}$. To see this, we divide into three cases.

- For $n > 0$, we have $\chi_A(\mathscr{O}_X(n)) = \dim_k(H^0(X, \mathscr{O}_X(n)))$, which is the number of homogeneous polynomials of degree n and is equal to $\binom{n+r}{r}$.
- For $n < -r$, we have $\chi_A(\mathscr{O}_X(n)) = (-1)^r \dim_k(H^r(X, \mathscr{O}_X(n)))$. If $n = -r - d$, the dimension of $H^r(X, \mathscr{O}_X(n))$ over k is is the number of sequences of integers $(\alpha_0, \ldots, \alpha_r)$ with $\alpha_i > 0$ and $|\alpha| = r + d$ (Proposition 24.2.6), which is equal to the number $\binom{d+r-1}{r} = (-1)^r \binom{n+r}{r}$.
- For $-r \le n \le 0$, we have $\binom{n+r}{r} = 0$ and also $H^i(X, \mathscr{O}_X(n)) = 0$ for $i \ge 0$.

Corollary 24.2.24. *Let A be a local Artinian ring, S be a graded A-algebra of finite type generated by S_1, M be a graded S-module, and $X = \mathrm{Proj}(S)$. Then we have $\chi_A(\widetilde{M}(n)) = \ell_A(M_n)$ for $n \gg 0$.*

Proof. This follows from Theorem 24.2.15, since $H^i(X, \widetilde{M}(n)) = 0$ for $i > 0$ if $n \gg 0$. □

24.2.5 Cohomological criterion for ampleness

Proposition 24.2.25. *Let Y be a Noetherian scheme, $f : X \to Y$ be a proper morphism, and $\mathscr{L}$ be an invertible $\mathscr{O}_X$-module. For any coherent $\mathscr{O}_X$-module $\mathscr{F}$, we set $\mathscr{F}(n) = \mathscr{F} \otimes \mathscr{L}^{\otimes n}$ for $n \in \mathbb{Z}$.*

(i) $\mathscr{L}$ is ample for f.

(ii) For any coherent $\mathscr{O}_X$-module $\mathscr{F}$, there exists an integer n_0 such that for $n \geq n_0$, we have $R^p f_*(\mathscr{F}(n)) = 0$ for $p > 0$.

(iii) For any coherent ideal $\mathscr{I}$ of $\mathscr{O}_X$, there exists an integer n_0 such that for $n \geq n_0$, we have $R^1 f_*(\mathscr{I}(n)) = 0$.

24.3 The finiteness theorem for proper morphisms

24.3.1 The dévissage lemma

Let $\mathscr{A}$ be an abelian category. We say that a subset $\mathfrak{E}$ of objects of $\mathscr{A}$ is exact if $0 \in \mathcal{E}$, and for any exact sequence $0 \to A' \to A \to A'' \to 0$ in $\mathscr{A}$ such that two of A, A', A'' are in $\mathfrak{E}$, then the third one is in $\mathfrak{E}$. The following technique, called the *dévissage lemma*, is introduced by Alexander Grothendieck to prove statements about coherent sheaves on Noetherian schemes. One can think this method as an adaption of Noetherian induction.

Theorem 24.3.1 (Dévissage Lemma). *Let X be a Noetherian scheme, $\mathfrak{E}$ be an exact subset of the category $\mathscr{A}$ of coherent $\mathscr{O}_X$-modules, and X' be a closed subset of X. Suppose that for any irreducible subset Y of X', with generic point y, there exists a coherent $\mathscr{O}_X$-module $\mathscr{G} \in \mathfrak{E}$ such that $\mathscr{G}_y$ is a $\kappa(y)$-vector space of dimension 1. Then any coherent $\mathscr{O}_X$-module with support in X' belongs to $\mathfrak{E}$.*

Proof. Consider the following property $\mathcal{P}(Y)$ on a closed subset Y of X: any coherent $\mathscr{O}_X$-module with support contained in Y belongs to $\mathfrak{E}$. In view of the Noetherian induction principle (Lemma 4.1.17), we are reduced to prove the following: if Y is a closed subset of X' such that $\mathcal{P}(Y')$ is valid for any proper closed subset $Y' \subseteq Y$, then $\mathcal{P}(Y)$ is valid.

