Commutative Algebra

Dhruv Goel

Contents

Preface 3

1 Fundamentals 4

1.1 Localization 5

1.2 Some Affine Algebraic Geometry 9

1.2.1 Scheinnullstellensatz, Radicals, and Local Rings 9

1.2.2 Minimal Primes and Prime Avoidance 11

1.2.3 Krull Dimension 12

1.3 Noetherian and Artinian Rings and Modules 14

1.3.1 Noetherian Rings 15

1.3.2 Artinian Rings 16

1.4 Unique Factorization I 19

1.5 Cayley-Hamilton Theorem, Nakayama's Lemma, and Krull's Intersection Theorem 22

1.6 Some Graded Commutative Algebra 25

1.6.1 Hilbert Functions and Polynomials 26

1.6.2 Completion and the Artin-Rees Lemma 28

1.7 Fractional Ideals and their Invertibility 30

1.8 Exercises 33

2 Primary Decomposition and Local Dimension Theory 37

2.1 Associated Primes 38

2.2 Primary Decomposition and the Lasker-Noether Theorem 41

2.3 Artinian Rings Revisited, Ideals of Definition, and the Hilbert-Samuel Polynomial 47

2.4 The Main Theorem of Local Dimension Theory 50

2.5 Regular (Local) Rings I 54

2.6 Regular Sequences, Depth, and Cohen-Macaulay Rings 57

2.7 Serre's Conditions R and S 60

2.8 Exercises 61

3 Integrality and Cohen-Seidenberg Theory 63

3.1 Fundamentals of Integrality 64
3.2 Cohen-Seidenberg Theory 68
3.3 Extensions of Homomorphisms to Algebraically Closed Fields 70
3.4 Krull-Akizuki Theorem 72
3.5 Exercises 73

4 Derivations 74

4.1 Derivations and Kähler Differentials 75
4.2 Fundamental Exact Sequences 78
4.3 Smoothness 79

5 Field Theory 80

5.1 Linear Disjointness 81
5.2 Some Dependence Relations Involving Fields 84
5.2.1 Algebraic Dependence 84
5.2.2 *p*-dependence 85
5.2.3 Differential Dependence 86
5.3 Separability 87
5.4 Étale Algebras and Grothendieck's Reformulation of Galois Theory 91
5.5 Exercises 95

6 Global Dimension Theory 97

6.1 Noether Normalization and Zariski's Lemma 98
6.2 Some Classical Algebraic Geometry 101
6.2.1 The Classical Nullstellensatz 101
6.2.2 Jacobson Rings 102
6.2.3 Dimension of Affine Varieties 103
6.3 Exercises 105

7 Valuation Rings and Dedekind Domains 106

7.1 Valuation Rings and Discrete Valuation Rings 107
7.2 Dedekind Domains and their Extensions 113
7.3 Modules over Dedekind Domains 117
7.4 Exercises 118

8 A Little Homological Algebra and Some Applications 119

8.1 Projective, Injective, and Flat Modules 120
8.2 Derived Functors: Tor and Ext 128
8.3 First Applications of Homological Methods 133

8.4 Exercises 135

9 Selected Advanced Topics 137

9.1 Unique Factorization II 138

9.2 More on Flatness 139

10 Appendices 140

10.1 Length and the Jordan-Hölder Theorem 141

10.2 Classical Algebra: Gauss and Eisenstein 144

10.3 Dependence Relations 148

10.4 Trace, Norm, and Discriminant 151

10.5 Derived Functors in Abelian Categories 154

10.6 Pathologies, or Counterexamples in Commutative Algebra 159

10.7 Exercises 161

11 Possible Hints to Selected Exercises 163

Bibliography 165

Preface

Based on Math 221 Fall 2020 by Popa. I make no originality claims. Much from Szamuely, Lang, Cohn, Sam's notes, Matsumura, Frölich-Taylor, Conrad's notes, Poonen's notes, Stacks project. The appendices collect some topics which some readers may have seen previously and fit in differently than the flow in the text.

[TODO]

Conventions

- A *ring* is always taken to mean a commutative unitary ring, unless explicitly specified otherwise (as will be in sections ...).
- We do not disallow the zero ring, although when we speak of proper ideals (including prime or maximal ideals, which are always assumed to be proper), we implicitly assume that the ring is nonzero. The zero ring is not considered to be a field.
- For a ring R, we denote the subset of units of R by $R^\times \subset R$, so that a nonzero ring R is a field iff $R^\times = R \smallsetminus \{0\}$.
- For subsets A, B of a set X, we take $A \subset B$ to mean $x \in A \Rightarrow x \in B$; therefore, the case $A = B$ is not excluded. If we want to specifically exclude this case, we write $A \subsetneq B$.
- The symbol $\mathbb{N}$ always refers to the set of all nonnegative integers, so that, in particular, $0 \in \mathbb{N}$.
- A *monoid* is always a commutative monoid written additively.

Chapter 1

Fundamentals

1.1 Localization

We introduce the concept of localization, which is absolutely fundamental to any serious ring theory. To motivate this, note that if $\eta : R \to R'$ is a ring homomorphism, then the set $S_\eta := \{x \in R : \eta(x) \in (R')^\times\}$ of elements of R which map to a unit of R' forms a *multiplicative subset* of R, i.e., finite products of elements of S_η again lie in S_η. Conversely, given a multiplicative subset S of a ring R, we can find a ring R' and a homomorphism $\eta : R \to R'$ such that $S \subset S_\eta$; moreover, there is a "universal" way to do this. This is the operation we perform when going from the integers $\mathbb{Z}$ to the rational numbers $\mathbb{Q}$, for instance, but is much more general than that (c.f. 1.1.7). This motivates

Definition 1.1.1 (Localization)**.** Let R be a ring.

(a) A subset $S \subset R$ is called *multiplicative* if finite products of elements of S are in S.

(b) If $S \subset R$ is a multiplicative system, the *localization of R with respect to S* is a ring $S^{-1}R$ and a homomorphism $\eta : R \to S^{-1}R$ such that $\eta(S) \subset (S^{-1}R)^\times$ and that $(S^{-1}R, \eta)$ is initial with respect to this property. The homomorphism η is called the *localization homomorphism.*

(c) In the above setting, if M is an R-module, then the *localization of M with respect to S* is an $S^{-1}R$-module $S^{-1}M$ with an R-module homomorphism[1] $\eta : M \to S^{-1}M$ such that any R-module homomorphism from M to (the underlying R-module of) an $S^{-1}R$-module factors through η.

Remark 1.1.2.

(a) By the universal property, localization is unique up to unique isomorphism commuting with the η's–if it exists. We give three explicit constructions: one is to take simply $S^{-1}R := R[\{x_s\}]_{s\in S}/(sx_s - 1)$, and another is given by taking classes $s^{-1}x$ with $s^{-1}x = t^{-1}y$ iff there is a $u \in S$ such that $u(sy - tx) = 0$, defining addition and multiplication in the usual way, and letting $\eta : x \mapsto 1^{-1}x$. The third construction first inverts a single element s (or equivalently the subset $S = \{1, s, s^2, \dots\}$ of powers of s) by consider the colimit $R[s^{-1}]$ of $R \xrightarrow{s} R \xrightarrow{s} R \cdots$ in the category of R-modules and equipping it with a suitable R-algebra structure; the general case is handled by noting that $S^{-1}R = \varinjlim_{s\in S} R[s^{-1}]$ as R-algebras.[2] Similarly, $S^{-1}M$ can be constructed in several ways; the most explicit is to take classes $s^{-1}m$ as in the second construction, although see (b).

(b) The universal property amounts to saying that the additive functor $S^{-1} : R\text{-}\mathsf{Mod} \to S^{-1}R\text{-}\mathsf{Mod}$ is left-adjoint to the restriction of scalars functor $\eta_* : S^{-1}R\text{-}\mathsf{Mod} \to R\text{-}\mathsf{Mod}$.This tells us that the localization of modules can be obtained only from localization of rings: there is a natural isomorphism $S^{-1}R \otimes_R M \to S^{-1}M$ of R-modules and $S^{-1}R$-modules for any R, S, M as above.

(c) Algebraically, localization of a ring R (resp. an R-module M) at a subset S is the "freest" way to make S invertible as elements of a ring to which R maps (resp. as endomorphisms of an R-module to which M maps). Geometrically, we can think of the localization of a ring R at a subset S as the operation of "throwing out (the vanishing locus of) S"; try to interpret 1.1.4, 1.1.5 and 1.1.12 this way.

Lemma 1.1.3. Let $S \subset R$ be a multiplicative subset in a ring R and M be an R-module. Then the localization map $\eta : M \to S^{-1}M$ has kernel

$$(0 :_S M) := \{m \in M : um = 0 \text{ for some } u \in S\}.$$

In particular:

[1] Here $S^{-1}M$ is considered an R-module by restriction of scalars via the map $\eta : R \to S^{-1}R$.

[2] Of course, in doing this, one should be familiar with arbitrary colimits of algebras.

(a) The localization $S^{-1}R$ is zero iff $0 \in S$.
(b) The localization homomorphism $\eta : R \to S^{-1}R$ is injective iff S contains no zero divisors.

Proof. We have $1^{-1}0 = 1^{-1}m$ iff there is a $u \in S$ such that $um = 0$; (a) and (b) follow immediately. ■

Example 1.1.4 (Inverting an Element)**.** Given any ring R and $s \in R$, the subset $S = s^{\mathbb{N}} = \{1, s, s^2, \dots\}$ of powers of s in R is multiplicative. The localization $S^{-1}R \cong R[x]/(sx - 1)$ is denoted by $R[s^{-1}]$. By 1.1.3(a), this is zero iff x is nilpotent.

Example 1.1.5 (Localization at a Prime)**.** Let R be a ring and $\mathfrak{p} \subset R$ an ideal. Then $\mathfrak{p}$ is prime iff its complement $S := R \smallsetminus \mathfrak{p}$ is multiplicative, in which case the ring $S^{-1}R = (R \smallsetminus \mathfrak{p})^{-1}R$ is called the *localization of* R *at* $\mathfrak{p}$ and denoted $R_{\mathfrak{p}}$. Similarly, given an R-module M, the localization $S^{-1}M =: M_{\mathfrak{p}}$ is called the *localization of* M *at* $\mathfrak{p}$.

Example 1.1.6 (Total Quotient Ring)**.** Given a ring R, the set $S = R \smallsetminus \mathcal{Z}(R) \subset R$ of nonzerodivisors of R is multiplicative. The localization $S^{-1}R =: \operatorname{Quot} R$ is called the *total quotient ring* of R. By 1.1.3(b), the map $\eta : R \to \operatorname{Quot} R$ is injective. This is the largest localization of R for which the localization map is injective: indeed, if S is another subset such that $\eta : R \to S^{-1}R$ is injective, then $S \subset R \smallsetminus \mathcal{Z}(R)$ and so by 1.1, the natural morphism $S^{-1}R \to \operatorname{Quot} R$ is injective. The total quotient ring of R satisfies the following universal property: if $\varphi : R \to S$ is a ring homomorphism such that $\varphi(R \smallsetminus \mathcal{Z}(R)) \subset S \smallsetminus \mathcal{Z}(S)$ (i.e., φ takes nonzerodivisors in R to nonzerodivisors in S), then φ extends to a homomorphism $\operatorname{Quot} R \to \operatorname{Quot} S$.

Example 1.1.7 (Field of Fractions)**.** When R is a domain, 1.1.6 is a special case of 1.1.5: a ring R is a domain iff the ideal (0) is prime iff $\mathcal{Z}(R) = (0)$, in which case the localization $R_{(0)} = \operatorname{Quot} R = \operatorname{Frac} R$ is the *field of fractions* or *fraction field* of R. Again, the map $\eta : R \to \operatorname{Frac} R$ is injective. The fraction field of an integral domain is universal with respect to injective homomorphisms out of the domain to fields; in other words, the fraction field functor from the category of integral domains and injective homomorphisms to the category of fields and field homomorphisms is left adjoint to the forgetful functor. By 1.1, if R is an integral domain, then all localizations of R can be embedded in $\operatorname{Frac} R$ and are integral domains themselves.

For an example of a total quotient ring of a ring that is not a domain, see 1.3. One reason for the usefulness of this notion comes from the fact that many module-theoretic properties can be checked locally. One instance of this phenomenon is

Lemma 1.1.8. Let R be a ring and M be an R-module. Then for any element $x \in M$, the following are equivalent:

(a) $x = 0$,
(b) $[x] = 0 \in S^{-1}M$ for every multiplicative $S \subset R$,
(c) $[x] = 0 \in M_{\mathfrak{p}}$ for every prime $\mathfrak{p}$, and
(d) $[x] = 0 \in M_{\mathfrak{m}}$ for every maximal ideal $\mathfrak{m}$.

In particular, the following are equivalent:

(a) $M = 0$,
(b) $S^{-1}M = 0$ for every multiplicative $S \subset R$.
(c) $M_{\mathfrak{p}} = 0$ for all $\mathfrak{p}$, and
(d) $M_{\mathfrak{m}} = 0$ for all $\mathfrak{m}$.

Proof. Clearly, (a) $\Rightarrow$ (b) $\Rightarrow$ (c) $\Rightarrow$ (d). For (d) $\Rightarrow$ (a), for $0 \neq x \in M$, the annihilator $\operatorname{Ann}_R(x) \subset R$ is a proper ideal, so there is an $\mathfrak{m} \subset R$ such that $\operatorname{Ann}_R(x) \subset \mathfrak{m}$; then $0 \neq [x] \in M_{\mathfrak{m}}$ by 1.1.3. ■

Another series of instances of this phenomenon are captured by

Theorem 1.1.9 (Localization is Exact)**.** If $\mathscr{C}$ is a complex of R-modules and $S \subset R$ is a multiplicative subset, then the natural map $S^{-1}\mathrm{H}\mathscr{C} \to \mathrm{H}(S^{-1}\mathscr{C})$ given by functoriality is an isomorphism.

Proof. This map takes $s^{-1}[n] \mapsto [s^{-1}n]$. For injectivity, if $[s^{-1}n] = 0$, then there is a $t^{-1}m$ such that $s^{-1}n = \partial(t^{-1}m) = t^{-1}\partial m$. Then there is a $u \in S$ such that $u(s \cdot \partial m - tn) = 0$ so that $utn = \partial(usm)$ and

$$s^{-1}[n] = (uts)^{-1}ut[n] = (uts)^{-1}[utn] = (uts)^{-1}[\partial(usm)] = (uts)^{-1}0 = 0.$$

For surjectivity, note that a class $[s^{-1}n]$ is given an element $s^{-1}n$ with $\partial(s^{-1}n) = s^{-1}\partial n = 0$, so there is a $u \in S$ such that $0 = u\partial n = \partial(un)$. Then $(us)^{-1}[un] \mapsto [s^{-1}n]$. ■

Corollary 1.1.10. Let R be a ring and $\varphi : M \to N$ and $\psi : N \to P$ homomorphisms of R-modules.

(i) The following are equivalent:
  (a) $M \xrightarrow{\varphi} N \xrightarrow{\psi} P$ is exact.
  (b) $S^{-1}M \xrightarrow{S^{-1}\varphi} S^{-1}N \xrightarrow{S^{-1}\psi} S^{-1}P$ is exact for every multiplicative $S \subset R$.
  (c) $M_\mathfrak{p} \xrightarrow{\varphi_\mathfrak{p}} N_\mathfrak{p} \xrightarrow{\psi_\mathfrak{p}} P_\mathfrak{p}$ is exact for all $\mathfrak{p}$.
  (d) $M_\mathfrak{m} \xrightarrow{\varphi_\mathfrak{m}} N_\mathfrak{m} \xrightarrow{\psi_\mathfrak{m}} P_\mathfrak{m}$ is exact for all $\mathfrak{m}$.

(ii) The following are equivalent:
  (a) $\varphi : M \to N$ is injective (resp. surjective, resp. bijective).
  (b) $S^{-1}\varphi : S^{-1}M \to S^{-1}N$ is injective (resp. surjective, resp. bijective) for every multiplicative $S \subset R$.
  (c) $\varphi_\mathfrak{p} : M_\mathfrak{p} \to N_\mathfrak{p}$ is injective (resp. surjective, resp. bijective) for all $\mathfrak{p}$.
  (d) $\varphi_\mathfrak{m} : M_\mathfrak{m} \to N_\mathfrak{m}$ is injective (resp. surjective, resp. bijective) for all $\mathfrak{m}$.

Proof. Part (i) follows from 1.1.8 and 1.1.9. Part (ii) follows by applying (i) and choosing one of the M and P to be zero. ■

The above corollary (specifically (ii)(b)) says that if R is a ring and $N \subset M$ an R-submodule, then for any multiplicative system $S \subset R$, the natural map $S^{-1}N \to S^{-1}M$ is injective, allowing us to think of $S^{-1}N$ as an $S^{-1}R$-submodule of $S^{-1}M$. We will implicitly use this identification in all that follows. This perspective allows us to relate submodules of the localization to submodules of the original module as in

Observation 1.1.11 (Submodules of Localization)**.** Let R be a ring, $S \subset R$ multiplicative, M an R-module, and $\eta : M \to S^{-1}M$ the localization map.

(a) If M is finitely generated over R, then so is $S^{-1}M$ over $S^{-1}R$, by the images under η of the generators.

(b) If $N \subset M$ is a submodule, then $N \subset \eta^{-1}(S^{-1}N) = \{m \in M : (\exists\, s \in S)\, sm \in N\}$.[3] For any $S^{-1}R$-submodule $L \subset S^{-1}M$ we have $L = S^{-1}(\eta^{-1}L)$.[4]

(c) Every $S^{-1}R$-submodule of $S^{-1}M$ is of the form $S^{-1}N$ for some R-submodule $N \subset M$. In particular, if M is Noetherian (resp. Artinian) as an R-module, then so is $S^{-1}M$ as an $S^{-1}R$-module.

[3] In general, equality need not hold; for instance, if $S = R$.

[4] The inclusion $L \subset S^{-1}\eta^{-1}L$ follows from noting that $s^{-1}\ell \in L \Rightarrow \ell \in \eta^{-1}L$.

(d) In particular, if R is a Noetherian (resp. Artinian) ring, then every localization $S^{-1}R$ is also Noetherian (resp. Artinian), because every $S^{-1}R$-module M is of the form $S^{-1}M'$ for some R-module M', namely $M' = M$ itself.

Reinterpreting the above in the language of ideals gives us

Corollary 1.1.12 (Ideals in Localization)**.** Let R be a ring and $S \subset R$ multiplicative and $\eta : R \to S^{-1}R$ the localization.

(a) If $\mathfrak{a} \subset R$ is an ideal, then so is $S^{-1}\mathfrak{a} \subset S^{-1}R$; if $\mathfrak{a}$ is finitely generated then so is $S^{-1}\mathfrak{a}$. Further, $S^{-1}\mathfrak{a}$ is proper iff $\mathfrak{a} \cap S = \emptyset$.

(b) If $\mathfrak{a} \subset R$ is an ideal, then $\mathfrak{a} \subset \eta^{-1}(S^{-1}\mathfrak{a})$. If $\mathfrak{b} \subset S^{-1}R$ is an ideal, then $\mathfrak{b} = S^{-1}(\eta^{-1}\mathfrak{b})$.

(c) If $\mathfrak{q} \subset R$ is prime with $\mathfrak{q} \cap S = \emptyset$, then in fact $\mathfrak{q} = \eta^{-1}(S^{-1}\mathfrak{q})$ and so $S^{-1}\mathfrak{q}$ is prime in $S^{-1}R$.

(d) The maps $\mathfrak{q} \mapsto S^{-1}\mathfrak{q}$ and $\mathfrak{Q} \mapsto \eta^{-1}\mathfrak{Q}$ give inverse bijections between primes $\mathfrak{q} \subset R$ disjoint from S and primes $\mathfrak{Q} \subset S^{-1}R$.

(e) In particular, if $S = R \setminus \mathfrak{p}$ is the complement of a prime, then there is a bijective correspondance between primes $\mathfrak{q} \subset R$ contained in $\mathfrak{p}$ and primes of $R_\mathfrak{p}$. In particular, $R_\mathfrak{p}$ has a unique maximal ideal, namely $\mathfrak{p}R_\mathfrak{p}$, so it is a local ring (see 1.2.7).

For a ring R, we let $\operatorname{Spec} R$ denote the set of its prime ideals and call it the *spectrum* of R. The above result says that $\operatorname{Spec} S^{-1}R$ can be identified with the subset of primes of $\operatorname{Spec} R$ disjoint from S.[5] In particular, $\operatorname{Spec} R_\mathfrak{p}$ is the set of primes contained in $\mathfrak{p}$: we have "localized" to look only at primes contained in $\mathfrak{p}$. (This is in analogy with the fact that the operation $R \mapsto R/\mathfrak{p}$ lets us look only at the primes containing $\mathfrak{p}$; c.f. the next section.) In this vein, the following result is very believable.

Corollary 1.1.13 (Contractions)**.** Let $\varphi : R \to S$ be a ring homomorphism and $\mathfrak{p} \subset R$ be a prime. The following conditions are equivalent.

(a) There is a prime $\mathfrak{q} \subset S$ such that $\mathfrak{p} = \varphi^{-1}\mathfrak{q}$.

(b) The ring $\kappa(\mathfrak{p}) \otimes_R S \cong (S/\mathfrak{p}S)_\mathfrak{p} \cong S_\mathfrak{p}/\mathfrak{p}S_\mathfrak{p}$ is nonzero.

(c) Equality holds in $\mathfrak{p} \subset \varphi^{-1}(\mathfrak{p}S)$.

Proof.

(a) ⇔ (b) By 1.1.12, the primes of $\kappa(\mathfrak{p}) \otimes_R S$ correspond to the primes of S contracting to $\mathfrak{p}$.

(b) ⇔ (c) By 1.1.12(a), the ideal $\mathfrak{p}S_\mathfrak{p} = (\mathfrak{p}S)S_\mathfrak{p}$ of $S_\mathfrak{p}$ is proper iff $\mathfrak{p}S \cap \varphi(R \setminus \mathfrak{p}) = \emptyset$, which happens iff $\varphi^{-1}(\mathfrak{p}S) \subset \mathfrak{p}$.