Now let $\mathscr{F}$ be a coherent $\mathscr{O}_X$-module with support contained in Y, we show that $\mathscr{F} \in \mathfrak{E}$. In this case, we endow Y with the reduced subscheme structure of X, and let $\mathscr{I}$ be the ideal of $\mathscr{O}_X$ defining it. By Proposition 22.6.17, we see there exists an integer $n > 0$ such that $\mathscr{I}^n\mathscr{F} = 0$; for $1 \leq k \leq n$, we then have an exact sequence

$$0 \longrightarrow \mathscr{I}^{k-1}\mathscr{F}/\mathscr{I}^k\mathscr{F} \longrightarrow \mathscr{F}/\mathscr{I}^k\mathscr{F} \longrightarrow \mathscr{F}/\mathscr{I}^{k-1}\mathscr{F} \longrightarrow 0$$

of coherent $\mathscr{O}_X$-modules. As $\mathfrak{E}$ is exact, by recurrence on k, it suffices to prove that $\mathscr{F}_k = \mathscr{I}^{k-1}\mathscr{F}/\mathscr{I}^k\mathscr{F}$ belongs to $\mathfrak{E}$; in other words, we may also assume that $\mathscr{I}\mathscr{F} = 0$, which means $\mathscr{F} = j_*(j^*(\mathscr{F}))$, where $j : Y \to X$ is the canonical injection.

First suppose that Y is reducible, and let $Y = Y' \cup Y''$, where Y', Y'' are proper closed subsets of Y. We endow Y', Y'' with the reduced subscheme structure, and let $\mathscr{I}', \mathscr{I}''$ be the defining ideals of $\mathscr{O}_X$. Put $\mathscr{F}' = \mathscr{F} \otimes_{\mathscr{O}_X} (\mathscr{O}_X/\mathscr{I}')$ and $\mathscr{F}'' = \mathscr{F} \otimes_{\mathscr{O}_X} (\mathscr{O}_X/\mathscr{I}'')$. The canonical homomorphisms $\mathscr{F} \to \mathscr{F}', \mathscr{F} \to \mathscr{F}''$ then define a homomorphism $u : \mathscr{F} \to \mathscr{F} \oplus \mathscr{F}''$ such that any point $z \notin Y' \cap Y''$, the induced homomorphism $u_z : \mathscr{F} \to \mathscr{F}'_z \oplus \mathscr{F}''_z$ is bijective. In fact, we have $\mathscr{I}' \cap \mathscr{I}'' = \mathscr{I}$; if $z \notin Y''$ then $\mathscr{I}'_z = \mathscr{I}_z$, so $\mathscr{F}'_z = \mathscr{F}_z$ and $\mathscr{F}''_z = 0$; and similarly if $z \notin Y'$. The

kernel and cokernel of u, which belong to $\mathcal{A}$, are then supported in $Y' \cap Y''$, and hence belong to $\mathfrak{E}$ by hypothesis. By the same reasoning, $\mathcal{F}'$ and $\mathcal{F}''$ are in $\mathfrak{E}$, hence so is $\mathcal{F}' \oplus \mathcal{F}''$. We now conclude from the following exact sequences

$$0 \longrightarrow \ker u \longrightarrow \mathcal{F} \longrightarrow \operatorname{im} u \longrightarrow 0$$
$$0 \longrightarrow \operatorname{im} u \longrightarrow \mathcal{F}' \oplus \mathcal{F}'' \longrightarrow \operatorname{coker} u \longrightarrow 0$$

that $\mathcal{F}$ belongs to $\mathfrak{E}$.

If on the other hand Y is irreducible, then the subscheme Y of X is integral. If y is the generic point of Y, we have $\mathcal{O}_{Y,y} = \kappa(y)$, and as $j^*(\mathcal{F})$ is a coherent $\mathcal{O}_Y$-module, $\mathcal{F}_y = (j^*(\mathcal{F}))_y$ is a $\kappa(y)$-vector space of finite dimension m. By hypothesis, there exists a coherent $\mathcal{O}_X$-module $\mathcal{G} \in \mathfrak{E}$ (necessarily supported in Y) such that $\mathcal{G}_y$ is a $\kappa(y)$-vector space of dimension 1, so there is an $\kappa(y)$-isomorphism $(\mathcal{G}_y)^m \cong \mathcal{F}_y$, which is also an $\mathcal{O}_Y$-isomorphism, and as $\mathcal{G}^m$ and $\mathcal{F}$ are coherent, there exists an open neighborhood W of y in X and an isomorphism $\mathcal{G}^m|_W \cong \mathcal{F}|_W$ (Proposition 19.4.6). Let $\mathcal{H}$ be the graph of this isomorphism, which is a coherent sub-$(\mathcal{O}_X|_W)$-module of $(\mathcal{G}^m \oplus \mathcal{F})|_W$. Then there is a sub-$\mathcal{O}_X$-module $\mathcal{H}_0$ of $\mathcal{G}^m \oplus \mathcal{F}$, inducing $\mathcal{H}$ over W and zero over $X - Y$ (Proposition 19.4.6). The restrictions $v : \mathcal{H}_0 \to \mathcal{G}^m$ and $w : \mathcal{H}_0 \to \mathcal{F}$ of the canonical projections of $\mathcal{G}^m \oplus \mathcal{F}$ are then homomorphisms of coherent $\mathcal{O}_X$-modules which are isomorphic over W and over $X - Y$. The kernel and cokernels of these homomorphisms are then supported in the proper closed subset $Y - (Y \cap W)$ of Y, so by hypotheses they belong to $\mathfrak{E}$. On the other hand, we have $\mathcal{G}^m \in \mathfrak{E}$ since $\mathcal{G} \in \mathfrak{E}$, so by the exactness of $\mathfrak{E}$ we conclude that $\mathcal{H}_0 \in \mathfrak{E}$, hence $\mathcal{F} \in \mathfrak{E}$. □