■

Remark 1.1.14. Geometrically, 1.1.13 amounts to the statement that if $f : X \to Y$ is a continuous map of spaces and $y \in Y$, then $y \in f(X)$ iff the fiber $X_y = f^{-1}(y)$ is nonempty iff equality holds in $f(X_y) \subset \{y\}$.

[5] In algebraic geometry, one shows that the natural morphism $\operatorname{Spec} S^{-1}R \to \operatorname{Spec} R$ is a topological embedding as a subspace.

1.2 Some Affine Algebraic Geometry

Next, we consider three fundamental aspects of affine algebraic geometry that will be helpful to keep in mind: the Scheinnullstellensatz, minimal primes and prime avoidance, and the notion of dimension. This will give us a good excuse to at least introduce the fundamentals of algebraic geometry that will help motivate many constructions below.

1.2.1 Scheinnullstellensatz, Radicals, and Local Rings

Let R be a ring. For any subset $\mathfrak{a} \subset R$, we define $\mathbb{V}(\mathfrak{a}) := \{\mathfrak{p} : \mathfrak{p} \supset \mathfrak{a}\} \subset \operatorname{Spec} R$, and for any subset $X \subset \operatorname{Spec} R$, we let $\mathbb{I}(X) := \bigcap_{\mathfrak{p} \in X} \mathfrak{p}$. Clearly $\mathbb{V}(\mathfrak{a}) = \mathbb{V}(\langle \mathfrak{a} \rangle)$, where $\langle \mathfrak{a} \rangle \subset R$ is the ideal generated by $\mathfrak{a}$; therefore, we can restrict ourselves to looking at ideals $\mathfrak{a}$. Then $\mathbb{V}$ and $\mathbb{I}$ give inclusion-reversing maps between the set of ideals in R and subsets of $\operatorname{Spec} R$; these are not inverse bijections, but rather inverse Galois correspondences, and hence inverse bijections on appropriate subsets–namely the set of subsets $X \subset \operatorname{Spec} R$ of the form $X = \mathbb{V}(\mathfrak{a})$ for some $\mathfrak{a}$, and the set of ideals $\mathfrak{a} \subset R$ of the form $\mathfrak{a} = \mathbb{I}(X)$ for some $X \subset \operatorname{Spec} R$.

Observation 1.2.1. Given a ring R, we have:

(a) $\mathbb{V}(0) = \operatorname{Spec} R$ and $\mathbb{V}(1) = \emptyset$,
(b) If $(\mathfrak{a}_i)$ is a family of ideals of R, then $\mathbb{V}\left(\bigcup_i \mathfrak{a}_i\right) = \mathbb{V}\left(\sum_i \mathfrak{a}_i\right) = \bigcap_i \mathbb{V}(\mathfrak{a}_i)$.
(c) If $\mathfrak{a}, \mathfrak{b} \subset R$ are ideals, then $\mathbb{V}(\mathfrak{a} \cap \mathfrak{b}) = \mathbb{V}(\mathfrak{a}\mathfrak{b}) = \mathbb{V}(\mathfrak{a}) \cup \mathbb{V}(\mathfrak{b})$.

It follows from 1.2.1 that the subsets of $\operatorname{Spec} R$ of the form $\mathbb{V}(\mathfrak{a})$ for $\mathfrak{a} \subset R$ satisfy the axioms for closed sets of a topology on $\operatorname{Spec} R$; this topology is called the *Zariski topology.* It is easy to see that if $X \subset \operatorname{Spec} R$ is any subset, then $\mathbb{V}(\mathbb{I}(X)) = \overline{X}$, where the closure is with respect to the Zariski topology. Conversely, if $\mathfrak{a} \subset R$ is any ideal, then $\mathbb{I}(\mathbb{V}(\mathfrak{a}))$ is given by

Theorem 1.2.2 (Scheinnullstellensatz)**.** For a ring R and ideal $\mathfrak{a} \subset R$, we have $\mathbb{I}(\mathbb{V}(\mathfrak{a})) = \sqrt{\mathfrak{a}}$.

Proof. Replace R by $R/\mathfrak{a}$ to assume $\mathfrak{a} = 0$. To show the nontrivial inclusion, suppose that $s \in R$ is *not* nilpotent. Then $R[s^{-1}]$ is not the zero ring by 1.1.4, and therefore has a maximal ideal $\mathfrak{m}$. If $\eta : R \to R[s^{-1}]$ is the localization map, then the preimage $\eta^{-1}\mathfrak{m} \subset R$ is a prime not containing s. ■

Remark 1.2.3. Geometrically, 1.2.2 says that the any regular function that vanishes at every point on the scheme $\operatorname{Spec} R$ is nilpotent, so the only regular function that vanishes that every point on a reduced affine scheme is zero. In light of the above discussion, we conclude from 1.2.2 that the maps $\mathbb{V}$ and $\mathbb{I}$ give inverse bijections between the set of closed subsets of $\operatorname{Spec} R$ and radical ideals of R. In algebraic geometry, this statement says that every closed subscheme of the affine scheme $\operatorname{Spec} R$ admits a unique reduced structure; this is true of all schemes and not just affine schemes.

Definition 1.2.4. Given a ring R, we define its *nilradical* to be

$$\operatorname{Nil}(R) := \sqrt{0} = \bigcap_{\mathfrak{p} \subset R} \mathfrak{p}.$$

The ring R is said to be *reduced* if $\operatorname{Nil}(R) = 0$. The *reduction* of a ring R is defined to be the quotient $R^{\mathrm{red}} := R/\operatorname{Nil}(R)$; this is the largest reduced quotient ring of R.

Remark 1.2.5. Reduction is functorial, and the reduction of a reduced ring is itself; put another way, $R \to R^{\mathrm{red}}$ is initial with respect to homomorphisms out of R to reduced rings, i.e., if $\varphi : R \to S$ is a homomorphism with S reduced, then φ factors as $R \to R^{\mathrm{red}} \xrightarrow{\bar{\varphi}} S$ for some $\bar{\varphi} : R^{\mathrm{red}} \to S$. In fact, the full subcategory of Ring consisting of reduced rings is reflective in the sense that the reduction functor is left adjoint to the inclusion; in particular, reduction commutes with arbitrary colimits.

Given that the intersection of all primes of a ring is interesting, it makes sense to look also at the intersection of all maximal ideals of a ring.

Proposition/Definition 1.2.6 (Jacobson Radical)**.** Let R be a ring and $x \in R$ be an element. Then the folowing are equivalent:

(a) The element x lies in every maximal ideal of R.
(b) For any $y \in R$ and unit $u \in R^\times$, we have $u + xy \in R^\times$.
(c) For any $y \in R$, we have $1 + xy \in R^\times$.

The ideal consisting of all such $x \in R$ is called the *Jacobson radical* of R, and is denoted by

$$\mathrm{Jac}(R) := \bigcap_{\mathfrak{m} \subset R} \mathfrak{m}.$$

Proof.

(a) ⇒ (b) If x were to lie in every maximal ideal of R, but there were $y \in R$ and $u \in R^\times$ such that $u + xy \notin R^\times$, then there would be a maximal $\mathfrak{m} \subset R$ such that $u + xy \in \mathfrak{m}$. Then $x, u + xy \in \mathfrak{m} \Rightarrow u \in \mathfrak{m}$, a contradiction.

(b) ⇒ (c) Clear.

(c) ⇒ (a) If x were such but there were a maximal ideal $\mathfrak{m} \subset R$ such that $x \notin \mathfrak{m}$, then $\mathfrak{m} + (x) = (1)$ implies $m - xy = 1$ for some $m \in \mathfrak{m}, y \in R$, giving $m = 1 + xy \in R^\times \cap \mathfrak{m}$, a contradiction.

■

Proposition/Definition 1.2.7 (Local Rings)**.** For a nonzero ring R, the folowing are equivalent:

(a) The set of nonunits $R \setminus R^\times$ is an ideal.
(b) The ring R has a unique maximal ideal.
(c) For any maximal ideal $\mathfrak{m} \subset R$, any element of $1 + \mathfrak{m}$ is a unit.

A ring R is said to be *local* if it is nonzero and satisfies these equivalent conditions. Finally, every nonzero localization and quotient of a local ring is local.

Proof.

(a) ⇒ (b) Every proper ideal of R is be contained in $R \setminus R^\times$, so if this subset is an ideal then it is the unique maximal ideal.

(b) ⇒ (a) The unique maximal ideal contains every element of $R \setminus R^\times$ and must also be contained in $R \setminus R^\times$.

(b) ⇒ (c) This follows from 1.2.6.

(c) ⇒ (b) Let $\mathfrak{m}$ be some maximal ideal in R[6] and $x \in \mathfrak{m}$. By 1.2.6 again, $x \in \mathrm{Jac}(R)$; this shows that $\mathfrak{m} \subset \mathrm{Jac}(R) \subset \mathfrak{m}$, so that $\mathrm{Jac}(R) = \mathfrak{m}$ is the unique maximal ideal.

The last statement is clear. ■

Local rings are usually denoted by the writing down the triple $(R, \mathfrak{m}, k)$ where $\mathfrak{m} \subset R$ is the maximal ideal and $k := R/\mathfrak{m}$ is the *residue field*. Corollary 1.1.12(e) says that if R is any ring and $\mathfrak{p} \subset R$ a prime, then $(R_\mathfrak{p}, \mathfrak{p}R_\mathfrak{p}, \kappa(\mathfrak{p}) := \mathrm{Frac}(R/\mathfrak{p}))$ is a local ring, where the identification of the residue field is clear via a suitable universal property.

[6] This uses that R is nonzero.

Remark 1.2.8. Since every maximal ideal is prime, it follows for any ring R that $\mathrm{Nil}(R) \subset \mathrm{Jac}(R)$, but equality need not hold in general, as any local domain other than a field (e.g. $\mathbb{Z}_{(p)}$ or $k[x]_{(x)}$) shows.

One other notion we will have occasion to use is found in

Definition 1.2.9. A nonzero ring R is called *semilocal* if it has only finitely many maximal ideals.

In particular, any local ring is semilocal. An example of a non-local semilocal ring is a finite product of fields, e.g., $\mathbb{Q} \times \mathbb{Q}$. We shall meet more examples of semilocal rings in §1.3.

1.2.2 Minimal Primes and Prime Avoidance

Next up are a couple of other very useful geometrical results.

Lemma 1.2.10. Let R be a ring, and $\mathfrak{a} \subset R$ be a proper ideal. There is a minimal prime over $\mathfrak{a}$. In fact, if we fix a prime $\mathfrak{p}$ containing $\mathfrak{a}$, then there is a minimal prime over $\mathfrak{a}$ which is contained in $\mathfrak{p}$.

A prime of R minimal over $\mathfrak{a} = (0)$ is simply called a *minimal prime.* The above result shows, in particular, that any nonzero ring admits a minimal prime.

Proof. It suffices to show the latter result, since every proper ideal is contained in some maximal (and hence prime) ideal. Apply Zorn's Lemma to $\mathbb{V}(\mathfrak{a}) \cap \operatorname{Spec} R_{\mathfrak{p}}$ ordered by reverse inclusion: if $(\mathfrak{q}_\alpha)$ is a chain then $\mathfrak{q} := \bigcap_\alpha \mathfrak{q}_\alpha$ is also a prime containing $\mathfrak{a}$, as follows. If $xy \in \mathfrak{q}$ but $x, y \notin \mathfrak{q}$, then there are α, β such that $x \notin \mathfrak{q}_\alpha, y \notin \mathfrak{q}_\beta$; without loss of generality, if $\mathfrak{q}_\alpha \subset \mathfrak{q}_\beta$, then $y \notin \mathfrak{q}_\alpha$ and so $xy \in \mathfrak{q}_\alpha$ but $x, y \notin \mathfrak{q}_\alpha$, a contradiction to the primality of $\mathfrak{q}_\alpha$. ■

Remark 1.2.11. Geometrically, this lemma says that if $X = \mathbb{V}(\mathfrak{a}) \subset \operatorname{Spec} R$ is any closed subscheme of an affine scheme, then X contains an irreducible component. The second part says that if we fix any point in X, then there is an irreducible component of X containing this given point. We will see in 2.2.10(a) below that in the Noetherian setting there are only finitely many irreducible components.

One other easy application of the machinery developed so far is

Corollary 1.2.12. In any ring, every element of a minimal prime is a zero-divisor.

Proof. Let R be a ring and $\mathfrak{p} \subset R$ a minimal prime. It follows from 1.1.12 that the localization $R_{\mathfrak{p}}$ has only one prime, namely $\mathfrak{p}R_{\mathfrak{p}}$, and so by 1.2.2 we conclude that $\mathrm{Nil}(R_{\mathfrak{p}}) = \mathfrak{p}R_{\mathfrak{p}}$. In particular, if $x \in \mathfrak{p}$, then the class of x in $R_{\mathfrak{p}}$ is nilpotent, from which it follows that x is a zero-divisor. ■

We end our discussion of minimal primes with another result that is often useful.

Corollary 1.2.13.

(a) Let $R \subset S$ be a subring. Every minimal prime of R is contracted from S.

(b) If $\varphi : R \to S$ is a ring homomorphism, and $\mathfrak{p} \subset R$ a minimal prime that is contracted from S, then it is the contraction of a minimal prime of S.

In particular, if $R \subset S$ is a subring, then every minimal prime of R is the contraction of a minimal prime of S.

Proof.

(a) If $\mathfrak{p} \subset R$ is any prime, then $S_{\mathfrak{p}} \neq 0$ implies that there is a prime $\mathfrak{q} \subset S$ such that $\mathfrak{q} \cap R \subset \mathfrak{p}$.
(b) Let $\mathfrak{q} \subset S$ be such that $\varphi^{-1}(\mathfrak{q}) = \mathfrak{p}$. Using 1.2.10, pick a minimal $\mathfrak{q}' \subset S$ contained in $\mathfrak{q}$. Then also $\varphi^{-1}(\mathfrak{q}') = \mathfrak{p}$ by minimality of $\mathfrak{p}$.

■

The second useful geometric result is

Lemma 1.2.14 (Prime Avoidance)**.** Let R be a ring, n a positive integer, and $\mathfrak{a}_1, \dots, \mathfrak{a}_n \subset R$ ideals.

(a) If $\mathfrak{p} \subset R$ is a prime with $\prod_{i=1}^n \mathfrak{a}_i \subset \mathfrak{p}$, then there is an i with $1 \leq i \leq n$ such that $\mathfrak{a}_i \subset \mathfrak{p}$.
(b) If $\mathfrak{a} \subset R$ is an ideal with $\mathfrak{a} \subset \bigcup_{i=1}^n \mathfrak{a}_i$, and either R contains an infinite field or at most two of the $\mathfrak{a}_i$ are not prime, then there is an i with $1 \leq i \leq n$ such that $\mathfrak{a} \subset \mathfrak{a}_i$.

Stated equivalently, (b) reads that if $\mathfrak{a}_1, \dots, \mathfrak{a}_n \subset R$ are ideals such that either R contains an infinite field or at most two of the $\mathfrak{a}_i$ are not prime, then if $\mathfrak{a} \subset R$ is any ideal such that $\mathfrak{a} \not\subset \mathfrak{a}_i$ for all $i = 1, \dots, n$, then $\mathfrak{a} \not\subset \bigcup_{i=1}^n \mathfrak{a}_i$, i.e. there is an $x \in \mathfrak{a}$ such that $x \notin \mathfrak{a}_i$ for all $i = 1, \dots, n$.

Proof.

(a) Else, pick for each i an $a_i \in \mathfrak{a}_i \smallsetminus \mathfrak{p}$; then $\prod_i a_i \in \prod_i \mathfrak{a}_i \smallsetminus \mathfrak{p}$ using the primality of $\mathfrak{p}$.
(b) We leave the case of when R contains an infinite field to the reader (see 1.13). In the second case, induct on n. When $n = 2$, there is no restriction on the $\mathfrak{a}_i$; if the result is false, then pick $x_1 \in \mathfrak{a} \smallsetminus \mathfrak{a}_2 \subset \mathfrak{a}_1 \smallsetminus \mathfrak{a}_2$ and $x_2 \in \mathfrak{a} \smallsetminus \mathfrak{a}_1 \subset \mathfrak{a}_2 \smallsetminus \mathfrak{a}_1$. Then $x_1 + x_2 \in \mathfrak{a} \smallsetminus \mathfrak{a}_1 \cup \mathfrak{a}_2$, a contradiction. Suppose now that $n \geq 3$ and $\mathfrak{a}_3, \dots, \mathfrak{a}_n$ are prime. Inductively, we may assume that $\mathfrak{a}$ does not belong to unions of $(n-1)$'s of the $\mathfrak{a}_i$'s, i.e. that for each i there is an
$$x_i \in \mathfrak{a} \smallsetminus (\mathfrak{a}_1 \cup \cdots \cup \hat{\mathfrak{a}}_i \cup \cdots \cup \mathfrak{a}_n) \subset \mathfrak{a}_i \smallsetminus (\mathfrak{a}_1 \cup \cdots \cup \hat{\mathfrak{a}}_i \cup \cdots \cup \mathfrak{a}_n).$$
Then $x_1 \cdots x_{n-1} \subset \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_{n-1} \smallsetminus \mathfrak{a}_n$ by primality of $\mathfrak{a}_n$ whereas $x_n \in \mathfrak{a}_n \smallsetminus (\mathfrak{a}_1 \cup \cdots \cup \mathfrak{a}_{n-1})$, so if $x := x_1 \cdots x_{n-1} + x_n$, then $x \in \mathfrak{a} \smallsetminus \bigcup_i \mathfrak{a}_i$, a contradiction.

■

Remark 1.2.15. Usually, only the statement in (b) is called the Prime Avoidance Lemma. Geometrically, (a) says that if a point (or irreducible closed subscheme) of an affine scheme is contained in a finite union of closed subschemes, then it must be contained in one of them. Similarly, the statement in (b), or its contrapositive, can be stated geometrically in many ways; here are two:

(i) If finitely many points of an affine scheme are contained in an open subset, then there is a smaller principal open subset containing all of them.
(ii) If $X_1, \dots, X_n$ are irreducible closed subschemes of an affine scheme X and $f_1, \dots, f_m$ functions on X such that for any X_i there is an f_j such that f_j doesn't vanish identically on X_i, then there is some linear combination of the f_j's that doesn't vanish identically on any of the X_i's.

1.2.3 Krull Dimension

Let us end this section by introducing one final important notion.

Definition 1.2.16. Let R be a ring.

(a) The *Krull dimension* of R, denoted $\dim R$, is the supremum of the lengths of chains of primes in R, i.e., it is the supremum of the set of integers $n \geq 0$ such that there are primes $\mathfrak{p}_i \subset R$ for $i = 0, \ldots, n$ such that

$$\mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_n.$$

By convention, we set $\dim 0 := -1$.

(b) Let M be an R-module. Define the *Krull dimension* of M to be the dimension of $R/\operatorname{Ann} M$, i.e., $\dim M := \dim R/\operatorname{Ann} M$.

(c) Let $\mathfrak{p} \subset R$ be a prime. The *height of* $\mathfrak{p}$ is the supremum of lengths of chains of primes contained in $\mathfrak{p}$, i.e., $\operatorname{ht} \mathfrak{p} = \dim R_{\mathfrak{p}}$, and the *coheight* of $\mathfrak{p}$ is the supremum of lengths of chains of primes containing $\mathfrak{p}$, i.e., $\operatorname{coht} \mathfrak{p} := \dim R/\mathfrak{p}$.

Example 1.2.17.

(a) For a ring R, we have $\dim R = 0$ iff all primes of R are incomparable iff $\operatorname{Spec} R$ has the discrete topology (e.g., if R has only one prime). For a domain R, this happens iff R is a field.

(b) If $(R, \mathfrak{m}, k)$ is a local ring then $\operatorname{ht} \mathfrak{m} = \dim R$.

(c) If R is a ring and $S \subset R$ a multiplicative subset, then $\dim S^{-1}R \leq \dim R$.

(d) If R is a PID that is not a field, then $\dim R = 1$ and $\dim R[X] = 2$ (10.2.6).

(e) If k is a field, then $\dim k[X_1, \ldots, X_n] \geq n$ and $k[\![X_1, \ldots, X_n]\!] \geq n$. Also, $\dim k[X_1, X_2, \ldots] = \infty$. In fact, equality holds in the first two, but this will have to wait (6.2.8(b) and 2.4.3(b)).

(f) If R is a ring and $\mathfrak{p} \subset R$ a prime, then $\operatorname{ht} \mathfrak{p} + \operatorname{coht} \mathfrak{p} \leq \dim R$ and equality holds for most reasonable rings (e.g., coordinate rings of affine varieties, see 6.2.8(d)), but not always (10.6.2).

(g) In fact, if R is a Noetherian ring, then for any $n \in \mathbb{Z}_{\geq 1}$ we have $\dim R[X_1, \ldots, X_n] = \dim R + n$, although this is much harder to prove ([TOCITE]). In fact, this result is false in general for non-Noetherian R ([TOCITE]), which is one indication that the proof is hard.

We will have much to say about dimension throughout these notes: it is an idea we will keep revisiting.

1.3 Noetherian and Artinian Rings and Modules

In this section, we consider two fundamental finiteness properties on ring and modules–that of being Noetherian and Artinian. While these initially seem “dual” to each other, we will soon see that there is a huge difference between these two notions.

Proposition/Definition 1.3.1. Let R be a ring.

i. An R-module M is *Noetherian* if it satisfies the following equivalent properties:
   (a) The ascending chain condition (a.c.c.) on submodules of M: every increasing sequence $M_0 \subset M_1 \subset M_2 \subset \cdots$ of submodules of M eventually stabilizes.
   (b) Every nonempty collection of submodules of M contains a maximal element.
   (c) Every submodule of M is finitely generated.
   (d) Given any sequence a of elements $a_1, a_2, \dots$ in M, there is an integer $m_0 = m_0(a) \geq 1$ such that for each $m > m_0$, there are $f_{mn} \in R$ for $n = 1, \dots, m_0$ with $a_m = \sum_{n=1}^{m_0} f_{mn} a_n$.

   The ring R is *Noetherian* if it is Noetherian as a module over itself, or equivalently if every ideal in R is finitely generated.

ii. An R-module M is *Artinian* if it satisfies any one of the following equivalent properties:
   (a) The descending chain condition (d.c.c.) on submodules.
   (b) Every nonempty collection of submodules contains a minimal element.

   The ring R is *Artinian* if it is Artinian as a module over itself.

Example 1.3.2.