Corollary 24.3.2. *Suppose that the exact subset $\mathfrak{E}$ satisfies the additional property that any direct factor in $\mathcal{A}$ of a coherent $\mathcal{O}_X$-module $\mathcal{F} \in \mathfrak{E}$ belongs to $\mathfrak{E}$. Then the conclusion of Theorem 24.3.1 is still valid if we replace "$\mathcal{G}_y$ is a $\kappa(y)$-vector space of dimension 1" by the condition that $\mathcal{G}_y \neq 0$ (or equivalently* $\operatorname{supp}(\mathcal{G}) = Y$*).*

Proof. In fact, in this case the proof of Theorem 24.3.1 when Y is irreducible can be modified as follows: $\mathcal{G}_y$ is a $\kappa(y)$-vector space of dimension $q > 0$, and we then have an isomorphism $(\mathcal{G}_y)^m \cong (\mathcal{F}_y)^q$. By the same reasoning, we obtain that $\mathcal{F}^q \in \mathfrak{E}$, so $\mathcal{F} \in \mathfrak{E}$ by our additional assumption on $\mathfrak{E}$. □

24.3.2 The finiteness theorem for proper morphisms

Theorem 24.3.3. *Let Y be a locally Noetherian scheme and $f : X \to Y$ be a proper morphism. Then for any coherent $\mathcal{O}_X$-module $\mathcal{F}$, the $\mathcal{O}_Y$-module $R^p f_*(\mathcal{F})$ is coherent for $p > 0$.*

Proof. Since this question is local over Y, we can suppose that Y is Noetherian, and hence X is Noetherian (Proposition 22.6.20). The coherent $\mathcal{O}_X$-module $\mathcal{F}$ satisfying the conclusion of Theorem 24.3.3 is easily seen to form an exact subset $\mathfrak{E}$ of the category $\mathcal{A}$ of coherent $\mathcal{O}_X$-modules. In fact, let $0 \to \mathcal{F}' \to \mathcal{F} \to \mathcal{F}'' \to 0$ be an exact sequence of coherect $\mathcal{O}_X$-modules, and suppose for example that $\mathcal{F}', \mathcal{F}$ belong to $\mathfrak{E}$. Then we have an exact sequence

$$R^{p-1} f_*(\mathcal{F}'') \xrightarrow{\partial} R^p f_*(\mathcal{F}) \longrightarrow R^p f_*(\mathcal{F}) \longrightarrow R^p f_*(\mathcal{F}'') \xrightarrow{\partial} R^{p+1} f_*(\mathcal{F}')$$

in which the four outer terms are conherent. It then follows from Corollary 19.4.19 that $R^p f_*(\mathcal{F})$ is coherent. We also note that any direct factor $\mathcal{F}' \in \mathcal{A}$ of a coherent $\mathcal{O}_X$-module $\mathcal{F} \in \mathfrak{E}$

belongs to $\mathfrak{E}$: in fact, $R^p f_*(\mathscr{F}')$ is then a direct factor of $R^p f_*(\mathscr{F})$ (**??**), so is of finite type, and since it is quasi-coherent (Proposition 24.1.13), it is coherent (note that Y is Noetherian). In view of Corollary 24.3.2, we only need to prove that if X is irreducible with generic point x, then there exists a coherent $\mathscr{O}_X$-module $\mathscr{F} \in \mathfrak{E}$ such that $\mathscr{F}_x \neq 0$. In fact, for any irreducible closed subscheme Y of X with canonical injection $j : Y \to X$, the composition $f \circ j$ is proper (Proposition 23.5.17), and if $\mathscr{G}$ is a coherent $\mathscr{O}_Y$-module supported in Y, then $j_*(\mathscr{G})$ is a coherent $\mathscr{O}_X$-module such that $R^p(f \circ j)_*(\mathscr{G}) = R^p f_*(j_*(\mathscr{G}))$ (**??**), so we can apply our result on Y.

By Chow's lemma (Theorem 23.5.28), there exists an irreducible scheme X' and a surjective projective morphism $g : X' \to X$ such that $f \circ g : X' \to Y$ is projective. □