(a) If $R = k$ is a field, then an R-module M is Noetherian iff it is Artinian iff it has finite dimension.
(b) The $\mathbb{Z}$-module $\mathbb{Z}$ is Noetherian but not Artinian. For any prime p, the $\mathbb{Z}$-module $\mathbb{Z}[1/p]/\mathbb{Z}$ is Artinian but not Noetherian (see 1.16).
(c) Finite rings, finite products of fields, and finite-dimensional algebras over fields (for instance, the rings $k[X_1, \dots, X_n]/(X_1, \dots, X_n)^m$ for $n, m \geq 1$) are both Noetherian and Artinian.[7]
(d) The rings $\mathbb{Z}, \mathcal{O}_K$ and $k[X_1, \dots, X_n]$ for fields k are Noetherian but not Artinian.
(e) Given any ring R, the polynomial ring $R[X_1, X_2, \dots]$ over R in countably many variables is not Noetherian (nor Artinian[8].)

Observation 1.3.3. Let R be a ring and M an R-module.

(a) Let $M' \subset M$ be a submodule. If $N \subset N' \subset M$ are submodules such that $N \cap M' = N' \cap M'$ and $(N + M')/M' = (N' + M')/M'$, then $N = N'$.
(b) If $0 \to M' \to M \to M'' \to 0$ is a short exact sequence of R-modules, then M is Noetherian (resp. Artinian) iff both M' and M'' are.
(c) If M is Noetherian (resp. Artinian), then so is $M^{\oplus n}$ for each $n \geq 1$.
(d) If R is Noetherian (resp. Artinian) and M a finitely generated R-module, then M is Noetherian (resp. Artinian).

Let’s start with one criterion relating length to the conditions of being Noetherian or Artinian.

Lemma 1.3.4. A module has finite length iff it is both Noetherian and Artinian.

[7] The phrase “both Noetherian and Artinian” is redundant for rings, where the apparent symmetry between the definitions of the two conditions is misleading. See 1.3.10.

[8] See previous footnote.

Proof. Let M be an R-module. If $\ell_R(M) < \infty$, then for all submodules $0 \subset N \subsetneq N' \subset M$ we have

$$0 \leq \ell_R(N) < \ell_R(N') \leq \ell_R(M),$$

so that M satisfies both the a.c.c. and the d.c.c. on submodules. If M is Noetherian, then 10.1.2 allows us to produce a series of submodules

$$M = M_0 \supsetneq M_1 \supsetneq M_2 \supsetneq \cdots$$

with simple successive quotients. If M is also Artinian, this series must eventually terminate. ■

1.3.1 Noetherian Rings

Next up are some standard results on (identifying) Noetherian rings.

Theorem 1.3.5 (Generalized Hilbert Basis Theorem)**.** If R is Noetherian, then so are $R[X]$ and $R[\![X]\!]$.

Proof. Let $\mathfrak{a} \subset R[X]$ be an ideal. For each $m \geq 0$, let $\mathfrak{a}_m \subset R$ be the ideal consisting of leading coefficients of polynomials in $\mathfrak{a}$ of degree m. Since R is Noetherian, each $\mathfrak{a}_m$ is finitely generated and we may find an $m_0 \geq 1$ such that $\mathfrak{a}_{m_0} = \mathfrak{a}_{m_0+1} = \cdots$. For each $0 \leq m \leq m_0$, let a_{mn} be finitely many generators of $\mathfrak{a}_m$, and pick polynomials $f_{mn} \in \mathfrak{a}$ of degree m with these leading coefficients. We claim that (f_{mn}) generate $\mathfrak{a}$. To show this, we proceed by induction on the degree of $f \in \mathfrak{a}$ to show that $f \in (f_{mn})$, with the case of negative degree (i.e. zero) being trivial. Hence suppose that $\deg f = d \geq 0$, and let a be the leading coefficient of f. If $d \leq m_0$, then we can write $a = \sum_n c_n a_{dn}$ for some $c_n \in R$, and then $f - \sum_n c_n f_{dn} \in \mathfrak{a}$ has degree less than d. If $d \geq m_0 + 1$, then $a = \sum_n c_n a_{m_0 n}$ for some $c_n \in R$, and then $f - \sum_n c_n X^{d-m_0} f_{m_0 n} \in \mathfrak{a}$ has degree less than d.

The proof for $R[\![X]\!]$ is similar. Let $\mathfrak{a} \subset R[\![X]\!]$, and for each $m \geq 0$, let $\mathfrak{a}_m \subset R$ be the ideal of leading cofficients of power series in $\mathfrak{a} \cap (X^m)$. Then let m_0, a_{mn} and $f_{mn} \in \mathfrak{a}$ be as before; again, we claim that the (f_{mn}) generate $\mathfrak{a}$. Given an $f \in \mathfrak{a}$, take an R-linear combination f_0 of the f_{0n} so that $f - f_0 \in \mathfrak{a} \cap (X)$. Then take an R-linear combination f_1 of the f_{1n} so that $f - f_0 - f_1 \in \mathfrak{a} \cap (X^2)$. Continue to produce $f_2, \ldots, f_{m_0}$ so that $f - f_0 - f_1 - \cdots - f_{m_0} \in \mathfrak{a} \cap (X^{m_0+1}b)$. Now since $\mathfrak{a}_{m_0} = \mathfrak{a}_{m_0+1}$, take a linear combination f_{m_0+1} of the $Xf_{m_0 n}$ so $f - f_0 - f_1 - \cdots - f_{m_0} - f_{m_0+1} \in \mathfrak{a} \cap (X^{m_0+2})$. Similarly, produce $f_{m_0+2}, f_{m_0+3}, \ldots$. For each $m \geq m_0$, write $f_m = \sum_n a_{mn} X^{m-m_0} f_{m_0 n}$ and for each n, let $g_n = \sum_{m=m_0}^{\infty} a_{mn} X^{m-m_0} \in R[\![X]\!]$. Then $f = f_0 + \cdots + f_{m_0-1} + \sum_n g_n f_{m_0 n}$. ■

Theorem 1.3.6 (Cohen)**.** Let R be a ring. Any ideal of R which is maximal (with respect to inclusion) in the collection of ideals of R which are not finitely generated is prime. In particular, if all prime ideals of R are finitely generated, then R is Noetherian.

Proof. Let $\mathfrak{a}$ be this maximal element. If $\mathfrak{a}$ is not prime, then there are $x, y \in R$ such that $x, y \notin \mathfrak{a}$ but $xy \in \mathfrak{a}$. By maximality, $\mathfrak{a}+(x)$ and $(\mathfrak{a} : x) \supset \mathfrak{a}+(y)$ are finitely generated, so pick generators $u_1, \ldots, u_n, x$ of $\mathfrak{a}+(x)$ with $u_j \in \mathfrak{a}$ and $v_1, \ldots, v_m$ of $(\mathfrak{a} : x)$. Then $\mathfrak{a} = (u_1, \ldots, u_n, v_1 x, \ldots, v_m x)$, which is a contradiction. ■

Theorem 1.3.7. Let R be a ring and M an R-module. If M is Noetherian (resp. finitely generated Artinian), then $R/\operatorname{Ann}(M)$ is a Noetherian (resp. Artinian) ring. In particular, if R admits a faithful Noetherian module, then it is Noetherian.

Proof. The submodules of M as an R-module and $R/\operatorname{Ann} M$-module coincide, so we may reduce to the case $\operatorname{Ann} M = 0$, i.e. when M is faithful. If M is generated by $x_1, \dots, x_n$, then the map $R \to M^{\oplus n}$ given by $[r] \mapsto (rx_1, \dots, rx_n)$ is injective; now apply 1.3.3(b). ■

Theorem 1.3.8 (Eakin-Nagata-Formanek)**.** Let R be a ring.

(a) Let M be a finitely generated faithful R-module. If the set of submodules of M of the form $\mathfrak{a}M$ for ideals $\mathfrak{a} \subset R$ satisfies the ascending chain condition, then R is Noetherian.
(b) Let $R \subset S$ be a ring extension. If S is Noetherian and a finitely generated R-module, then R is Noetherian.

Proof. For (b), take $M = S$ in (a). To show (a), by 1.3.7, it suffices to show that M is a Noetherian R-module. Suppose not, so that the collection

$$\mathscr{A} := \{\mathfrak{a}M : \mathfrak{a} \subset R \text{ ideal and } M/\mathfrak{a}M \text{ is not Noetherian}\}$$

is nonempty. By assumption, this collection has a maximal element, say $\mathfrak{a}M$. Replacing M by $M/\mathfrak{a}M$ and R by $R/\operatorname{Ann}(M/\mathfrak{a}M)$, we can assume that M is non-Noetherian but for any nonzero ideal $\mathfrak{a} \subset R$, the quotient $M/\mathfrak{a}M$ is Noetherian. Now let

$$\mathscr{B} := \{N \subset M : M/N \text{ is a faithful } R\text{-module}\}.$$

If M is generated by $x_1, \dots, x_n$, then a submodule $N \subset M$ is in B iff for all $r \in R \smallsetminus \{0\}$ we have $\{rx_1, \dots, rx_n\} \not\subset N$. Therefore, Zorn's Lemma applies to $\mathscr{B}$ and produces a maximal element $N_0 \in \mathscr{B}$. If M/N_0 is Noetherian, then by 1.3.7 the ring R is Noetherian and hence so is M, which is a contradiction. Therefore, replacing M by M/N_0 gives us an R-module M with the following three properties:

(i) M is not a Noetherian R-module.
(ii) For any nonzero ideal $\mathfrak{a} \subset R$, the quotient $M/\mathfrak{a}M$ is Noetherian.
(iii) For any nonzero submodule $N \subset M$, the quotient M/N is not a faithful R-module.

Let $N \subset M$ be any nonzero submodule. By (iii), there is a nonzero $r \in R$ such that $rM \subset N$. By (ii), the quotient M/rM is Noetherian, so that the submodule $N/rM \subset M/rM$ is finitely generated. Since M and hence rM is finitely generated as well, it follows that N is finitely generated. Since this is true for every $N \subset M$, it follows that M is Noetherian, contradicting (i).

■

1.3.2 Artinian Rings

We end this section with a closer examination of Artinian rings.

Theorem 1.3.9. Let R be an Artinian ring.

(a) If R is a domain or a reduced local ring, then R is a field.
(b) Every prime ideal of R is maximal (i.e., $\dim R = 0$).
(c) The radical $\operatorname{Nil}(R) = \operatorname{Jac}(R)$ is nilpotent.
(d) R is semilocal.
(e) R is a finite direct product of Artinian local rings.

Proof.

(a) Given a nonzero $a \in R$, applying the d.c.c. to $(a) \supset (a^2) \supset \cdots$ gives us an integer $k \geq 1$ such that $(a^k) = (a^{k+1})$. By 1.17 applied to the case where R is a domain or a local ring, there is a unit $u \in R^\times$ such that $a^{k+1} = ua^k$, i.e., $a^k(a-u) = 0$. If R is a domain, then this implies that $a = u$, so we are done. If R is a local ring and $a \notin R^\times$, then $u \in R^\times$ implies that $a - u \in R^\times$ (1.2.6 and 1.2.7), and so $a^k = 0$. If R is also reduced, it follows that $a = 0$, which is a contradiction. Therefore, we must have $a \in R^\times$.

(b) If $\mathfrak{p} \subset R$ is a prime ideal, then $R/\mathfrak{p}$ is an Artinian domain, so we are done by (a).

(c) Let $\mathfrak{n} = \mathrm{Nil}(R) = \mathrm{Jac}(R)$. By the d.c.c. applied to $\mathfrak{n} \supset \mathfrak{n}^2 \supset \cdots$, there is a $k \geq 1$ such that $\mathfrak{n}^k = \mathfrak{n}^{k+1} = \cdots$. If $\mathfrak{n}^k \neq 0$, then the family of ideals $\mathscr{A} = \{\mathfrak{a} \subset R : \mathfrak{a}\mathfrak{n}^k \neq 0\}$ is nonempty since $\mathfrak{n} \in \mathscr{A}$. Since R is Artinian, $\mathscr{A}$ contains a minimal element, say $\mathfrak{a}$. Now $\mathfrak{a}\mathfrak{n}^k \neq 0$, so there is an $r \in \mathfrak{a}$ such that $r \cdot \mathfrak{n}^k \neq 0$; then by minimality $\mathfrak{a} = (r)$. But now $r \cdot \mathfrak{n} \subset (r)$ is such that $r \cdot \mathfrak{n} \cdot \mathfrak{n}^k = r \cdot \mathfrak{n}^k \neq 0$, so that by minimality $r \cdot \mathfrak{n} = (r)$. Therefore, $r = rs$ for some $s \in \mathfrak{n}$, so that $r = rs^n$ for all $n \geq 1$. But $s \in \mathfrak{n} = \mathrm{Nil}(R)$, so this means $r = 0$, contrary to hypothesis. Therefore, $\mathfrak{n}^k = 0$.

(d) Consider the collection of all finite intersections of maximal ideals of R, which is nonempty as soon as R is not the zero ring. Since R is Artinian, this has a minimal element, say $\bigcap_{i=1}^n \mathfrak{m}_i$. We claim that $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ are all the maximal ideals of R. Indeed, if $\mathfrak{m} \subset R$ is any other maximal ideal, then minimality gives us $\bigcap_{i=1}^n \mathfrak{m}_i = \mathfrak{m} \cap \bigcap_{i=1}^n \mathfrak{m}_i \subset \mathfrak{m}$, so by 1.2.14(a) there is an i such that $\mathfrak{m}_i \subset \mathfrak{m}$, whence $\mathfrak{m}_i = \mathfrak{m}$ by maximality.

(e) By (c) and (d), there is a $k \geq 1$ such that $\mathfrak{n}^k = 0$ where $\mathfrak{n} = \bigcap_{i=1}^n \mathfrak{m}_i = \prod_{i=1}^n \mathfrak{m}_i$. Since the $\{\mathfrak{m}_i^k\}_i$ are pairwise comaximal, the Chinese Remainder Theorem gives us that

$$R = R/\prod_{i=1}^n \mathfrak{m}_i^k \cong \prod_{i=1}^n R/\mathfrak{m}_i^k.$$

Each quotient $R/\mathfrak{m}_i^k$ is Artinian (because it is a quotient of R), and local (thanks to 1.14).

■

This result shows that Artinian local rings are nonreduced analogs of fields. The key asymmetry between the two notions is manifest in

Theorem 1.3.10 (Akizuki-Hopkins)**.** An Artinian ring is Noetherian.

Proof 1 of 1.3.10. Let R be an Artinian ring. We will show that if M is an Artinian R-module, then M is finitely generated; this suffices, since every ideal of R is an Artinian R-module by 1.3.3(b). If M is not finitely generated, then the family $\mathscr{A}$ of submodules of M that are not finitely generated is nonempty, so we may choose a minimal element M_0; replacing M by M_0 we can assume that every proper submodule of M is finitely generated. We claim that $\mathfrak{p} = \mathrm{Ann}(M)$ is a prime of R: pick $a, b \in R$ such that $ab \in \mathfrak{p}$ but $a \notin \mathfrak{p}$. Then $M[a] := (0 :_M a) \subsetneq M$, so it is finitely generated. From the short exact sequence

$$0 \to M[a] \to M \xrightarrow{\cdot a} aM \to 0$$

we see that aM is not finitely generated, so that $aM = M$. Then $0 = b(aM) = bM$ implies $b \in \mathfrak{p}$. But now $R/\mathfrak{p}$ is a field, and M is an Artinian $R/\mathfrak{p}$ module that is not finitely generated–a contradiction. ■

Proof 2 of 1.3.10. We will show that a ring R is Artinian iff $\ell_R(R) < \infty$. The "if" direction, as well as the result of the theorem, follow then from 1.3.4. By (the proof of) 1.3.9(e), there are maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_N \subset R$, not necessarily distinct, with $\prod_{i=1}^N \mathfrak{m}_i = 0$. Consider the chain $R \supset \mathfrak{m}_1 \supset \mathfrak{m}_1\mathfrak{m}_2 \supset \cdots \supset \mathfrak{m}_1 \cdots \mathfrak{m}_N = 0$, and consider the subquotients $Q_i := \mathfrak{m}_1 \cdots \mathfrak{m}_{i-1}/\mathfrak{m}_1 \cdots \mathfrak{m}_i$. Each Q_i is an Artinian R-module, and so an Artinian $k_i := R/\mathfrak{m}_i$-module, hence a Noetherian k_i-module (1.3.2(a)), and hence a Noetherian R-module. It follows then from 1.3.4 that each $\ell_R(Q_i) < \infty$. From the additivity of length (10.1.6), we conclude that

$$\ell_R(R) = \sum_{i=1}^{N} \ell_R(Q_i) < \infty.$$

■

We shall prove later (§2.3) that a Noetherian ring of dimension zero is Artinian.

1.4 Unique Factorization I

In this section we study unique factorization of elements into irreducibles in domains.

Definition 1.4.1. A domain R is said to be *atomic* if every nonzero nonunit of R can be written as a finite product of irreducible elements.

If a domain R satisfies the ascending chain condition on principal ideals (e.g., if R is Noetherian), then R is atomic, although the converse does not hold (see [1]). We will need

Definition 1.4.2. Let R be a ring, and $x, y \in R$ elements.

(a) An element $\ell \in R$ is said to be a *least common multiple* (lcm) of x and y if $x, y \mid \ell$ and if $\ell' \in R$ is any other element such that $x, y \mid \ell'$, then $\ell \mid \ell'$.
(b) An element $g \in R$ is said to be a *greatest common divisor* (gcd) of x and y if $g \mid x, y$ and if $g' \in R$ is any other element such that $g' \mid x, y$, then $g' \mid g$.

By 1.17, lcms and gcds are unique in strongly associate rings when they exist.

Theorem/Definition 1.4.3 (Unique Factorization Domains)**.** The following conditions on an atomic (e.g., Noetherian) domain are equivalent:

(a) The factorization of any nonzero element into irreducibles is unique up to reordering of factors and multiplication by units.
(b) Every irreducible element is prime.
(c) The intersection of an arbitrary collection of principal ideals is principal.
(d) The intersection of any two principal ideals is principal.
(e) Any two elements have a lcm.
(f) Any two elements have a gcd.
(g) Any minimal nonzero prime (i.e., prime of height one) is principal.

An atomic domain satisfying these conditions is said to be a *unique factorization domain* (UFD).

In an atomic domain, we are allowed to take lcms and gcds of finitely many elements (check this is well-defined!).

Proof. The implications (c) $\Rightarrow$ (d) $\Rightarrow$ (e) are clear.

(a) $\Leftrightarrow$ (b) Standard and left to the reader (see 1.20).

(a) $\Rightarrow$ (c) Factoring each $x_i = u_i \prod_\alpha p_\alpha^{v_{\alpha,i}}$ with $u_i \in R^\times$ and p_α distinct primes gives $\bigcap_i (x_i) = \left(\prod_\alpha p_\alpha^{\max_i v_{\alpha,i}}\right)$, where the intersection is zero iff $\max_i v_{\alpha,i}$ does not exist (i.e. is ∞) for some α.

(e) $\Rightarrow$ (f) More generally, if R is any domain and $x, y \in R$ elements which have a lcm ℓ, then x and y have a gcd g. Indeed, if $(x) \cap (y) = (\ell)$, then there is a $g \in R$ with $xy = zg$; check that g is a gcd of x and y.

(f) $\Rightarrow$ (b) Let p be an irreducible element, and suppose $x, y \in R$ are such that $p \mid xy$ but $p \nmid y$. By irreducibility of p, it is easy to see (check!) that $\gcd(x, p) = 1$ and now $p \mid \gcd(xy, py) = \gcd(x, p)y = y$.

(b) $\Rightarrow$ (g) Let $\mathfrak{p}$ be a minimal nonzero prime, and let $0 \neq f \in \mathfrak{p}$. Factor f into irreducibles and use the primality of $\mathfrak{p}$ to conclude that $\mathfrak{p}$ contains an irreducible element. Conclude from (b) using the minimality of $\mathfrak{p}$ that $\mathfrak{p}$ is principal.

(g) $\Rightarrow$ (b) This is harder. Let p be an irreducible element, and let $\mathfrak{p}$ be a minimal prime over (p) (1.2.10). By 2.4.4, $\mathfrak{p}$ has height one and hence is principal by hypothesis; say $\mathfrak{p} = (q)$ for some prime $q \in R$. Now $p = qr$ for some $r \in R$, so by irreducibility of p and primality of q we conclude that r is a unit, whence $\mathfrak{p} = (p)$.

■

Corollary 1.4.4. A PID is a UFD.

Proof. A PID is Noetherian and hence atomic; we are done by 1.4.3(c), say. ■

Corollary 1.4.5 (Nagata)**.** Let R be a domain and $S \subset R$ multiplicative. Consider the statements:

(a) The ring R is a UFD.
(b) The localization $S^{-1}R$ is a UFD.

Then (a) $\Rightarrow$ (b), and (b) $\Rightarrow$ (a) if R satisfies the ascending chain condition on principal ideals (e.g., if R is Noetherian) and S is generated by a set of prime elements.

Proof. The implication (a) $\Rightarrow$ (b) is clear; for (b) $\Rightarrow$ (a) under the given hypotheses, we use 1.4.3(g). Let Γ be a generating set for S and $\mathfrak{p} \subset R$ be a prime of height one. If $\mathfrak{p} \cap S \neq \emptyset$, then $\mathfrak{p}$ contains a $p \in \Gamma$, and then $\mathfrak{p} = (p)$ by minimality. Else $S^{-1}\mathfrak{p} \subset S^{-1}R$ is a prime of height one, so by hypothesis we have $S^{-1}\mathfrak{p} = xS^{-1}R$ for some $x \in \mathfrak{p}$. Look at the collection of ideals $\{(x)\}$ that arise in this way; by Zorn's lemma and the hypothesis on R, this has a maximal element (p). By maximality, p is not divisible by any $q \in S$. If $x \in \mathfrak{p}$, then $sx = py$ for some $s \in S$ and $y \in R$. If $s = q_1 \cdots q_N$ with $q_j \in \Gamma$, then $p \notin (q_j)$ implies $y \in (q_j)$ for each j. By induction on N, it follows that $y \in (s)$, and so $x \in (p)$. Thus $\mathfrak{p} \subset (p)$ as needed. ■

Let us now look at some important classes of examples of UFDs. The first of these comes from PIDs, which often arise as Euclidean domains.

Definition 1.4.6. A domain R is said to be *Euclidean* if there is some function $d : R \smallsetminus \{0\} \to \mathbb{Z}_{>0}$ such that for all $a, b \in R$ with $b \neq 0$, there are $q, r \in R$ such that

$$a = bq + r$$

and either $r = 0$ or $d(r) < d(b)$.

The function d, called the *Euclidean function*, is not part of the definition, only the existence of such a d is; in general, a Euclidean domain admits many different Euclidean functions. Briefly, a Euclidean domain is a domain in which you can perform Euclid's algorithm.

Example 1.4.7.

(a) For $R = K$ a field, the function $d \equiv 1$ is Euclidean.
(b) For $R = \mathbb{Z}$, the function $d(n) = |n|$ is Euclidean.
(c) For $R = \mathbb{Z}[\mathrm{i}]$ or $R = \mathbb{Z}[\omega]$, the norm function $d(\alpha) = \mathrm{N}(\alpha)$ is Euclidean.
(d) For $R = K[X]$, the polynomial ring over the field K, the function $d(f) = \deg f$ is Euclidean.
(e) For $R = K[\![X]\!]$, the $d(f) = \mathrm{ord}_X f$ taking a power series to the highest power of X dividing it is Euclidean.

Corollary 1.4.8. A Euclidean domain is a PID and hence a UFD.

This is standard, so we only indicate a sketch, and that too only of the UFD part. For details and a slightly different argument, see [2]. Proofs of this result can also be found in any algebra textbook.

Proof. If R is Euclidean and d a Euclidean function, then the function $\tilde{d} : R \smallsetminus \{0\} \to \mathbb{Z}_{>0}$ defined by $\tilde{d}(x) = \min_{y \neq 0} d(xy)$ is also Euclidean with the additional property that $\tilde{d}(x) \mid \tilde{d}(y)$ if $x \mid y$;

replace d by $\tilde{d}$ to assume this property. Show that if $x, y \in R \setminus \{0\}$, then $d(x) \leq d(xy)$ with equality iff y is a unit, and use this (and the well-ordering principle) to show that R satisfies the ascending chain condition on principal ideals, and is hence atomic. Finally, perform Euclid's algorithm to find the greatest common divisor of any two elements and use 1.4.3(f). ■

Remark 1.4.9. Note that there are PIDs which are not Euclidean. Two standard examples are $R = \mathbb{Z}[(1+\sqrt{-19})/2]$ and $R = \mathbb{R}[X,Y]/(X^2+Y^2+1)$; see [2] for proofs of these claims.

We end by relating the unique factorization in a domain R to that in polynomial rings over it.

Corollary 1.4.10. Let R be a ring. The following are equivalent:

(a) R is a UFD.
(b) $R[X]$ is a UFD.
(c) $R[X_1, \ldots, X_n]$ is UFD for any $n \geq 1$.
(d) $R[X_\lambda]_{\lambda\in\Lambda}$ is a UFD for any Λ.
(e) $R[X_\lambda]_{\lambda\in\Lambda}$ is a UFD for some Λ.

The implication (a) ⇒ (b) is key in the above; the rest follow formally, as explained below. The standard proof of (a) ⇒ (b) using Gauss's Lemma can be found in §10.2. Another proof is given in 1.20. Here we give a third proof, under the additional assumption that $R[X]$ satisfies the ascending chain condition on principal ideals (e.g., when R is Noetherian, using 1.3.5).

Proof of Special Case. In what follows, let $K := \operatorname{Frac} R$ be the fraction field of R.

(a) ⇒ (b) If $S \subset R[X]$ is the set of all non-units in R, then S is a multiplicative subset generated by primes in R, which are primes in $R[X]$ by 1.19. Since the localization $S^{-1}R[X] = K[X]$ is a PID and hence UFD (1.4.7(d) and 1.4.8), we are done by 1.4.5.

(b) ⇒ (c) Follows from the previous implication by induction.

(c) ⇒ (d) Any element of $R[X_\lambda]_{\lambda\in\Lambda}$ belongs to $R[X_\lambda]_{\lambda\in\Lambda'}$ for some finite $\Lambda' \subset \Lambda$; in particular, any nonzero nonunit in the former admits a factorization into primes in this finite polynomial ring. Since these elements are still prime in $R[X_\lambda]_{\lambda\in\Lambda}$ (1.19(b)), we are done by 1.20(b).

(d) ⇒ (e) Clear.

(e) ⇒ (a) Note that $R \subset R[X_\lambda]_{\lambda\in\Lambda}$, so if the latter is domain, so is the former. Any nonzero nonunit in R can be factored uniquely into primes in the latter, but this factorization cannot have any elements of positive degree (thanks to 1.19(a)). Since primes of $R[X_\lambda]_{\lambda\in\Lambda}$ that lie in R are primes of R (1.19(b)), we are done by 1.20(b).

■

It is not true in general that if R is a UFD, then so is $R[\![X]\!]$; see 10.6.1. However, if R is a *regular* UFD, then so is $R[\![X]\!]$ (9.1.2), so that, in particular, rings such as $\mathbb{Z}[\![X_1, \ldots, X_n]\!]$ and $k[\![X_1, \ldots, X_n]\!]$ (where k denotes a field) are UFDs. We will have much to say about unique factorization at the end of the course.

1.5 Cayley-Hamilton Theorem, Nakayama's Lemma, and Krull's Intersection Theorem

In this section we discuss the circle of ideas behind the Cayley-Hamilton Theorem and Nakayama's Lemma. Using this, we give some delicious applications, including but not limited to Krull's Intersection Theorem. These fundamental results will be used repeatedly throughout the notes.

Theorem 1.5.1 (Cayley-Hamilton)**.** Let R be a ring, M be a finitely generated R-module, $\mathfrak{a} \subset R$ an ideal, and $\varphi \in \operatorname{End}_R(M)$ such that $\varphi M \subset \mathfrak{a}M$. Then there is an $n \in \mathbb{Z}_{\geq 1}$ and $a_1, \ldots, a_n \in R$ such that for all i, we have $a_i \in \mathfrak{a}^i$, and further φ satisfies an equation of the form

$$\varphi^n + a_1\varphi^{n-1} + \cdots + a_n = 0$$

in $\operatorname{End}_R(M)$.

Proof. Write $M = \sum_{i=1}^n Rx_i$ for some $n \in \mathbb{Z}_{\geq 1}$ and let $\varphi(x_j) = \sum_{i=1}^n a_{ij}x_i$ for some $a_{ij} \in \mathfrak{a}$. Consider the matrix $A := [a_{ij}]$. Multiplying on the left by the adjoint of the matrix $\varphi I_n - A \in \operatorname{Mat}_n(R[\varphi])$ shows that $\det(\varphi I_n - A)x_i = 0$ for all i. Expanding yields and equation of the required form. ■

Corollary 1.5.2. Let $R \subset S$ be a ring extension and M a finitely generated R-module. Suppose for some $s \in S$ we have that M is also a faithful $R[s]$-module compatibly with the R-module structure, and suppose that $\mathfrak{a} \subset R$ is an ideal with $sM \subset \mathfrak{a}M$. Then there is an $n \in \mathbb{Z}_{\geq 1}$ and $a_1, \ldots, a_n \in R$ such that for all i, we have $a_i \in \mathfrak{a}^i$ and such that in S we have the identity $s^n + a_1s^{n-1} + \cdots + a_n = 0$.

Proof. Apply 1.5.1, and finish by using $\operatorname{Ann}_{R[s]} M = 0$. ■

Corollary 1.5.3 (Nakayama's Lemma)**.** Let R be a ring.

(a) If M is an R-module and $\mathfrak{a} \subset R$ an ideal with $M = \mathfrak{a}M$, then there is an $a \in \mathfrak{a}$ with $(1 + a)M = 0$.
(b) Let M be a finitely generated R-module and $\mathfrak{a} \subset \operatorname{Jac}(R)$ with $M = \mathfrak{a}M$. Then $M = 0$.
(c) Let M be an R-module, and $N \subset M$ a submodule such that M/N is finitely generated. If for some $\mathfrak{a} \subset \operatorname{Jac}(R)$ we have $M = N + \mathfrak{a}M$, then $M = N$.

Proof. For (a), apply 1.5.1 to $\varphi = 1$. For (b), apply (a) and use 1.2.6.[9] For (c), apply (b) to M/N. ■

Nakayama's lemma is immensely useful and will be used repeatedly.

Corollary 1.5.4. Let $(R, \mathfrak{m}, k)$ be a local ring and M a finitely generated R-module.

(a) Given $x_1, \ldots, x_n \in M$, the set $\{x_1, \ldots, x_n\}$ generates M over R iff $\{\overline{x}_1, \ldots, \overline{x}_n\}$ spans $M/\mathfrak{m}M$ over k. In particular, $M/\mathfrak{m}M$ is a finite-dimensional vector space over k.
(b) In the situation of (a), the former is a minimal set of generators of M over R iff the latter is a k-basis of $M/\mathfrak{m}M$. In particular, any two minimal sets of generators for M over R have the same size, namely $\dim_k(M/\mathfrak{m}M)$.
(c) If $\mathfrak{m} \neq 0$ is finitely generated, then $\mathfrak{m}$ is principal iff $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 1$.

When $\mathfrak{m}$ is finitely generated, the quantity $\dim_k \mathfrak{m}/\mathfrak{m}^2$ is known as the *embedding dimension* of the local ring R, and is denoted by $\operatorname{edim} R$.

[9] Here's an alternative proof: if $M \neq 0$, then use 10.1.2 to produce a surjection $\varphi : M \to R/\mathfrak{m}$ for some maximal ideal $\mathfrak{m} \subset R$. Since $\mathfrak{a} \subset \mathfrak{m}$, we must have $\mathfrak{a}M \subset \mathfrak{m}M \subset \ker\varphi \subsetneq M$, a contradiction to hypothesis.

Proof.

(a) If $x_1, \dots, x_n \in M$ generate M over R, then the images certainly span $M/\mathfrak{m}M$ over k. Conversely, suppose $x_1, \dots, x_n \in M$ are such that $\{\overline{x}_1, \dots, \overline{x}_n\}$ is a k-basis for $M/\mathfrak{m}M$. Let $N := \sum_{i=1}^n Rx_i \subset M$; by 1.5.3(c), we conclude that $M = N$, so M is generated by the x_i.

(b) If $\{x_1, \dots, x_n\}$ is not a minimal set of generators, then some proper subset of it generates M and hence also the images of these span $M/\mathfrak{m}M$. Similarly, if there is a proper subset of $\{x_1, \dots, x_n\}$ whose images form a basis of $M/\mathfrak{m}M$, then applying the previous implication would show that this proper subset would be a set of generators for M.

(c) Take $M = \mathfrak{m}$ in (b).

■

Before moving on, let us note one easy consequence of the definition we will use in the future.

Observation 1.5.5. Let $(R, \mathfrak{m})$ be a local ring with $\mathfrak{m}$ finitely generated. If $x \in \mathfrak{m}$, then $\operatorname{edim} R/(x)$ is either $\operatorname{edim} R$ or $\operatorname{edim} R - 1$ depending on whether or not $x \in \mathfrak{m}^2$ respectively.

Let us end this section with a few miscellaneous consequences.

Corollary 1.5.6 (Krull Intersection Theorem)**.** Let R be a ring, $\mathfrak{a} \subset R$ be an ideal, and $K_\mathfrak{a} := \bigcap_{N \geq 0} \mathfrak{a}^N$. If R is Noetherian, then $K_\mathfrak{a} = \mathfrak{a}K_\mathfrak{a}$. If, in addition, $1 + a$ is not a zero divisor for any $a \in \mathfrak{a}$ (e.g., if $\mathfrak{a} \subset \operatorname{Jac}(R)$ or if R is a domain and $\mathfrak{a} \subset R$ a proper ideal), then $K_\mathfrak{a} = 0$.

The ideal $K_\mathfrak{a}$ is the kernel of the completion map $R \to \hat{R}_\mathfrak{a}$ (see §1.6.2), so that if $K_\mathfrak{a} = 0$ then R embeds into its $\mathfrak{a}$-adic completion. This result gives us conditions for when this happens; for instance, this always happens for a Noetherian local ring R with maximal ideal $\mathfrak{a} = \mathfrak{m}$.

Proof 1. ([3]) The second statement follows immediately from the first and 1.5.3(a). For the first statement, let $\mathfrak{a} = (a_1, \dots, a_n)$ and let $b \in K_\mathfrak{a}$. For each $N \geq 1$, there is a polynomial $p_N \in R[X_1, \dots, X_n]$ such that p_N is homogeneous of degree N and $b = p_N(a_1, \dots, a_n) =: p_N(a)$. Since the ring $R[X_1, \dots, X_n]$ is Noetherian (1.3.5), there is an integer $N \geq 1$ and polynomials $q_1, \dots, q_N \in R[X_1, \dots, X_n]$ such that each q_j is homogeneous of degree j and $p_{N+1} = q_N p_1 + \cdots + q_1 p_N$. Then

$$b = p_{N+1}(a) = (q_N(a) + \cdots + q_1(a))\, b \in \mathfrak{a}K_\mathfrak{a}.$$

■

Proof 2. Take $M = R$ and $N = K_\mathfrak{a}$ in the Artin-Rees Lemma 1.6.20(b) below. ■

The hypothesis on $\mathfrak{a}$ in the second half of the statement cannot be easily strengthened: if $R = \mathbb{Q} \times \mathbb{Q}$ and $\mathfrak{a} = \mathbb{Q} \times 0$, then R is Noetherian (1.3.2(c)) but $\mathfrak{a}^2 = \mathfrak{a}$ and so $K_\mathfrak{a} = \mathfrak{a} \neq 0$, and there is a non-Noetherian domain with a proper ideal $\mathfrak{a} \subset R$ such that $K_\mathfrak{a} \neq 0$ (10.6.4).

Corollary 1.5.7. Every surjective endomorphism of a finitely generated module is an isomorphism.

Proof. Specifying an endomorphism φ of an R-module M is the same as specifying a $R[X]$-module structure lifting the R-module structure on M (where X acts by φ). If φ is surjective, then $M = \mathfrak{a}M$ with $\mathfrak{a} = (X) \subset R[X]$. By 1.5.3(a), there is an $a \in \mathfrak{a}$ such that $(1+a)M = 0$. Now if $m \in M$ is such that $\varphi(m) = 0$, then $0 = (1 + a)m = m + a(\varphi)(m) = m$, where $a(\varphi)(m) = 0$ by $a \in (X)$ and $\varphi(m) = 0$. ■

Counterexample 1.5.8. Corollary 1.5.7 is false if we replace "surjective" by "injective": take $\mathbb{Z} \xrightarrow{2} \mathbb{Z}$. See also 1.18.

Corollary 1.5.9. Let R be a ring and M, N be a finitely generated R-modules. If $M \otimes_R N = 0$, then $\operatorname{Ann}_R(M) + \operatorname{Ann}_R(N) = R$. In particular, if R is local, then either $M = 0$ or $N = 0$.

Proof. First suppose that $(R, \mathfrak{m}, k)$ is local and $M \neq 0$ but $M \otimes_R N = 0$. Then $M/\mathfrak{m}M \neq 0$ by Nakayama and so there is a surjection $M/\mathfrak{m}M \twoheadrightarrow k$. By right-exactness of the tensor product, this means that $0 = M \otimes_R N$ surjects onto $k \otimes_R N \cong N/\mathfrak{m}N$, and so again by Nakayama $N = 0$. In general, if $\operatorname{Ann}_R(M) + \operatorname{Ann}_R(N)$ is contained in some prime $\mathfrak{p}$, then $0 = (M \otimes_R N) \otimes_R R_\mathfrak{p} \cong M_\mathfrak{p} \otimes_{R_\mathfrak{p}} N_\mathfrak{p}$ implies by the first part that either $M_\mathfrak{p} = 0$ or $N_\mathfrak{p} = 0$. If, say, $M_\mathfrak{p} = 0$, then for each of the finitely many generators x_i of M, there is some $u_i \in R \smallsetminus \mathfrak{p}$ with $u_i x_i = 0$. Then $u = \prod_i u_i \in \operatorname{Ann}_R(M) \smallsetminus \mathfrak{p}$, a contradiction. ■

Remark 1.5.10. Geometrically, 1.5.9 asserts that the support of the tensor product $\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G}$ of two coherent $\mathcal{O}_X$-modules $\mathcal{F}, \mathcal{G}$ on a locally Noetherian scheme X is exactly the intersection of the supports of $\mathcal{F}$ and $\mathcal{G}$.

Corollary 1.5.11. Let R be a Noetherian domain and $\mathfrak{a} \subset R$ an ideal. If $\mathfrak{p} \subset R$ is a prime such that $\mathfrak{a} = \mathfrak{p}\mathfrak{a}$, then $\mathfrak{a} = 0$.

Proof. In the localization $R_\mathfrak{p}$, we have $\mathfrak{a}R_\mathfrak{p} = \mathfrak{p}R_\mathfrak{p} \cdot \mathfrak{a}R_\mathfrak{p}$. By 1.5.3(b), $\mathfrak{a}R_\mathfrak{p} = 0$. Since R is a domain, this forces $\mathfrak{a} = 0$. ■

1.6 Some Graded Commutative Algebra

Just as affine algebraic geometry deals with ideals in rings, *projective algebraic geometry* deals with homogeneous ideals in graded rings. Let us develop the basics of this vocabulary.

Definition 1.6.1. Let I be a monoid.

(a) An *I-graded ring* S is a ring together with a family of additive subgroups S_i indexed by $i \in I$ such that $S = \bigoplus_{i \in I} S_i$ and for all $i, j \in I$ we have $S_i S_j \subset S_{i+j}$.
(b) If S is an I-graded ring, then a *graded module* over S is an S-module M with a family of submodules M_i indexed by $i \in I$ such that $M = \bigoplus_{i \in I} M_i$ and for all $i, j \in I$ we have $S_i M_j \subset M_{i+j}$.
(c) If S is an I-graded ring and M a graded S-module, then the *twist* of M by $i \in I$ is the graded S-module $M(i)$ defined by $M(i)_j := M_{i+j}$.

Similarly, given a base ring k, it is easy to guess the definition of an I-graded k-algebra. Given an I-graded ring S, the submodule $S_0 \subset S$ is a ring, each S_i a module over S_0, and S is naturally a graded S_0-algebra. Similarly, if M is a graded S-module, then each M_i is an S_0-submodule of M. Given an I-graded ring S and a graded S-module M, for each $i \in I$, a nonzero element $m \in M_i$ is said to be *homogeneous of degree i*. Every element $m \in M$ can be uniquely decomposed into its homogeneous "components".

Proposition/Definition 1.6.2. Let I be a monoid, S an I-graded ring, and M a graded S-module. The following conditions on an S-submodule N of M are equivalent:

(a) For an $m \in M$, we have $m \in N$ iff each homogeneous component m_i of m is in N.
(b) The submodule N is generated over S by homogeneous elements of M.
(c) The natural map $\bigoplus_{i \in I} N \cap M_i \to N$ is an isomorphism.

In this case, we say that N is a *homogeneous submodule* of M.

Proof. Clear; details left to the reader. ■

In the above setting, if $N \subset M$ is a homogeneous submodule, then N is itself a graded S-module with grading $N_i := N \cap M_i$, and the quotient $M/N = \bigoplus_{i \in I} M_i/N_i$ is also a graded S-module.

Example 1.6.3.

(a) If V be a finite-dimensional vector space over a field k, then the *symmetric aglebra*

$$\operatorname{Sym}^* V^\vee := \bigoplus_{d \geq 0} \operatorname{Sym}^d V^\vee$$

is an $\mathbb{N}$-graded k-algebra. If V has dimension $n + 1 \geq 1$, then choosing a basis for V gives an isomorphism between $\operatorname{Sym}^* V^\vee$ and the polynomial ring $k[X_0, X_1, \ldots, X_n]$ which is also clearly $\mathbb{N}$-graded. If k is a field of characteristic two, then the exterior algebra $\Lambda^* V^\vee$ is also an $\mathbb{N}$-graded k-algebra.
(b) Given homogeneous polynomials $F_1, \ldots, F_r \in k[X_0, \ldots, X_n]$, the quotient ring

$$S := k[X_0, \ldots, X_n]/(F_1, \ldots, F_r)$$

is an $\mathbb{N}$-graded k-algebra; this is the *homogeneous coordinate ring of the projective variety V defined by the vanishing of the F_i, i.e., $V = \mathbb{V}(F_1, \ldots, F_r) \subset \mathbb{P}^n_k$.*

Example 1.6.4. Let R be a ring and $\mathfrak{a} \subset R$ be an ideal.

(a) The *Rees algebra* or *blowup* of R along $\mathfrak{a}$ is the graded R-algebra $\mathrm{Bl}_{\mathfrak{a}}(R) := \bigoplus_{n\geq 0} \mathfrak{a}^n$.
(b) The *associated graded ring* to R and $\mathfrak{a}$ is defined to be $\mathrm{gr}_{\mathfrak{a}}(R) := \bigoplus_{n\geq 0} \mathfrak{a}^n/\mathfrak{a}^{n+1}$.
(c) If M is an R-module, then the *associated graded module* to M and $\mathfrak{a}$ is defined by $\mathrm{gr}_{\mathfrak{a}}(M) := \bigoplus_{n\geq 0} \mathfrak{a}^n M/\mathfrak{a}^{n+1}M$. This is a graded $\mathrm{gr}_{\mathfrak{a}}(R)$-module.

If $\mathfrak{a} = (a_1, \ldots, a_r)$, then $a_1, \ldots, a_r \in \mathfrak{a} = \mathrm{Bl}_{\mathfrak{a}}(R)_1$ generate $\mathrm{Bl}_{\mathfrak{a}}(R)$ over $\mathrm{Bl}_{\mathfrak{a}}(R)_0 = R$, and $\overline{a}_1, \ldots, \overline{a}_r \in \mathfrak{a}/\mathfrak{a}^2 = \mathrm{gr}_{\mathfrak{a}}(R)_1$ generate $\mathrm{gr}_{\mathfrak{a}}(R)$ over $\mathrm{gr}_{\mathfrak{a}}(R)_0 = R/\mathfrak{a}$. For instance, if $R = k[x,y]$ and $\mathfrak{a} = (x,y)$, then $\mathrm{Bl}_{\mathfrak{a}}(R) \cong k[x,y,u,v]/(vx - uy)$ with $|u| = |v| = 1$. In particular, if R is a Noetherian ring, then for any ideal $\mathfrak{a} \subset R$, the blowup $\mathrm{Bl}_{\mathfrak{a}}(R)$ as well its associated graded ring $\mathrm{gr}_{\mathfrak{a}}(R)$ are both Noetherian rings; this follows from the next two results.

Lemma/Definition 1.6.5. Let S be an $\mathbb{N}$-graded ring. Then the following are equivalent:

(a) The ideal $S_+ := \bigoplus_{i\geq 1} S_i \subset S$ is a finitely generated ideal of S.
(b) The ring S is a finitely generated S_0-algebra.

In this situation, we say that S is a *finitely generated graded S_0-algebra*.

Proof. The homogeneous components of generators of S_+ as an ideal of S generate S as an S_0-algebra, and similary for the other direction, by an easy induction on the degree. ■

Corollary 1.6.6. Let S be an $\mathbb{N}$-graded ring. Then S is a Noetherian ring iff S_0 is a Noetherian ring and S is a finitely generated graded S_0-algebra.

Proof. If S is Noetherian, then $S_0 \cong S/S_+$ is as well, and further the criterion of 1.6.5(a) is clear. The converse follows from 1.3.5. ■

1.6.1 Hilbert Functions and Polynomials

Definition 1.6.7. Let R, S be rings and $f : R \to S$ a function. For each $k \geq 1$, we recursively define the k^{th} *finite difference function of* f, denoted $\Delta^{[k]} f : R \to S$, by

$$\Delta^{[1]} f(r) := f(r+1) - f(r) \text{ and } \Delta^{[k]} f := \Delta^{[1]}(\Delta^{[k-1]} f) \text{ for } k \geq 2.$$

In this definition, R does not really even need to be a ring; an additive monoid like $R = \mathbb{N}$ also suffices. It is inductively clear that for any $k \geq 1$ we have

$$\Delta^{[k]}(f)(r) := \sum_{i=0}^{k} (-1)^{i-1} \binom{k}{i} f(r+i).$$

Further, if R is a $\mathbb{Q}$-algebra and f is polynomial (i.e., if R is a subalgebra of S and there is a polynomial in $S[X]$ which yields the polynomial function f), then for any $a \in R$, it can be expanded as

$$f(X) = \sum_{k=0}^{\infty} (\Delta^k f)(a) \binom{X-a}{k}.$$

Definition 1.6.8. Let $f : \mathbb{N} \to \mathbb{Q}$ be a function. We say that f is *polynomial-like* if there is a polynomial $g(X) \in \mathbb{Q}[X]$ such that $f(n) = g(n)$ for all but finitely many $n \in \mathbb{N}$. In this case, g is determined uniquely and we let the *degree* of f be $\deg f := \deg g$.

Remark 1.6.9. By convention in this circle of ideas, we say that the zero polynomial has degree -1.

The fundamental observation in this direction is

Observation 1.6.10. Let $f : \mathbb{N} \to \mathbb{Q}$ be a function and $d \in \mathbb{Z}_{\geq 0}$. Then f is polynomial-like of degree d iff $\Delta^{[1]} f$ is polynomial-like of degree $d - 1$.

We are now ready for a fundamental definition in the subject.

Definition 1.6.11. Let S be an $\mathbb{N}$-graded ring such that S_0 is Artinian and S is a finitely generated graded S_0-algebra. If M is a finitely generated graded S-module, then for any $n \in \mathbb{N}$ the length $\ell_{S_0}(M_n)$ is finite. We define the *Hilbert function* $h_M : \mathbb{N} \to \mathbb{N}$ of M by

$$h_M(n) := \ell_{S_0}(M_n)$$

for $n \in \mathbb{N}$.

Note that for each $n \in \mathbb{N}$, the S_0-module M_n is finitely generated and hence Artinian; in particular, it has finite length by 1.3.10 and 1.3.4.

Theorem/Definition 1.6.12. Let S be as in 1.6.11, and suppose further that S is generated over S_0 by say $r + 1$ elements of S_1 for some $r \in \mathbb{Z}_{\geq -1}$.[10] For any finitely generated graded S-module M and $n \in \mathbb{N}$, the Hilbert function h_M is polynomial-like of degree at most r. The polynomial $p_M(t) \in \mathbb{Q}[t]$ it eventually equals is called the *Hilbert polynomial* of M.

Before giving the proof, let's consider some basic properties and examples.

Remark 1.6.13. Let S be as in 1.6.12.

(a) For a finitely generated graded S-module M and $d \in \mathbb{Z}_{\geq 0}$, we have $p_{M(d)}(t) = p_M(t+d) \in \mathbb{Q}[t]$.

(b) If $0 \to M' \to M \to M'' \to 0$ is a short exact sequence of finitely generated graded S-modules, then $p_M(t) = p_{M'}(t) + p_{M''}(t) \in \mathbb{Q}[t]$. A similar result to Exercise 10.2 holds for longer exact sequences.

Example 1.6.14.

(a) Let $r \in \mathbb{Z}_{\geq 0}$, and let $S := k[X_0, \dots, X_r]$.

  (i) Consider $M = S$ as a graded module. Then $p_M(t) = \binom{t+r}{r} \in \mathbb{Q}[t]$.

  (ii) Given a $d \in \mathbb{Z}_{\geq 0}$ and a nonzero $f \in S_d$, if $M := S/(f)$, then

$$p_M(X) = \binom{t+r}{r} - \binom{t-d+r}{r} = \frac{d}{(r-1)!} t^{r-1} + \cdots \in \mathbb{Q}[t].$$

(b) The hypothesis that S is generated by elements of degree 1 cannot be removed. For instance, if $S = k[X, Y]$ with $|Y| = 2|X| = 2$, then we have for $n \in \mathbb{N}$ that $h_M(n) = \lceil (n+1)/2 \rceil$, which is not polynomial-like. However, see Exercise 1.23.

Proof of 1.6.12. We induct on r. When $r = -1$, we have $S = S_0$ and it is clear that $h_M(n) = 0$ for all $n \gg 0$. Now suppose that $r \geq 0$, and elements $x_0, \dots, x_r \in S_1$ are chosen so that $S = S_0[x_0, \dots, x_r]$. Given an M as in the theorem and $n \in \mathbb{N}$, consider the morphism $x_r : M \to M(1)$ of graded S-modules given by multiplication by x_r, and let K and L denote its kernel and cokernel respectively. Then K and L are also graded S-modules which are finitely generated since S is Noetherian. Note also that K and L are annihilated by x_r and hence can be thought of as graded $S/(x_r)$-modules. By the induction hypothesis, we conclude that the

[10] The fundamental example to keep in mind here is (unweighted) projective space, i.e., when $S := k[X_0, \dots, X_r]$ with each X_i of degree one for $i = 0, \dots, r$.

Hilbert functions h_K and h_L are polynomial-like of degree at most $r-1$. Now the short exact sequence of finitely generated graded S-modules

$$0 \to K \to M \xrightarrow{x_r} M(1) \to L \to 0$$

shows us using 1.6.13 that

$$\Delta^{[1]} h_M = h_L - h_K.$$

The result then follows from 1.6.10. ∎

1.6.2 Completion and the Artin-Rees Lemma

Let us now talk about a close cousin of gradings: filtrations.

Definition 1.6.15. Let R be a ring, $\mathfrak{a} \subset R$ an ideal, and M an R-module.

(a) A *filtration* $\mathscr{M} = (M_n)_{n\in\mathbb{N}}$ on M is a chain $M = M_0 \supset M_1 \supset M_2 \supset \cdots$ of R-submodules of M.

(b) A filtration $\mathscr{M}$ of M is called an $\mathfrak{a}$*-filtration* if for all $n \in \mathbb{N}$ we have $\mathfrak{a}M_n \subset M_{n+1}$. It is called a *stable* $\mathfrak{a}$*-filtration* if $\mathfrak{a}M_n = M_{n+1}$ for all $n \gg 0$ (e.g., the filtration given by $M_n = \mathfrak{a}^n M$ for $n \in \mathbb{N}$.)

Every filtration $\mathscr{M}$ on M determines a topology on $\mathscr{M}$ by taking the elements of the filtration to be a niehgborhood basis of $0 \in M$; this makes M into a topological module. Two filtrations $\mathscr{M}$ and $\mathscr{M}'$ determine the same topology on M iff they have *bounded difference*, i.e., when there is an $N \in \mathbb{N}$ such that for all $n \in \mathbb{N}$ we have $M_{n+N} \subset M'_n$ and $M'_{n+N} \subset M_n$.

Lemma/Definition 1.6.16. In the above set-up, if $\mathscr{M}$ and $\mathscr{M}'$ are two $\mathfrak{a}$-stable filtrations on M, then they have bounded difference. In particular, the topology induced on M by an $\mathfrak{a}$-stable filtration is independent of the filtration, and is called the $\mathfrak{a}$*-adic topology on* M.

Proof. We may assume without loss of generality that $M'_n = \mathfrak{a}^n M$ for all $n \in \mathbb{N}$. Since M is an $\mathfrak{a}$-filtration, we have $M'_n \subset M_n$ for all $n \in \mathbb{N}$; since M is a *stable* $\mathfrak{a}$-filtration, there is an $N \in \mathbb{N}$ such that for all $n \in \mathbb{N}$ with $n \geq N$, we have $\mathfrak{a}M_n = M_{n+1}$, and hence $M_{n+N} = \mathfrak{a}^n M_N \subset M'_n$. ∎

In the above set-up, we denote by $\hat{M}_{\mathfrak{a}}$ the completion of M with respect to the $\mathfrak{a}$-adic topology. The completion $\hat{M}_{\mathfrak{a}} \cong \varprojlim_n M/\mathfrak{a}^n M$ is a topological module, and there is a natural continuous morphism $\kappa_{\mathfrak{a}} : M \to \hat{M}_{\mathfrak{a}}$ with kernel $K_{M,\mathfrak{a}} = \bigcap_n \mathfrak{a}^n M$; further this pair $(\hat{M}_{\mathfrak{a}}, \kappa_{\mathfrak{a}})$ satisfies an obvious universal property which characterizes it uniquely (check!). The $\mathfrak{a}$-adic topology on M is Hausdorff iff $K_{M,\mathfrak{a}} = 0$, and it is complete Hausdorff iff the map $\kappa_{\mathfrak{a}}$ is an isomorphism. If $M = R$, then the completion $\hat{R}_{\mathfrak{a}}$ is in fact a ring and $\kappa_{\mathfrak{a}}$ is a ring homomorphism; we usually let $K_{\mathfrak{a}} := K_{R,\mathfrak{a}}$.

Definition 1.6.17. The module M (resp. ring R) is said to be $\mathfrak{a}$*-adically complete* if the natural map $\kappa_{\mathfrak{a}} : M \to \hat{M}_{\mathfrak{a}}$ (resp. $\kappa_{\mathfrak{a}} : R \to \hat{R}_{\mathfrak{a}}$) is an isomorphism.

Example 1.6.18. Let R be a ring. For any maximal ideal $\mathfrak{m} \subset R$, the completion $\hat{R}_{\mathfrak{m}}$ is a local ring. Indeed, an element $(x_n) \in \varprojlim_n R/\mathfrak{m}^n$ is invertible in the limit iff $0 \neq x_1 \in R/\mathfrak{m}$, which follows from an easy inductive construction.

Suppose we are given a ring R, an ideal $\mathfrak{a} \subset R$, and an R-module M. Given a filtration $\mathscr{M}$ on M, we construct the total graded module $\mathrm{Bl}^{\mathscr{M}}_{\mathfrak{a}}(M) := \bigoplus_{n\geq 0} M_n$. If $\mathscr{M}$ is an $\mathfrak{a}$-filtration, then $\mathrm{Bl}^{\mathscr{M}}_{\mathfrak{a}}(M)$ is naturally a graded $\mathrm{Bl}_{\mathfrak{a}}(R)$-module.

Proposition 1.6.19. In the above notation, if R is a Noetherian ring and M a finitely generated R-module, then the $\mathrm{Bl}_{\mathfrak{a}}(R)$-module $\mathrm{Bl}_{\mathfrak{a}}^{\mathscr{M}}(M)$ is finitely generated iff $\mathscr{M}$ is a stable $\mathfrak{a}$-filtration.

Proof. As observed above (1.6.4), the ring $\mathrm{Bl}_{\mathfrak{a}}(R)$ is Noetherian. If $\mathscr{M}$ is $\mathfrak{a}$-stable, then there is an $N \in \mathbb{N}$ such that for all $n \geq N$ we have $\mathfrak{a}M_n = M_{n+1}$; then $\mathrm{Bl}_{\mathfrak{a}}^{\mathscr{M}}(M)$ is generated as a $\mathrm{Bl}_{\mathfrak{a}}(R)$-module by $\bigoplus_{n \leq N} M_n$ and is hence finitely generated. Conversely, if $\mathrm{Bl}_{\mathfrak{a}}^{\mathscr{M}}(M)$ is finitely generated, then it is Noetherian, and so the chain (S_n) of submodules given by

$$S_n = M_0 \oplus M_1 \oplus \cdots \oplus M_n \oplus \mathfrak{a}M_n \oplus \mathfrak{a}^2 M_n \oplus \cdots$$

for $n \in \mathbb{N}$ eventually stabilizes. Since $\bigcup_n S_n = \mathrm{Bl}_{\mathfrak{a}}^{\mathscr{M}}(M)$, we then conclude that there is an $N \in \mathbb{N}$ such that $\mathrm{Bl}_{\mathfrak{a}}^{\mathscr{M}}(M) = S_N$, and hence for all $n \geq N$ we have $\mathfrak{a}M_n = M_{n+1}$. ■

Lemma 1.6.20 (Artin-Rees)**.** Let R be a Noetherian ring, $\mathfrak{a} \subset R$ an ideal, M a finitely generated R-module, and $N \subset M$ a submodule.

(a) In $\mathscr{M} = (M_n)$ is a stable $\mathfrak{a}$-filtration on M, then $\mathscr{N} = (N \cap M_n)$ is a stable $\mathfrak{a}$-filtration on N. In other words, the $\mathfrak{a}$-adic topology on M restricts to the subspace $N \subset M$ to give the $\mathfrak{a}$-adic topology on N.

(b) There is an integer $m \in \mathbb{N}$ such that for all $n \in \mathbb{N}$ we have $N \cap \mathfrak{a}^{m+n}M = \mathfrak{a}^n(N \cap \mathfrak{a}^m M)$.

Proof.

(a) Since $\mathscr{M}$ is stable, the $\mathrm{Bl}_{\mathfrak{a}}(R)$-module $\mathrm{Bl}_{\mathfrak{a}}^{\mathscr{M}}(M)$ is finitely generated (by 1.6.19) and hence Noetherian, since $\mathrm{Bl}_{\mathfrak{a}}(R)$ is Noetherian (1.6.4). Therefore, the $\mathrm{Bl}_{\mathfrak{a}}(R)$-submodule $\mathrm{Bl}_{\mathfrak{a}}^{\mathscr{N}}(N) \subset \mathrm{Bl}_{\mathfrak{a}}^{\mathscr{N}}(M)$ is also finitely generated, so again by 1.6.19 we conclude that $\mathscr{N}$ is a stable $\mathfrak{a}$-filtration.

(b) Apply (a) to the filtration $\mathscr{M} = (\mathfrak{a}^n M)_n$.

■

In general, it is not true that for all any $m \in \mathbb{N}$ we have $N \cap \mathfrak{a}^m M = \mathfrak{a}^m N$, as easily constructed counterexamples show (check!).

1.7 Fractional Ideals and their Invertibility

Fix a domain R with field of fractions $K = \operatorname{Frac} R$.

Lemma/Definition 1.7.1.

- Consider the following conditions on an R-submodule $\mathfrak{f} \subset K$:
  (a) There is an $x \in K^\times$ such that $x\mathfrak{f} \subset R$.
  (b) There is an ideal $\mathfrak{a} \subset R$ and a nonzero $t \in R$ such that $\mathfrak{f} = t^{-1}\mathfrak{a}$.
  (c) There is an ideal $\mathfrak{a} \subset R$ and a $y \in K^\times$ such that $\mathfrak{f} = y\mathfrak{a}$.
  (d) The submodule $\mathfrak{f} \subset K$ is finitely generated.

  Then (a)-(c) are equivalent and implied by (d). If R is Noetherian, then all conditions are equivalent. An R-submodule $\mathfrak{f} \subset K$ satisfying equivalent conditions (a)-(c) is said to be a *fractional ideal* of R. A fractional ideal $\mathfrak{f} \subset R$ is said to be *principal* iff there is an $f \in \mathfrak{f}$ such that $\mathfrak{f} = fR$.

Note that a fractional ideal of R contained in R (sometimes known as an *integral* ideal) is just an ideal of R; likewise a principal integral ideal is the same thing as a principal ideal of R.

- There is an evident notion of the sum and product of fractional ideals extending the usual notions for ideals; further this notion is compatible with localization of R. Evidently, the set of fractional ideals forms a commutative monoid under multiplication.
- Let $\mathfrak{f}, \mathfrak{g} \subset K$ be fractional ideals. We define the colon ideal $(\mathfrak{g} : \mathfrak{f})$ to be

$$(\mathfrak{g} : \mathfrak{f}) := \{x \in K : x\mathfrak{f} \subset \mathfrak{g}\},$$

  and the *inverse* of $\mathfrak{f}$ to be $\mathfrak{f}^{-1} := (R : \mathfrak{f})$. Note that if $\mathfrak{f} \neq 0$, then for any $\mathfrak{g}$, the colon $(\mathfrak{g} : \mathfrak{f})$ is also a fractional ideal (check!), and further $\mathfrak{f} \cdot (\mathfrak{g} : \mathfrak{f}) \subset \mathfrak{g}$, although equality need not hold in general.

We begin with an easy lemma.

Lemma 1.7.2. Let $\mathfrak{f} \subset K$ be a nonzero R-submodule. If $\beta : \mathfrak{f} \to K$ is an R-linear map, then there is a unique $b \in K$ such that $\beta(x) = bx$ for all $x \in \mathfrak{f}$.

Proof. Pick an $x_0 \in \mathfrak{f} \smallsetminus \{0\}$, and check that $b := \lambda(x_0) \cdot x_0^{-1}$ works, and is the only such element. ■

The fractional ideals $\mathfrak{f}$ for which equality holds in $\mathfrak{f} \cdot \mathfrak{f}^{-1} \subset R$ are rather special.

Theorem/Definition 1.7.3 (Invertible Ideals)**.** The following conditions on a nonzero fractional ideal $\mathfrak{f}$ of R are equivalent.

(a) We have $\mathfrak{f} \cdot \mathfrak{f}^{-1} = R$.
(b) There is some fractional ideal $\mathfrak{g}$ such that $\mathfrak{f} \cdot \mathfrak{g} = R$, i.e., $\mathfrak{f}$ is invertible in the monoid of fractional ideals under multiplication.
(c) There is a finite set I, elements $a \in \mathfrak{f}^I$ and $b \in R^I$ such that $\sum_{i \in I} a_i b_i = 1$, and such that for all $i \in I$, we have $b_i\mathfrak{f} \subset R$.
(d) The ideal $\mathfrak{f}$ is a projective R-module.
(e) The ideal $\mathfrak{f}$ is finitely generated, and for all primes $\mathfrak{p}$, the fractional ideal $\mathfrak{f}_\mathfrak{p} = \mathfrak{f}R_\mathfrak{p}$ of $R_\mathfrak{p}$ is principal.
(f) The ideal $\mathfrak{f}$ is finitely generated, and for all maximal $\mathfrak{m}$ the fractional ideal $\mathfrak{f}_\mathfrak{m}$ of $R_\mathfrak{m}$ is principal.

A fractional ideal $\mathfrak{f}$ is said to be *invertible* iff it is nonzero and satisfies equivalent conditions (a)-(e).

Proof. The implications (a) $\Rightarrow$ (b) $\Rightarrow$ (c) and (e) $\Rightarrow$ (f) are clear.

(c) $\Rightarrow$ (a) Clearly, each $b_i \in \mathfrak{f}^{-1}$, but $\sum_{i\in I} a_i b_i = 1$ implies $\mathfrak{f}^{-1} \subset (b_i)$ as well, and $\mathfrak{f}\cdot\mathfrak{f}^{-1} = \mathfrak{f}\cdot(b_i) \ni 1$.

(c) $\Leftrightarrow$ (d) For the forward implication, note that $\mathfrak{f}$ is finitely generated by the a_i; then the surjection $R^I \overset{a}{\twoheadrightarrow} \mathfrak{f}$ with section $\mathfrak{f} \overset{b}{\to} R^I$ exhibits $\mathfrak{f}$ as a direct summand of R^I. For the reverse implication, let I be a set and $a : R^{\oplus I} \to \mathfrak{f}$ a split surjection with section $\beta : \mathfrak{f} \to R^{\oplus I}$. By 1.7.2, there is a unique $b \in R^{\oplus I}$ such that λ is given by b; finish by replacing I by a finite subset containing the support of b.

(c) $\Rightarrow$ (e) It only remains to be shown that $\mathfrak{f}_\mathfrak{p}$ is principal. Pick a $j \in I$ such that $a_j b_j \in R_\mathfrak{p}^\times$; we show that $\mathfrak{f}_\mathfrak{p} \subset a_j R_\mathfrak{p}$. Indeed, if $x \in \mathfrak{f}_\mathfrak{p}$, then

$$x = \sum_{i\in I} a_i b_i x = a_j \sum_{i\in I} (a_j b_j)^{-1}(a_i b_i)(b_j x)$$

with $a_i b_i \in R$ and $b_j x \in R_\mathfrak{p}$ (since $b_j\mathfrak{f} \subset R$).

(f) $\Rightarrow$ (a) Clearly, $(\mathfrak{f}^{-1})_\mathfrak{m} \subset \mathfrak{f}_\mathfrak{m}^{-1}$ with equality if $\mathfrak{f}$ is finitely generated (check!). Since $\mathfrak{f}_\mathfrak{m}$ is principal, it is invertible. If $\mathfrak{f}\cdot\mathfrak{f}^{-1} \subsetneq R$, there is a maximal $\mathfrak{f}_\mathfrak{m}$ such that $\mathfrak{f}\cdot\mathfrak{f}^{-1} \subset \mathfrak{m}$; then we get a contradiction from the sequence

$$R_\mathfrak{m} = \mathfrak{f}_\mathfrak{m}\cdot\mathfrak{f}_\mathfrak{m}^{-1} = \mathfrak{f}_\mathfrak{m}\cdot(\mathfrak{f}^{-1})_\mathfrak{m} = (\mathfrak{f}\cdot\mathfrak{f}^{-1})_\mathfrak{m} \subset \mathfrak{m}R_\mathfrak{m}.$$

■

Example 1.7.4. A non-finitely-generated ideal cannot be projective as a module; in particular, any non-Noetherian ring admits an ideal which is not a projective module.

We like invertible ideals because they behave a lot like numbers. Here's one example of this phenomenon.

Lemma 1.7.5. If a nonzero ideal in a domain can be written as a product of finitely many invertible primes, then this expression is unique.

Proof. Let R be a domain, $n, m \in \mathbb{Z}_{\geq 0}$ be integers, and $\mathfrak{p}_1, \ldots, \mathfrak{p}_n, \mathfrak{q}_1, \ldots, \mathfrak{q}_m$ be invertible primes of R such that $\prod_i \mathfrak{p}_i = \prod_j \mathfrak{q}_j$; we have to show that $n = m$, and up to reordering, $\mathfrak{p}_i = \mathfrak{q}_i$ for all $i = 1, \ldots, n$. Without loss of generality, assume $n \leq m$; we induct on n, with the case $n = 0$ being clear. Suppose $n \geq 1$. For each $i = 1, \ldots, n$, the inclusion $\prod_j \mathfrak{q}_j \subset \mathfrak{p}_i$ implies by 1.2.14(a) that there is a j with $\mathfrak{q}_j \subset \mathfrak{p}_i$. If we choose an i so that $\mathfrak{p}_i$ is minimal among $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$, then the previous observation applied twice gives us that there is a j such that $\mathfrak{p}_i = \mathfrak{q}_j$. Multiplying both sides by $\mathfrak{p}_i^{-1}$ then reduces n by 1 and finishes the proof. ■

Definition 1.7.6.

- The group of invertible fractional ideals of R is called the *ideal group* of R and denoted by Ideal(R).
- The group Ideal(R) contains as a subgroup the group of nonzero principal fractional ideals. We define the *ideal class group* or *Picard group* of R, denoted Pic(R), to be the quotient by this subgroup, i.e., via the exact sequence

$$0 \to R^\times \to K^\times \to \mathrm{Ideal}(R) \to \mathrm{Pic}(R) \to 0.$$

- We define the *ideal class number* of R, denoted $h(R)$, to be the cardinality of Pic(R).[11]

[11] Note that this need not be finite, as is the case, for instance, for $R := \mathbb{C}[X,Y]/(Y^2 - X^3 - 1)$.

Example 1.7.7. Let R be a UFD; we show that $h(R) = 1$. Indeed, let $\mathfrak{f} \subset R$ be an invertible fractional ideal; as noted above, $\mathfrak{f}$ is finitely generated, say by $a_i = x_i/y_i$ for $i \in I$ for some finite set I and $x_i, y_i \in R \smallsetminus \{0\}$ satisfying $\gcd(x_i, y_i) = 1$ for all i. If $z := \operatorname{lcm}(y_i)/\gcd(x_i)$, then clearly $z \in \mathfrak{f}^{-1}$. Conversely, any $b \in \mathfrak{f}^{-1}$ of the form $b = x/y$ for $x, y \in R \smallsetminus \{0\}$ with $\gcd(x, y) = 1$ satisfies $\operatorname{lcm}(y_i) \mid x$ and $y \mid \gcd(x_i)$ so that $\mathfrak{f}^{-1} = (z)$.

1.8 Exercises

Exercise 1.1. Let R be a ring and $S, T \subset R$ be multiplicative subsets such that $S \subset T$. The universal property of localizations gives us homomorphisms $S^{-1}R \to T^{-1}R$ and $S^{-1}M \to T^{-1}M$ for any module M. Show that the kernel of $S^{-1}R \to T^{-1}R$ is

$$\{s^{-1}r \in S^{-1}R : tr = 0 \text{ for some } t \in T\}.$$

Exercise 1.2. Let R be a ring and $S \subset R$ a multiplicative subset. Characterize, in terms of S, the elements of R which map to units in the localization $R \to S^{-1}R$. Let $\overline{S}$ denote the set of such elements; this is known as the "saturation" of S. Show that $\overline{S}$ is multiplicative, $S \subset \overline{S}$, and the natural morphism $S^{-1}R \to (\overline{S})^{-1}R$ is an isomorphism. A multiplicative subset S is said to be *saturated* if $S = \overline{S}$. Show that for any S, the saturation $\overline{S}$ is saturated.

Exercise 1.3. Show that if R and S are rings, then $\mathrm{Quot}(R \times S) \cong \mathrm{Quot}(R) \times \mathrm{Quot}(S)$. Conclude that $\mathrm{Quot}(\mathbb{Z} \times \mathbb{Z}) \cong \mathbb{Q} \times \mathbb{Q}$. Does the same result also hold for arbitrary (possibly infinite) products of rings?

Exercise 1.4. Let R be a ring and $S \subset R$ a multiplicative subset. Show that if $f \in R$ is a nonzerodivisor, then so is $f/1 \in S^{-1}R$. Does some sort of a converse hold?

Exercise 1.5. Show that if R is a ring and $S \subset R$ a multiplicative subset, then the localization morphism $\eta : R \to S^{-1}R$ is an epimorphism in the category of rings.

Exercise 1.6. Show that the following conditions on a ring R are equivalent.

(a) The underlying abelian group of R is torsion-free. In other words, if $\varepsilon \in R$ is such that for some $n \in \mathbb{Z}_{\geq 1}$, we have $n\varepsilon = 0$, then $\varepsilon = 0$.
(b) The natural map $R \to \mathbb{Q} \otimes_{\mathbb{Z}} R$ is injective.
(c) There is a $\mathbb{Q}$-algebra K and a ring monomorphism $R \to K$.

A ring satisfying these equivalent conditions is called *torsion-free.*

Exercise 1.7. Let R be a ring and $S \subset R$ a multiplicative subset. Show that if M is an R-module and $N \subset M$ an R-submodule, then for any $x \in M$, the following are equivalent.

(a) $x \in N$.
(b) $[x] \in S^{-1}N$ for every multiplicative $S \subset R$.
(c) $[x] \in N_{\mathfrak{p}}$ for all $\mathfrak{p}$.
(d) $[x] \in N_{\mathfrak{m}}$ for all $\mathfrak{m}$.

Exercise 1.8. Let $\mathfrak{a}, \mathfrak{b} \subset R$ be two ideals of the ring R. Consider the following conditions:

(a) Every prime containing $\mathfrak{a}$ also contains $\mathfrak{b}$, i.e., $\mathbb{V}(\mathfrak{a}) \subset \mathbb{V}(\mathfrak{b})$.
(b) We have $\mathfrak{b} \subset \sqrt{\mathfrak{a}}$.
(c) There is an $N \gg 1$ such that $\mathfrak{b}^N \subset \mathfrak{a}$.

Show that (a) and (b) are equivalent and implied by (c), and that (c) is equivalent to (a) and (b) if $\mathfrak{b}$ is finitely generated (e.g. if R is Noetherian).

Exercise 1.9. Let R be a ring. Show that:

(a) If $S \subset R$ a multiplicative subset, then $\mathrm{Nil}(S^{-1}R) = S^{-1}\,\mathrm{Nil}(R) = \mathrm{Nil}(R) \cdot S^{-1}R$.
(b) The following are equivalent:
    (i) R is reduced.
    (ii) $S^{-1}R$ is reduced for each multiplicative $S \subset R$.
    (iii) $R_{\mathfrak{p}}$ is reduced for each $\mathfrak{p}$.
    (iv) $R_{\mathfrak{m}}$ is reduced for each $\mathfrak{m}$.

Exercise 1.10. Let R be a ring, M be an R-module, and $\mathfrak{p} \subset R$ a prime. Show that there is a natural isomorphism of $R_\mathfrak{p}$ modules

$$M_\mathfrak{p} \cong \varinjlim_{f \notin \mathfrak{p}} R[f^{-1}] \otimes_R M.$$

(Part of the problem is to make sense of the colimit in the above and to give it an $R_\mathfrak{p}$ module structure.)

Exercise 1.11. Let R be a ring and $S \subset R$ a multiplicative subset. For an ideal $\mathfrak{a} \subset R$, let $\mathfrak{a}^e := \mathfrak{a}S^{-1}R$ denote its extension to $S^{-1}R$.

(a) Show that $\mathfrak{a}^e$ consists of exactly all the elements of the form $\{s^{-1}a : a \in \mathfrak{a}, s \in S\}$.

Now suppose we are given a family of ideals $(\mathfrak{a}_i)_{i \in I}$ of R.

(b) Let $\mathfrak{a} = \bigcap \mathfrak{a}_i$. Show that $\mathfrak{a}^e \subset \bigcap_i \mathfrak{a}_i^e$.
(c) Let $\mathfrak{a} = (\mathfrak{a}_i)$ be the ideal generated by the $\mathfrak{a}_i$. Show that $(\mathfrak{a}_i^e) \subset \mathfrak{a}^e$.

In both cases (b) and (c), show that equality holds if the indexing set I is finite, and determine whether equality holds without this assumption on I. If it does, prove it. If it does not, give a counterexample.

Exercise 1.12. Let $\phi : R \to S$ be a ring homomorphism between local rings. Are the following conditions on ϕ are equivalent?

(a) We have $\phi(\mathfrak{m}_R) \subset \mathfrak{m}_S$.
(b) We have $\phi^{-1}\mathfrak{m}_S = \mathfrak{m}_R$.
(c) We have $\phi^{-1}(S^\times) = R^\times$.
(d) We have $\phi(R^\times) \subset S^\times$.

If they are, prove their equivalence. If they are not, give a counterexample, and prove all possible implications between the statements to salvage it to the maximum degree.

Exercise 1.13.

(a) Suppose that k is an infinite field, V a k-vector space, n a positive integer, and $U, V_1, \dots, V_n \subset V$ subspaces. Show that if $U \subset \bigcup_{i=1}^n V_i$, then there is an i with $1 \leq i \leq n$ such that $U \subset V_i$. In particular, a vector space over k cannot be a finite union of proper subspaces.
(b) Show by example that the statement in (a) is false if we do not require k to be infinite.

Exercise 1.14. Show that if R is a ring and $\mathfrak{m} \subset R$ a maximal ideal, then for each integer $n \geq 1$, the ring $R/\mathfrak{m}^n$ is a local ring. What is the unique maximal ideal of $R/\mathfrak{m}^n$?

Exercise 1.15. Let R be a domain with fraction field K so all localizations $S^{-1}R$ for $S \subset R \smallsetminus \{0\}$ can be considered as subrings of K. Show that, inside K, we have $\bigcap_\mathfrak{m} R_\mathfrak{m} = R$.

Exercise 1.16. For any natural number N, let $\mathbb{Z}\langle 1/N \rangle := \{q \in \mathbb{Q} : Nq \in \mathbb{Z}\} \subset \mathbb{Q}$ be the abelian subgroup of $\mathbb{Q}$ generated by $1/N$, so that for any natural number n, we have a chain of additive subgroups

$$\mathbb{Z} \subset \mathbb{Z}\langle 1/n \rangle \subset \mathbb{Z}\langle 1/n^2 \rangle \subset \cdots \subset \mathbb{Z}[1/n] \subset \mathbb{Q}.$$

Show that if $n = p$ is prime, then these are all the subgroups of (the underlying additive subgroup of) the ring $\mathbb{Z}[1/n]$ which contain $\mathbb{Z}$. Conclude that the $\mathbb{Z}$-module $\mathbb{Z}[1/p]/\mathbb{Z}$ is Artinian but not Noetherian. What happens when n is not prime?

Exercise 1.17. A ring R is said to be *strongly associate* if the following holds: if $r, s \in R$ are such that $(r) = (s)$ (i.e. the principal ideals generated by r and s are the same), then there is a unit $u \in R^\times$ such that $r = us$. Show that domains, local rings, principal ideal rings, and Artinian rings are strongly associate. Find a ring that is not strongly associate.

Exercise 1.18.

(a) ([4, Exercise 6.1]) Let M be a Noetherian (resp. Artinian) module, and $\varphi : M \to M$ an endomorphism. Show that if φ is surjective (resp. injective), then φ is an isomorphism.

(b) (Ross) Prove or disprove and salvage if possible: if R is a ring, then $R \not\cong R[X]$ as rings.

Exercise 1.19. Let R be a ring.

(a) Show that R is a domain iff the polynomial ring $R[X]$ is, and in this case (and only in this case) the degree function $\deg : R[X] \to \mathbb{Z}_{\geq 0} \cup \{-\infty\}$ is additive (i.e., satisfies $\deg(fg) = \deg(f) + \deg(g)$ for $f, g \in R[X]$).

(b) Show that given a $p \in R$, this p is a prime element in R iff it is a prime element in $R[X]$.

Generalize to an arbitrary number of variables.

Exercise 1.20. Show that the following conditions on a domain are equivalent:

(a) The domain is a UFD.

(b) Every nonzero nonunit is a finite product of *prime* elements.

(c) (Kaplansky) Every nonzero prime ideal contains a prime element.

Use Kaplansky's criterion (c) to give alternative proofs of 1.4.5 and 1.4.10.

Exercise 1.21.

(a) Prove or disprove and salvage if possible: If R is a UFD and $\mathfrak{a} \subset R$ an ideal, then $R/\mathfrak{a}$ is a UFD. Do the same for when $R = K[X_1, \dots, X_n]$ for some field K and $\mathfrak{a} = (f)$ is principal.

(b) (Klein-Nagata) Fix an $n \geq 1$ and let $R := \mathbb{C}[X_1, \dots, X_n]$ and $f := X_1^2 + \cdots + X_n^2$. Then $R/(f)$ is a UFD if $n \geq 5$. What happens when $1 \leq n \leq 4$?

(c) (Samuel) Let K be any field, $R = K[X, Y, Z]$ and $f = X^2 + Y^3 + Z^7$. Then $R/(f)$ is a UFD.

Exercise 1.22. Given an R-algebra $\mathbb{Q}$, element $a \in R$, and integer $n \in \mathbb{Z}_{\geq 0}$, we define the *binomial coefficient polynomial*

$$b(a, n)(t) := \binom{t+a}{n} := \frac{(t+a)(t+a-1)\cdots(t+a-n+1)}{n!} \in R[t].$$

By convention, we define $b(a, n)(t) := 0$ for any a when $n < 0$.

For a polynomial $f(t) \in R[t]$, we define the *first difference polynomial* $\Delta^{[1]}f$ to be $(\Delta^{[1]}f)(t) := f(t+1) - f(t)$; the higher difference polynomials $\Delta^{[k]}f$ for $k \geq 2$ are then defined inductively as for higher difference functions.

(a) Show that for any $a \in R$ and $n, k \in \mathbb{Z}_{\geq 0}$, we have $\Delta^{[k]}b(a, n) = b(a, n-k)$.

(b) Fix a $d \in \mathbb{Z}_{\geq 0}$ and elements $a_0, \dots, a_d \in R$. Then the polynomials $\{b(a_i, i)\}_{i=0}^{d}$ form an R-basis for $R[t]_{\leq d}$. Show that if $a_0, \dots, a_d \in \mathbb{Z}$, then the following are equivalent:

(i) The function defined by f is integer-valued on integers, i.e., for all $n \in \mathbb{Z}$, we have $f(n) \in \mathbb{Z}$.

(ii) For all $i = 0, \dots, d$, we have $c_i \in \mathbb{Z}$.

Produce a counterexample to this result when not all the a_i are in $\mathbb{Z}$.

Therefore, a rational polynomial is integer-valued on the integers iff it can be written as an integral combination of binomial coefficients.

Exercise 1.23. Let S and M be as in 1.6.11, and suppose we write $S = S_0[x_0, \dots, x_r]$, where for $i = 0, \dots, d$, the variable x_i has degree $d_i \in \mathbb{Z}_{\geq 1}$. Define the *Hilbert series* of M to be

$$H_M(t) := \sum_{n \in \mathbb{N}} h_M(n) t^n \in \mathbb{Z}[\![t]\!].$$

Suppose now that the $S/(x_0, \ldots, x_r)$ is Artinian.

(a) Show that there is a $P(t) \in \mathbb{Z}[t]$ such that

$$H_M(t) = \frac{P(t)}{\prod_{i=0}^{r}(1 - t^{d_i})}.$$

In particular, $H_M(t)$ is a rational function of t with poles only at roots of unity.

(b) If $d := \mathrm{lcm}_{i=0}^{r}(d_i)$, then for each $s \in \mathbb{N}$, the function $n \mapsto h_M(dn + s)$ is polynomial-like. (This means that although h_M is not polynomial like, it is polynomial like with periodic coefficients.)

Chapter 2

Primary Decomposition and Local Dimension Theory

In this chapter, we discuss the fundamentals of associated primes and primary decomposition. We do not make any Noetherian hypotheses until we need to. We then prove the Lasker-Noether Theorem, and end with a few applications to Artinian rings and local dimension theory.

2.1 Associated Primes

In this section we introduce the notion of associated primes and discuss basic properties.

Definition 2.1.1. Let R be a ring and M an R-module.

(a) A prime $\mathfrak{p} \subset R$ of R is said to be *associated to* M if the following equivalent conditions hold:
   (i) There is an $m \in M$ such that $\mathfrak{p} = \operatorname{Ann}(m)$.
   (ii) There is an injection of R-modules $R/\mathfrak{p} \hookrightarrow M$.

The set of all primes associated to M is denoted by $\operatorname{Ass}(M) = \operatorname{Ass}_R(M)$.

(b) The minimal elements of $\operatorname{Ass}(M)$ are called *isolated*, and the others are called *embedded* primes.

(c) A $\mathfrak{p} \subset R$ is said to be *associated to an ideal* $\mathfrak{a} \subset R$ if it is associated to the R-module $R/\mathfrak{a}$.

Here are some easy observations.

Observation 2.1.2. Let R be a ring.

(a) The only prime associated to a prime ideal $\mathfrak{p} \subset R$ is $\mathfrak{p}$ itself, i.e., $\operatorname{Ass}(R/\mathfrak{p}) = \{\mathfrak{p}\}$.

(b) For any ideal $\mathfrak{a} \subset R$, we have that $\operatorname{Ass}_R(R/\mathfrak{a}) = \operatorname{Ass}_{R/\mathfrak{a}}(R/\mathfrak{a})$ under the usual identification $\operatorname{Spec}(R/\mathfrak{a}) \cong \mathbb{V}(\mathfrak{a}) \subset \operatorname{Spec} R$.

(c) Let $\mathscr{Z}(M) := \bigcup_{m \in M \smallsetminus \{0\}} \operatorname{Ann}(m)$ be the set of zero-divisors of M in R; then $\bigcup \operatorname{Ass}(M) \subset \mathscr{Z}(M)$.

(d) If $M' \subset M$ is a submodule, then $\operatorname{Ass}(M') \subset \operatorname{Ass}(M)$.

Here are some slightly harder observations.

Lemma 2.1.3. Let R be a ring and M an R-module.

(a) If $\mathscr{A}$ is the collection of ideals of R of the form $\operatorname{Ann}(m)$ for nonzero $m \in M$, then any maximal element of $\mathscr{A}$ is prime.

(b) There is an inclusion $\operatorname{Ass}(M) \subset \operatorname{Supp}(M) \subset \mathbb{V}(\operatorname{Ann} M)$, and equality holds in the latter if M is finitely generated.[1]

(c) If $S \subset R$ is a multiplicative subset, then $\operatorname{Ass}_{S^{-1}R}(S^{-1}M) \supset \operatorname{Ass}_R(M) \cap \operatorname{Spec} S^{-1}R$ under the identification of $\operatorname{Spec} S^{-1}R$ with a subset of $\operatorname{Spec} R$ via 1.1.12(d).

(d) If $0 \to M' \to M \to M'' \to 0$ is a short exact sequence, then

$$\operatorname{Ass}(M') \subset \operatorname{Ass}(M) \subset \operatorname{Ass}(M') \cup \operatorname{Ass}(M'').$$

Proof.

(a) Suppose $\mathfrak{a} = \operatorname{Ann}(m) \in \mathscr{A}$ is maximal and $x, y \in R$ are such that $xy \in \mathfrak{a}$ but $y \notin \mathfrak{a}$. Then $ym \neq 0$ and $\operatorname{Ann}(m) \subset \operatorname{Ann}(ym)$, so by maximality $\operatorname{Ann}(ym) = \operatorname{Ann}(m) = \mathfrak{a}$, whence $xym = 0$ implies $x \in \mathfrak{a}$.

(b) If $\mathfrak{p} = \operatorname{Ann}(m)$ for some nonzero $m \in M$, then $[m] \in M_{\mathfrak{p}}$ is nonzero.[2] For the second part, the inclusion $\operatorname{Supp}(M) \subset \mathbb{V}(\operatorname{Ann} M)$ is clear; for the other, suppose that M is finitely generated and $\mathfrak{p} \in \mathbb{V}(\operatorname{Ann} M)$ but $M_{\mathfrak{p}} = 0$. Then for each of the finitely many generators m_i of M, there is an $s_i \in R \smallsetminus \mathfrak{p}$ such that $s_i m_i = 0$, and then $\prod_i s_i \in \operatorname{Ann}(M) \smallsetminus \mathfrak{p}$, which is a contradiction.

[1] Recall that $\operatorname{Supp}(M)$ is the set of primes $\mathfrak{p} \subset R$ such that $M_{\mathfrak{p}} \neq 0$. Equivalently, $\operatorname{Supp}(M) \subset \operatorname{Spec} R$ is the support of the quasicoherent sheaf $\tilde{M}$ on the affine scheme $\operatorname{Spec} R$.

[2] Equivalently, since $R/\mathfrak{p} \hookrightarrow M$ and $R_{\mathfrak{p}}$ is flat over R, we have $\kappa(\mathfrak{p}) = R_{\mathfrak{p}} \otimes_R R/\mathfrak{p} \hookrightarrow R_{\mathfrak{p}} \otimes_R M = M_{\mathfrak{p}}$, and $\kappa(\mathfrak{p})$ is a field.

(c) We show that if $\mathfrak{p} = \operatorname{Ann}(m)$ for some $0 \neq m \in M$ and $\mathfrak{p} \cap S = \emptyset$, then $S^{-1}\mathfrak{p} = \operatorname{Ann}([m])$ for $0 \neq [m] \in S^{-1}M$. The inclusion $S^{-1}\mathfrak{p} \subset \operatorname{Ann}([m])$ is clear. For the converse, suppose that $(s^{-1}x)[m] = 0$ for some $s \in S$ and $x \in R$; then $txm = 0$ for some $t \in S$. Since $t \notin \mathfrak{p}$ but $tx \in \mathfrak{p}$, we must have $x \in \mathfrak{p}$.

(d) The first inclusion is clear. For the second, if $\mathfrak{p} \in \operatorname{Ass}(M) \smallsetminus \operatorname{Ass}(M')$, then there is an $m \in M \smallsetminus M'$ such that $\mathfrak{p} = \operatorname{Ann}(m)$, and then we claim that $\mathfrak{p} = \operatorname{Ann}([m])$ for $0 \neq [m] \in M''$. The inclusion $\mathfrak{p} \subset \operatorname{Ann}([m])$ is clear; conversely, if $x \in \operatorname{Ann}([m]) \smallsetminus \mathfrak{p}$, then $xm \in M'$ and $\mathfrak{p} = \operatorname{Ann}(xm) \in \operatorname{Ass}(M')$, a contradiction to hypothesis.[3]

■

Remark 2.1.4.

(a) In 2.1.3(b), the hypothesis of finite generation is necessary for equality to hold in the second inclusion. A simple counterexample otherwise is given by taking $R = \mathbb{Z}$ and $M = \bigoplus_p \mathbb{Z}/p$, where the sum is over all primes $p \in \mathbb{Z}$. Then $\operatorname{Ann} M = 0$ and $(0) \in \mathbb{V}(\operatorname{Ann} M) \smallsetminus \operatorname{Supp}(M)$ because $E_{(0)} = E \otimes_{\mathbb{Z}} \mathbb{Q} = 0$.

(b) In 2.1.3(d), it is *not* always true that if $0 \to M' \to M \to M'' \to 0$ is a short exact sequence of R-modules, then $\operatorname{Ass}(M) = \operatorname{Ass}(M') \cup \operatorname{Ass}(M')$; a simple counterexample otherwise is given by taking $R = \mathbb{Z}$ and the exact sequence to be $0 \to \mathbb{Z} \xrightarrow{2} \mathbb{Z} \to \mathbb{Z}/2 \to 0$. However, see 2.1.5(f).

The notion of associated primes behaves best in the Noetherian setting.

Theorem 2.1.5. Let R be a Noetherian ring and M a nonzero R-module.

(a) The set $\operatorname{Ass}(M)$ is nonempty. It is finite if M is finitely generated.
(b) The map $M \to \prod_{\mathfrak{p} \in \operatorname{Ass}(M)} M_{\mathfrak{p}}$ is injective.
(c) We have $\bigcup \operatorname{Ass}(M) = \mathscr{Z}(M)$.
(d) Equality holds in 2.1.3(c).
(e) The sets of minimal elements of $\operatorname{Ass}(M)$ and $\operatorname{Supp}(M)$ coincide; in other words, every prime in $\operatorname{Supp}(M)$ that is minimal with respect to inclusion is an associated prime.
(f) If $0 \to M' \to M \to M'' \to 0$ is a short exact sequence, then $\operatorname{Ass}(M'') \smallsetminus \operatorname{Supp}(M') \subset \operatorname{Ass}(M)$.

Part (e) says in particular that, when M is finitely generated (or more generally when $\operatorname{Supp} M$ is closed), the isolated primes associated to M are exactly the minimal elements in (e.g., the generic points of the irreducible components of) the support of M; therefore, in this case, we have $\operatorname{Supp}(M) = \overline{\operatorname{Ass}(M)}$. Parts (c) and (e) combined for $M = R$ recover 1.2.12 when R is Noetherian. If R is not Noetherian, then it is possible that $\operatorname{Ass}(M)$ is empty for nonzero M; see 10.6.6.

Proof.

(a) That $\operatorname{Ass}(M)$ is nonempty is immediate from 2.1.3(a) and the Noetherian hypothesis. For the finiteness when M is finitely generated, we show that there is an integer $n \geq 1$ and sequence of submodules $0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n = M$ with each successive quotient of the form $M_i/M_{i-1} \cong R/\mathfrak{p}_i$ for some prime $\mathfrak{p}_i \subset R$; then by 2.1.2(a) and 2.1.3(d), it would follow that $\operatorname{Ass}(M) \subset \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$. To show this, note that since $\operatorname{Ass}(M)$ is nonempty, there is a prime $\mathfrak{p}_1$ and an injection $R/\mathfrak{p}_1 \hookrightarrow M$. Take M_1 to be the image of this map. If

[3] Alternatively, one can argue as follows. Suppose $\mathfrak{p} \in \operatorname{Ass}(M)$ and pick $m \in M$ so that $\mathfrak{p} = \operatorname{Ann}(m)$. Replace the triple (M, M', M'') by $(Rm, Rm \cap M', Rm/(Rm \cap M'))$ to reduce to the case of a short exact sequence of the form $0 \to \mathfrak{a}/\mathfrak{p} \to R/\mathfrak{p} \to R/\mathfrak{a} \to 0$ for some $\mathfrak{a} \subset R$ with $\mathfrak{p} \subset \mathfrak{a}$. Now we note simply that if $\mathfrak{p} \neq \mathfrak{a}$, then for any $x \in \mathfrak{a} \smallsetminus \mathfrak{p}$ we have that $\operatorname{Ann}_R([x]_{\mathfrak{a}/\mathfrak{p}}) = \mathfrak{p}$.

$M_1 = M$ we are done; else apply this procedure to M/M_1 and continue recursively. Since M is Noetherian, this procedure must eventually terminate.

(b) If the kernel is nonzero, then by (a) it has an associated prime, which is then associated to M as well (by 2.1.2(d)). This gives us an element $0 \neq m \in M$ with $\mathfrak{p} = \operatorname{Ann}(m)$ but $[m] = 0 \in M_{\mathfrak{p}}$, which can't happen.

(c) The inclusion $\bigcup \operatorname{Ass}(M) \subset \mathscr{Z}(M)$ is 2.1.2(c). For the other inclusion, if $r \in \mathscr{Z}(M)$ then $r \in \operatorname{Ann}(m)$ for some $0 \neq m \in M$. Then the submodule $Rm \subset M$ is nonzero, so by (a) there is an $s \in R$ such that $\mathfrak{p} = \operatorname{Ann}(sm)$. Then $\mathfrak{p}$ is also associated to M (Lemma 2.1.2(d)) and

$$r \in \operatorname{Ann}(m) \subset \operatorname{Ann}(sm) = \mathfrak{p} \subset \bigcup \operatorname{Ass}(M).$$

The second statement follows from the first along with (a) and prime avoidance (1.2.14(b)).

(d) Let $\mathfrak{p} \in \operatorname{Ass}_{S^{-1}R}(S^{-1}M) \subset \operatorname{Spec} S^{-1}R \subset \operatorname{Spec} R$, so there are $s \in S, m \in M$ with $S^{-1}\mathfrak{p} = \operatorname{Ann}(s^{-1}m)$. Clearly, $\operatorname{Ann}(m) \subset \mathfrak{p}$ and for each $x \in \mathfrak{p}$, there is a $t \in S$ such that $tx \in \operatorname{Ann}(m)$. By the Noetherian hypothesis, if $x_1, \ldots, x_n$ are generators for $\mathfrak{p}$ and $t_1, \ldots, t_n$ as mentioned, then it is easy to see that $\mathfrak{p} = \operatorname{Ann}(tm)$ for $t = \prod_{i=1}^n t_i$.

(e) For any prime $\mathfrak{p} \subset R$, by (d), the set $\operatorname{Ass}_{R_{\mathfrak{p}}}(M_{\mathfrak{p}}) = \operatorname{Ass}(M) \cap \operatorname{Spec} R_{\mathfrak{p}}$ consists of primes $\mathfrak{q} \in \operatorname{Ass}(M) \subset \operatorname{Supp}(M)$ contained in $\mathfrak{p}$. Therefore, if $\mathfrak{p} \in \operatorname{Supp}(M)$ is a minimal element, then either $\operatorname{Ass}_{R_{\mathfrak{p}}}(M_{\mathfrak{p}}) = \emptyset$ or $\operatorname{Ass}_{R_{\mathfrak{p}}}(M_{\mathfrak{p}}) = \{\mathfrak{p}\}$, and the former cannot hold thanks to (a).

(f) Let $\mathfrak{p} \in \operatorname{Ass}(M'') \smallsetminus \operatorname{Supp}(M')$. Pick an $m \in M$ such that $\mathfrak{p} = \operatorname{Ann}([m]_{M''})$, and replace the triple (M, M', M'') by $(Rm, Rm \cap M', R[m]_{M''})$ to reduce to the case of a short exact sequence of the form $0 \to \mathfrak{p}/\mathfrak{a} \to R/\mathfrak{a} \to R/\mathfrak{p} \to 0$ for some $\mathfrak{a} \subset \mathfrak{p} \subset R$. Then $(\mathfrak{p}/\mathfrak{a})_{\mathfrak{p}} = 0$ along with the fact that $\mathfrak{p}$ is finitely generated implies there is an $s \in R \smallsetminus \mathfrak{p}$ such that $s\mathfrak{p} \subset \mathfrak{a}$; then $\operatorname{Ann}([s]_{R/\mathfrak{a}}) = \mathfrak{p}$.

■

Corollary 2.1.6. Let R be a Noetherian ring, M a finitely generated R-module, and $\mathfrak{a} \subset R$ an ideal. Then either $\mathfrak{a}$ contains a nonzerodivisor for M, or $\mathfrak{a} \subset \operatorname{Ann}(m)$ for some $0 \neq m \in M$.

Proof. Combine 2.1.5(a) and (c) with prime avoidance (1.2.14(b)). ■

Finally, let us study how associated primes behave on changing the base ring.

Theorem 2.1.7. Let $\varphi : R \to S$ be a ring homomorphism. For any S-module M, we have that $(\operatorname{Spec} \varphi)(\operatorname{Ass}_S(M)) \subset \operatorname{Ass}_R(\varphi_* M)$, with equality if S is Noetherian.

Proof. For any $m \in M$, we have $\operatorname{Ann}_R(m) = \varphi^{-1}(\operatorname{Ann}_S(m))$, which gives the first inclusion. For the second, let $m \in M$ be such that $\operatorname{Ann}_R(m)$ is prime; then from 1.2.13 applied to the extension $R/\operatorname{Ann}_R(m) \hookrightarrow S/\operatorname{Ann}_S(m)$, there is a prime $\mathfrak{q}$ of S minimal over $\operatorname{Ann}_S(m)$ such that $\varphi^{-1}(\mathfrak{q}) = \operatorname{Ann}_R(m)$. By 2.1.3(b) and 2.1.5(e) applied to the finitely generated S-module Sm, the prime $\mathfrak{q}$ is associated to Sm and hence to M. ■

Remark 2.1.8. Taking $R = \mathbb{R}$ and $S = \mathcal{C}(\mathbb{R}, \mathbb{R}) = M$ as in 10.6.6(a) gives a simple counterexample to the previous theorem when S is not Noetherian.

2.2 Primary Decomposition and the Lasker-Noether Theorem

In this section we discuss primary submodules (and hence ideals) and prove the existence of primary decompositions, deducing in particular the Lasker-Noether theorem. We then show the uniqueness of the isolated primes and discuss the kinds of uniqueness statements possible for embedded primes.

Proposition/Definition 2.2.1 (Primary Submodules)**.** Let R be a ring, M an R-module and $N \subsetneq M$ a proper submodule.

- Consider the following conditions.
  (a) For all $x \in R$ and $m \in M$ if $xm \in N$ then either $m \in N$ or there is an $n \geq 1$ such that $x^n M \subset N$.
  (b) We have $\mathscr{Z}(M/N) \subset \sqrt{\operatorname{Ann}(M/N)}$.
  (c) The ideal $\sqrt{\operatorname{Ann}(M/N)}$ is prime and $\operatorname{Ass}(M/N) \subset \{\sqrt{\operatorname{Ann}(M/N)}\}$.
  (d) There is a unique prime associated to M/N.
  Then (a) ⇔ (b) ⇒ (c). Further, if R is Noetherian and M is finitely generated, then also (c) ⇒ (d) ⇒ (b), so all conditions are equivalent.
- A submodule $N \subset M$ is said to be *primary* if it is proper and satisfies the equivalent conditions (a) and (b). If $\mathfrak{p} := \sqrt{\operatorname{Ann}(M/N)}$, then we say that N is *primary to prime* $\mathfrak{p}$ or simply $\mathfrak{p}$-primary.
- If $N \subset M$ is a primary submodule and $\operatorname{Ass}(M/N)$ is nonempty (e.g., if R is Noetherian and M finitely generated), then in fact $\mathscr{Z}(M/N) = \sqrt{\operatorname{Ann}(M/N)}$.

Proof.

(a) ⇔ (b) Clear.

(b) ⇒ (c) Let $x, y \in R$ and $n \geq 1$ be such that $(xy)^n \in \operatorname{Ann}(M/N)$. If $y \notin \sqrt{\operatorname{Ann}(M/N)}$, then there is an $m \in M$ such that $y^n m \notin N$. By (a) we conclude that $x^n \in \sqrt{\operatorname{Ann}(M/N)}$, whence $x \in \sqrt{\operatorname{Ann}(M/N)}$. Now suppose $\mathfrak{p} \in \operatorname{Ass}(M/N)$; then by 2.1.3(b) we have

$$\sqrt{\operatorname{Ann}(M/N)} \subset \mathfrak{p} \subset \bigcup \operatorname{Ass}(M/N) \subset \mathscr{Z}(M/N) \subset \sqrt{\operatorname{Ann}(M/N)}.$$

Now suppose that R is Noetherian and M is finitely generated.

(c) ⇒ (d) Clear from 2.1.5(a).

(d) ⇒ (b) Suppose $\operatorname{Ass}(M/N) = \{\mathfrak{p}\}$. By 2.1.5(c), we have $\mathscr{Z}(M/N) = \mathfrak{p}$. By 1.2.2, it suffices to show that if $\mathfrak{q}$ is a prime containing $\operatorname{Ann}(M/N)$, then $\mathfrak{q} \supset \mathfrak{p}$. By 1.2.10, $\mathfrak{q}$ contains a minimal prime over $\operatorname{Ann}(M/N)$, but by 2.1.5(e) (combined with 2.1.3(b)), this minimal prime is $\mathfrak{p}$.

■

In the special case of $M = R$, primary *ideals* are the primary objects of study. Unpacking the definition above says that if R is a ring an $\mathfrak{a} \subset R$ is an ideal, then $\mathfrak{a}$ is primary iff for every $x, y \in R$, if $xy \in \mathfrak{a}$, then either $x \in \mathfrak{a}$ or $y \in \sqrt{\mathfrak{a}}$. Thus, primary ideals generalize the definition of prime ideals in the sense that every prime ideal is visibly primary (to itself).

Lemma 2.2.2 (Primary Ideals)**.** Let R be a ring.

(a) A proper ideal $\mathfrak{a} \subset R$ is primary iff every zero divisor in $R/\mathfrak{a}$ is nilpotent, so primes are primary.
(b) If $\mathfrak{a} \subset R$ is primary then $\sqrt{\mathfrak{a}}$ is the unique minimal prime containing $\mathfrak{a}$ and $\mathfrak{a}$ is $\sqrt{\mathfrak{a}}$-primary.
(c) If $\mathfrak{m} \subset R$ is a maximal ideal, then an ideal $\mathfrak{a} \subset R$ is $\mathfrak{m}$-primary iff $\sqrt{\mathfrak{a}} = \mathfrak{m}$. If further R is Noetherian, then this is equivalent to saying that there is an $n \in \mathbb{Z}_{\geq 1}$ such that $\mathfrak{m}^n \subset \mathfrak{a} \subset \mathfrak{m}$.

(d) Let $S \subset R$ be a multiplicative subset and $\eta : R \to S^{-1}R$ the localization map. The maps $\mathfrak{a} \mapsto S^{-1}\mathfrak{a}$ and $\mathfrak{A} \mapsto \eta^{-1}\mathfrak{A}$ give an inverse bijection between primary ideals of R disjoint from S and those of $S^{-1}R$. Under this correspondence, $S^{-1}\sqrt{\mathfrak{a}} = \sqrt{S^{-1}\mathfrak{a}}$.

(e) Let $\mathfrak{p} \subset R$ be a prime and $\eta : R \to R_\mathfrak{p}$ the localization. The maps in (d) for $S = R \smallsetminus \mathfrak{p}$ give a bijection between primary ideals of R primary to a prime contained in $\mathfrak{p}$ and those of $R_\mathfrak{p}$.

Therefore, the correspondence in (d) strictly generalizes 1.1.12(d). It will be further generalized in 2.2.12.

Proof.

(a) Clear.

(b) Follows from 1.2.2.

(c) For the nontrivial bit, suppose that $\mathfrak{a} \subset R$ has $\sqrt{\mathfrak{a}} = \mathfrak{m}$ and that $x, y \in R$ are such that $xy \in \mathfrak{a}$ but $y \notin \sqrt{\mathfrak{a}} = \mathfrak{m}$. Then $\mathfrak{m} + (y) = (1)$ so $m + ry = 1$ for some $m \in \mathfrak{m}$ and $r \in R$. Since $m \in \sqrt{\mathfrak{a}}$, there is an $n \geq 1$ such that $m^n \in \mathfrak{a}$. Then $1 = 1^n = (m + ry)^n = m^n + sy$ for some $s \in R$, so $x = xm^n + sxy \in \mathfrak{a}$.

(d) In light of 1.1.12, it only remains to be shown that if $\mathfrak{a} \subset R$ is a primary ideal such that $\mathfrak{a} \cap S = \emptyset$, then $\eta^{-1}(S^{-1}\mathfrak{a}) \subset \mathfrak{a}$, which is clear by definition.

(e) Follows from (d).

■

Example 2.2.3.

(a) If R is a PID, then the primary ideals of R are (0) and (p^r) for p prime and $r \geq 1$ (Exercise 2.4).

(b) In general, if R is a ring, $\mathfrak{p} \subset R$ a prime, and $r \geq 1$, then $\mathfrak{p}^r$ need not be $\mathfrak{p}$-primary (2.5), although condition always holds when $\mathfrak{p}$ is maximal (2.2.2(c)). The prime powers also need not be the only primary ideals; for instance, if $R = k[X, Y]$, then the ideal $\mathfrak{a} = (X, Y^2)$ is a primary ideal that is not a prime power.

(c) The best replacement in (b) are the *symbolic powers*. Namely, if R is a ring and $\mathfrak{p} \subset R$ a prime ideal, then for each integer $n \geq 1$, we define the n^{th} *symbolic power* of $\mathfrak{p}$ to be $\mathfrak{p}^{(n)} := \eta^{-1}(\mathfrak{p}^n R_\mathfrak{p}) = \{x \in R : sx \in \mathfrak{p}^n \text{ for some } s \notin \mathfrak{p}\}$, where $\eta : R \to R_\mathfrak{p}$ is the localization map. Then $\mathfrak{p}^n \subset \mathfrak{p}^{(n)} \subset \mathfrak{p}$ for each n, we have $\mathfrak{p} = \mathfrak{p}^{(1)} \supset \mathfrak{p}^{(2)} \supset \cdots$, and each $\mathfrak{p}^{(n)}$ is $\mathfrak{p}$-primary (check!).

The goal now is a *primary decomposition* of an arbitrary submodule $N \subset M$.

Definition 2.2.4 (Primary Decomposition)**.** Let R be a ring and M an R-module. Let $N \subsetneq M$ be a submodule.

(a) A *primary decomposition* of N is an expression of the form

$$N = N_1 \cap N_2 \cap \cdots \cap N_r$$

where $r \geq 1$ is an integer and $N_1, \ldots, N_r$ are primary submodules of M.

(b) For $i = 1, \ldots, r$, let $\mathfrak{p}_i := \sqrt{\operatorname{Ann}(M/N_i)}$, so that each N_i is $\mathfrak{p}_i$-primary. The above primary decomposition is said to be *minimal* if the $\mathfrak{p}_i$ are pairwise distinct and N is not the intersection of any proper collection of $\{N_1, \ldots, N_r\}$; in this case, we call the N_i *primary components* of (this minimal primary decomposition of) N.

The existence and uniqueness of a primary decomposition is best achieved in the Noetherian setting. This is convenient, as the following lemma shows.

Lemma 2.2.5. Let R be a Noetherian ring and M a finitely generated R-module.

(a) Suppose that $\mathfrak{p} \subset R$ is a prime, $r \geq 1$ an integer, and $N_1, \dots, N_r \subset M$ submodules which are $\mathfrak{p}$-primary. Then the intersection $N_1 \cap \dots \cap N_r$ is also $\mathfrak{p}$-primary.

(b) If $N \subsetneq M$ is a submodule that admits a primary decomposition, then it admits a minimal primary decomposition. In fact, any primary decomposition of N gives rise to a minimal primary decomposition.

Proof.

(a) By 2.1.3(d) and 2.1.5(a),

$$\emptyset \subsetneq \operatorname{Ass}\left(M/\bigcap_i N_i\right) \subset \operatorname{Ass}\left(\bigoplus_i M/N_i\right) \subset \bigcup_i \operatorname{Ass}(M/N_i) = \{\mathfrak{p}\}.$$

(b) Consider the primary decomposition of N which involves the least number r of factors; by (a), this must be minimal.[4]

■

We are ready for the main existence theorem.

Theorem 2.2.6 (Primary Decomposition: Existence)**.** Let R be a Noetherian ring and M a finitely generated R-module. Every propery submodule of M admits a minimal primary decomposition.

Proof. We say that a submodule $N \subset M$ is *irreducible* if it is proper and it cannot be written as $N = N_1 \cap N_2$ for some submodules $N_1, N_2 \subset M$ with $N \subsetneq N_1$ and $N \subsetneq N_2$.[5] From Noetherian induction, it is clear that every proper submodule of N can be written as an intersection of irreducible submodules; therefore, we will finish by showing that every irreducible $N \subset M$ is primary. For this suppose that $N \subset M$ is a proper submodule that is not primary; we have to show that N is not irreducible. Replacing M by M/N, we may assume $N = (0)$. To say that (0) is not primary implies by 2.2.1(d) that there are two distinct primes $\mathfrak{p}_1, \mathfrak{p}_2$ associated to M, so that there are elements $x_1, x_2 \in M$ with $R/\mathfrak{p}_i \cong Rx_i \hookrightarrow M$ for $i = 1, 2$. It remains to check (do!) that if $y_i \in Rx_i$ is any nonzero element, then $\operatorname{Ann}(y_i) = \mathfrak{p}_i$; then it follows that $Rx_1 \cap Rx_2 = (0)$, so that (0) is reducible. ■

Applying this to $M = R$ immediately yields

Corollary 2.2.7 (Lasker-Noether)**.** Every proper ideal of a Noetherian ring admits a minimal primary decomposition.

Finally, we turn to uniqueness; here the picture cannot be too nice, as evidenced by the following example.

Example 2.2.8.

(a) (Line with Embedded Point) Let k be a field, $R = k[X, Y]$ and $\mathfrak{a} = (X^2, XY)$. Then $\sqrt{\mathfrak{a}} = (X)$, and so $XY \in \mathfrak{a}$ but $X \notin \mathfrak{a}$ and $Y \notin \sqrt{\mathfrak{a}}$ shows that $\mathfrak{a}$ is not primary. Indeed,

[4] Equivalently, but more constructively, given a primary decomposition, we may discard redundant N_i and use (a) to intersect all the remaining N_i that are primary to the same prime; iterating this procedure finitely many times yields a minimal primary decomposition.

[5] When $M = R$, an ideal $\mathfrak{a} \subset R$ is irreducible according to this definition iff the closed subset $\mathbb{V}(\mathfrak{a}) \subset \operatorname{Spec} A$ is irreducible as a topological space.

two minimal primary decompositions of $\mathfrak{a}$ are seen to be

$$\mathfrak{a} = (X, Y)^2 \cap (X) = (X^2, Y) \cap (X),$$

where in each case the first ideal is (X, Y)-primary (embedded) and the second is (X)-primary (isolated).

(b) (Quadric Cone) Let k be a field, $R = k[x, y, z] := k[X, Y, Z]/(XY - Z^2)$ and $\mathfrak{p} = (x, z)$. Then even though $\sqrt{\mathfrak{p}^2} = \mathfrak{p}$, the ideal $\mathfrak{p}^2$ is not primary (2.5(a)), and indeed we have

$$\mathfrak{p}^2 = (x) \cap (x, y, z)^2,$$

where the first ideal is $\mathfrak{p}$-primary, and the second ideal is (x, y, z)-primary. In particular, in the primary decomposition of the ideal $\mathfrak{p}^2$, we have the "embedded point" (x, y, z) showing up.

Nonetheless, we do have some uniqueness statements–this is where associated primes come in.

Theorem 2.2.9 (Primary Decomposition: Uniqueness I)**.** Let R be a Noetherian ring, M a finitely generated R-module and $N \subset M$ a proper submodule. If $r \geq 1$ and submodules $N_1, \dots, N_r \subset M$ are such that $N = N_1 \cap \dots \cap N_r$ is a minimal primary decomposition with $\mathfrak{p}_i := \sqrt{\operatorname{Ann}(M/N_i)}$ for $i = 1, \dots, r$, then

$$\operatorname{Ass}(M/N) = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_r\}.$$

In particular, the prime ideals occuring in any minimal primary decomposition of N are uniquely determined by N.

Proof. Replacing M by M/N, we may assume $N = 0$. First suppose that $\mathfrak{p} \in \operatorname{Ass}(M)$, so there is a $0 \neq m \in M$ with $\mathfrak{p} = \operatorname{Ann}(m)$. By relabelling if needed, pick a j with $1 \leq j \leq r$ such that $m \in (N_{j+1} \cap \dots \cap N_r) \smallsetminus (N_1 \cup \dots \cup N_j)$. By the Noetherian hypothesis, there is an integer $k \gg 1$ such that $\mathfrak{p}_i^k \cdot M \subset N_i$ for all $i = 1, \dots, r$, so that $\bigcap_{i=1}^j \mathfrak{p}_i^k \subset \operatorname{Ann}(m) = \mathfrak{p}$. By 1.2.14(a), there is an i with $1 \leq i \leq j$ such that $\mathfrak{p}_i \subset \mathfrak{p}$. We claim that equality must hold; indeed, if $x \in \mathfrak{p}$, then $xm = 0$ but $m \notin N_i$ implies that $x \in \mathfrak{p}_i$ by the primary hypothesis.

For the other direction, we'll show $\mathfrak{p}_1 \in \operatorname{Ass}(M)$. Since the decomposition of N is reduced, there is an $m \in \bigcap_{i=2}^r N_i \smallsetminus N_1$. Let $k \geq 1$ be the smallest integer such that $\mathfrak{p}_1^k \cdot (m) \subset N_1$, and pick a $n \in \mathfrak{p}_1^{k-1}(m) \smallsetminus N_1$. The claim is $\mathfrak{p}_1 = \operatorname{Ann}(n)$. Indeed, $\mathfrak{p}_1 \subset \operatorname{Ann}(n)$ follows from $\bigcap_{i=1}^r N_i = 0$, and if $x \in \operatorname{Ann}(n)$, then $xn = 0$ but $n \notin N_1$ implies by the primary hypothesis that $x \in \mathfrak{p}_1$. ■

Corollary 2.2.10. Let R be a Noetherian ring and $\mathfrak{a} \subset R$ be a proper ideal.

(a) The following conditions on a prime $\mathfrak{p} \subset R$ are equivalent:
  (i) The prime $\mathfrak{p}$ contains $\mathfrak{a}$.
  (ii) The prime $\mathfrak{p}$ contains a prime associated to $\mathfrak{a}$.
  (iii) The prime $\mathfrak{p}$ contains an isolated prime associated to $\mathfrak{a}$.
In other words, the minimal primes containing $\mathfrak{a}$ are exactly the isolated primes of $\mathfrak{a}$, and in particular there are only finitely many of these.

(b) The radical $\sqrt{\mathfrak{a}}$ is the intersection of all the associated primes of $\mathfrak{a}$, and hence all the isolated primes of $\mathfrak{a}$. In particular, $\mathfrak{a}$ is radical iff the primary components of any minimal primary decomposition of $\mathfrak{a}$ are all prime ideals. In this case, there are no embedded primes and the primary decomposition is unique.

(c) There is an integer $n \geq 1$ and not necessarily distinct primes $\mathfrak{p}_1, \dots, \mathfrak{p}_n \subset R$ such that $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subset \mathfrak{a}$.

Proof.

(a) The implications (iii) $\Leftrightarrow$ (ii) $\Rightarrow$ (i) are clear (using 2.1.5(a)-(e) and 2.1.3(b)). For (i) $\Rightarrow$ (ii), by 2.2.7, $\mathfrak{a}$ has a minimal primary decomposition, say of the form $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$ for some $r \geq 1$ with each $\mathfrak{q}_i$ a $\mathfrak{p}_i$-primary ideal for some prime $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$, with each $\mathfrak{p}_i \in \operatorname{Ass}(R/\mathfrak{a})$ by 2.2.9. Then $\mathfrak{a} \subset \mathfrak{p}$ implies by 1.2.14(a) that there is an i with $1 \leq i \leq r$ such that $\mathfrak{q}_i \subset \mathfrak{p}$, whence $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i} \subset \sqrt{\mathfrak{p}} = \mathfrak{p}$.

(b) In the notation of (a), we have $\sqrt{\mathfrak{a}} = \sqrt{\mathfrak{q}_1} \cap \cdots \cap \sqrt{\mathfrak{q}_r} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r$, so we are done by 2.2.9. If the primary components of some minimal primary decomposition of $\mathfrak{a}$ are primes, then $\mathfrak{a}$ is certainly radical; conversely, if $\mathfrak{a}$ is radical, then it is the intersection of its associated primes: say $\mathfrak{a} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r$. We claim that this expression is the only minimal primary decomposition of $\mathfrak{a}$ (upto rearrangement). Indeed, the integer r in this decomposition is uniquely determined as $\# \operatorname{Ass}(R/\mathfrak{a})$ from 2.2.9, whence $\mathfrak{a}$ does not admit a primary decomposition with fewer than r primes; from this reducedness of this decomposition follows, as well as the fact that there are no embedded primes associated to $\mathfrak{a}$. Finally, if $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$ is any other minimal primary decomposition, then again by 2.2.9 we have $s = r$, and after rearranging if needed we can assume $\sqrt{\mathfrak{q}_i} = \mathfrak{p}_i$ for each $i = 1, \ldots, r$. By reducedness, for each i, there is an $x \in \bigcap_{j \neq i} \mathfrak{p}_j \setminus \mathfrak{p}_i$; then if $y \in \mathfrak{p}_i$, then $xy \in \mathfrak{a} \subset \mathfrak{q}_i$ and $x \notin \mathfrak{p}_i$ with $\mathfrak{q}_i$ being $\mathfrak{p}_i$-primary implies that $y \in \mathfrak{q}_i$, showing that in fact $\mathfrak{q}_i = \mathfrak{p}_i$.

(c) Since R is Noetherian, there is an integer $m \geq 1$ such that $(\sqrt{\mathfrak{a}})^m \subset \mathfrak{a}$, so we are done by (b).

■

We should note also that 2.2.10(c) can be deduced very directly by Noetherian induction (2.9). Finally, we turn to the final version of uniqueness. For this, we will need some more preparation on how primary components interact with localization.

Lemma 2.2.11. Let R be a ring and $S \subset R$ a multiplicative subset. M an R-module, and $N \subset M$ a primary submodule, primary to the prime $\mathfrak{p} \subset R$. Suppose $S \subset R$ is a multiplicative subset.

(a) If $S \cap \mathfrak{p} \neq \emptyset$, then $S^{-1}N = S^{-1}M$.

(b) If $S \cap \mathfrak{p} = \emptyset$, then $S^{-1}N \subset S^{-1}M$ is primary to the prime $S^{-1}\mathfrak{p}$. In fact, if $\eta : M \to S^{-1}M$ is the localization map, then $N = \eta^{-1}(S^{-1}N)$.

Proof. Exercise. ■

This yields a complete picture of what the operation $N \mapsto \eta^{-1}S^{-1}M$ does to submodules of a module M under localization by S as follows.

Theorem 2.2.12. Let R be a Noetherian ring, M a finitely generated R-module, and $N \subsetneq M$ a proper submodule. Suppose we are given a minimal primary decomposition of N of the form

$$N = N_1 \cap \cdots \cap N_r$$

for some $r \in \mathbb{Z}_{\geq 1}$ and primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \subset R$ such that each N_i is $\mathfrak{p}_i$-primary. Let $S \subset R$ be a multiplicatively closed subset. Then $S^{-1}N \subset S^{-1}M$ is proper iff there is some i such that $\mathfrak{p}_i \cap S = \emptyset$. In this case, suppose further that $s \in \mathbb{Z}$ with $1 \leq s \leq r$ is chosen so that $\mathfrak{p}_i \cap S = \emptyset$ for $1 \leq i \leq s$ and $\mathfrak{p}_i \cap S \neq \emptyset$ for $s < i \leq r$. Then

$$S^{-1}N = S^{-1}N_1 \cap \cdots \cap S^{-1}N_s$$

is a minimal primary decomposition of $S^{-1}N$ in $S^{-1}M$ with $S^{-1}N$ a $S^{-1}\mathfrak{p}_i$-primary ideal for each i with $1 \leq i \leq s$. Further, if $\eta : M \to S^{-1}M$ is the localization map, then $\eta^{-1}S^{-1}N \subset M$ is proper and in fact

$$\eta^{-1}(S^{-1}N) = N_1 \cap \cdots \cap N_s$$

is a minimal primary decomposition of the submodule $\eta^{-1}(S^{-1}N) \subset M$.

Proof. Follows immediately from the previous lemma (2.2.11). We only note that the fact that $S^{-1}N = S^{-1}N_1 \cap \cdots \cap S^{-1}N_s$ is a minimal primary decomposition follows from the previous lemma and 1.1.12(d) combined with the facts that $\eta^{-1}(S^{-1}N) = N_1 \cap \cdots \cap N_s$ and that $N = N_1 \cap \cdots \cap N_r$ is a minimal primary decomposition. ■

Theorem 2.2.13 (Primary Decomposition: Uniqueness II)**.** Let R be a Noetherian ring, M a finitely generated R-module and $N \subset M$ a proper submodule. The primary submodules in a minimal primary decomposition which correspond to isolated primes of M/N are determined uniquely by N.

Proof. Suppose we are given a minimal primary decomposition $N = N_1 \cap \cdots \cap N_r$ for some $r \in \mathbb{Z}_{\geq 1}$ as above with corresponding primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$. Then, as noted in 2.2.9 above, we have $\operatorname{Ass}(M/N) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ so that the primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are determined uniquely by N. Now, after relabelling if needed, suppose that $\mathfrak{p} = \mathfrak{p}_1$ corresponds to an isolated prime of M/N, i.e., is a minimal element of $\operatorname{Ass}(M/N)$. In 2.2.12 above, taking $S := R \smallsetminus \mathfrak{p}$ shows us that $N_1 = \eta^{-1}S^{-1}N$ where $\eta : M \to S^{-1}M$ is the localization map. Since the $\mathfrak{p}_i$ are uniquely determined by N, this tells us that so is the primary submodule N_1 as needed. ■

We cannot, in fact, do better–the embedded components are far from being uniquely determined (2.12).

2.3 Artinian Rings Revisited, Ideals of Definition, and the Hilbert-Samuel Polynomial

Let us discuss some applications of primary decomposition here. The first one is to finish our discussion on Artinian rings. For this, we'll need one more piece of terminology: if R is a ring, we will denote by $\operatorname{mSpec} R$ its maximal spectrum, i.e. the set of its maximal ideals. The first result then is

Theorem 2.3.1. Let R be a Noetherian ring and M be a finitely generated R-module. The following conditions are equivalent:

(a) M is Artinian.
(b) The length $\ell_R(M)$ of M is finite.
(c) $\operatorname{Ass}(M) \subset \operatorname{mSpec} R$, i.e., every prime associated to M is maximal.
(d) $\operatorname{Supp}(M) \subset \operatorname{mSpec} R$, i.e., M is supported on maximal ideals.
(e) We have $\dim M = 0$.[6]

In this case, $\operatorname{Ass}(M) = \operatorname{Supp}(M)$.

Proof. Since M is Noetherian, (a) ⇔ (b) is the content of 1.3.4, (d) ⇒ (c) follows from 2.1.3(b) and (c) ⇒ (d) follows from 2.1.5(e). Also, (e) is clearly equivalent to $\mathbb{V}(\operatorname{Ann} M) \subset \operatorname{mSpec} R$, and so (d) ⇔ (e) follows from 2.1.3(b).

For the rest, we choose, using the proof of 2.1.5(a), an integer $n \geq 1$ and a sequence of submodules $0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n = M$ with each successive quotient of the form $M_i/M_{i-1} \cong R/\mathfrak{p}_i$ for some prime $\mathfrak{p}_i$. We claim that

$$\operatorname{Ass}(M) \subset \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} \subset \operatorname{Supp}(M).$$

The first of these inclusions was shown in the proof of 2.1.5(a); for the second one, note that for each $i = 1, \ldots, n$, we have

$$0 \neq \operatorname{Frac}(R/\mathfrak{p}_i) \cong (R/\mathfrak{p}_i)_{\mathfrak{p}_i} \cong (M_i/M_{i-1})_{\mathfrak{p}_i} \cong (M_i)_{\mathfrak{p}_i}/(M_{i-1})_{\mathfrak{p}_i},$$

whence $(M_i)_{\mathfrak{p}_i} \subset M_{\mathfrak{p}_i}$ is nonzero. Finally, by the additivity of length (10.1.6) $\ell_R(M)$ is finite iff for each $i = 1, \ldots, n$, the length $\ell_R(R/\mathfrak{p}_i) = \ell_{R/\mathfrak{p}_i}(R/\mathfrak{p}_i)$ is finite, which happens iff $\mathfrak{p}_i$ is maximal (by 1.3.4 and 1.3.9(a)); this directly proves (d) ⇒ (b) ⇒ (c). Then 2.1.5(e) implies in this case that $\operatorname{Ass}(M) = \operatorname{Supp}(M)$. ■

In particular, if R is an Artinian ring and M a finitely generated R-module, then $\ell_R(M) < \infty$, so that M is also Noetherian (using 1.3.4); this gives another proof of 1.3.10. Finally, from this result we immediately obtain the required characterization of Artinian rings.

Corollary 2.3.2. For a ring R, the following are equivalent:

(a) R is Artinian.
(b) The length $\ell_R(R)$ is finite.
(c) R is Noetherian of dimension zero, i.e., $\operatorname{Spec} R = \operatorname{mSpec} R$.
(d) R is Noetherian and $\operatorname{Ass}(R) \subset \operatorname{mSpec} R$.

Proof. Combine 1.3.10, 1.3.4, and 2.3.1. ■

Let us now revisit some dimension theory.

[6] Recall that $\dim M := \dim R/\operatorname{Ann} M$, where the latter denotes the Krull dimension.

Proposition/Definition 2.3.3 (Ideals of Definition)**.** Let $(R, \mathfrak{m})$ be a Noetherian local ring. For an ideal $\mathfrak{a} \subset R$, the following conditions are equivalent.

(a) The $\mathfrak{a}$-adic topology on R is the same as the $\mathfrak{m}$-adic topology.
(b) There is an $N \geq 1$ such that $\mathfrak{m}^N \subset \mathfrak{a} \subset \mathfrak{m}$.
(c) The radical $\sqrt{\mathfrak{a}} = \mathfrak{m}$.
(d) The ideal $\mathfrak{a}$ is $\mathfrak{m}$-primary, i.e., the only prime associated to $\mathfrak{a}$ is $\mathfrak{m}$.
(e) The only prime containing $\mathfrak{a}$ is $\mathfrak{m}$, i.e., $\mathfrak{m}$ is a minimal prime over $\mathfrak{a}$.
(f) The Krull dimension $\dim R/\mathfrak{a} = 0$.
(g) The ring $R/\mathfrak{a}$ is Artinian.
(h) The length $\ell_R(R/\mathfrak{a}) < \infty$.

Any ideal $\mathfrak{a} \subset R$ satisfying these equivalence conditions is called an *ideal of definition.*

(i) For any integer $n \geq 1$, the ideal $\mathfrak{a}^n$ is also an ideal of definition.
(j) Any proper ideal containing $\mathfrak{a}$ is also an ideal of definition.
(k) If M is a finitely generated R-module, then $M/\mathfrak{a}M$ is a finitely generated $R/\mathfrak{a}$-module, and hence both Noetherian and Artinian and satisfies $\ell_R(M/\mathfrak{a}M) = \ell_{R/\mathfrak{a}}(M/\mathfrak{a}M) < \infty$.

Proof.

(a) ⇔ (b) Clear from the definition of the $\mathfrak{a}$-adic topology.
(b) ⇔ (c) The ring R is Noetherian.
(c) ⇔ (d) This is 2.2.2(c).
(d) ⇔ (e) One direction is 2.2.2(b); the other is 2.2.10(a).
(e) ⇔ (f) Clear.
(f) ⇔ (g) ⇔ (h) This is 2.3.2, noting that $\ell_R(R/\mathfrak{a}) = \ell_{R/\mathfrak{a}}(R/\mathfrak{a})$.

Then (i) and (j) follow from (b), and (k) is clear from the above discussion. ■

Definition 2.3.4 (Hilbert-Samuel Polynomial)**.** Let $(R, \mathfrak{m})$ be a Noetherian local ring, $\mathfrak{a} \subset R$ an ideal of definition, and M a finitely generatd R-module. Define the *Hilbert-Samuel* function of M with respect to $\mathfrak{a}$ to be the function $S_M^{\mathfrak{a}} : \mathbb{N} \to \mathbb{N}$ given by

$$S_M^{\mathfrak{a}}(n) := \ell_R(M/\mathfrak{a}^n M).$$

Theorem 2.3.5. Suppose we are in the same set-up as 2.3.4.

(a) The function $S_M^{\mathfrak{a}}$ is polynomial-like of degree independent of the choice of $\mathfrak{a}$. In fact, if $\mathfrak{a}$ is generated by at most $r \in \mathbb{Z}_{\geq 1}$ elements, then $\deg S_M^{\mathfrak{a}} \leq r$.
(b) If $0 \to M' \to M \to M'' \to 0$ is a short exact sequence of finitely generated R-modules, then
$$\deg S_M^{\mathfrak{a}} = \max\{\deg S_{M'}^{\mathfrak{a}}, \deg S_{M''}^{\mathfrak{a}}\}.$$
In fact, $S_M^{\mathfrak{a}} = S_{M'}^{\mathfrak{a}} + S_{M''}^{\mathfrak{a}} + R$ for some R polynomial-like of degree less than $\deg S_M^{\mathfrak{a}}$.

Proof.

(a) For each $n \in \mathbb{N}$, the short exact sequence $0 \to \mathfrak{a}^n M/\mathfrak{a}^{n+1}M \to M/\mathfrak{a}^{n+1}M \to M/\mathfrak{a}^n M \to 0$ tells us
$$\Delta^{[1]} S_M^{\mathfrak{a}}(n) = \ell_R(\mathfrak{a}^n M/\mathfrak{a}^{n+1}M) = \ell_{\mathrm{gr}_{\mathfrak{a}}(R)_0}(\mathrm{gr}_{\mathfrak{a}}(M)_n) = h_{\mathrm{gr}_{\mathfrak{a}}(M)}(n),$$
which is polynomial-like of degree at most $r - 1$ by 1.6.12; we are then done by 1.6.10. If $N \geq 1$ is chosen so that $\mathfrak{m}^N \subset \mathfrak{a} \subset \mathfrak{m}$, then we have for all $n \in \mathbb{N}$ that $S_M^{\mathfrak{m}}(Nn) \geq S_M^{\mathfrak{a}}(n) \geq S_M^{\mathfrak{m}}(n)$, which tells us that the degree of $S_M^{\mathfrak{a}}$ is independent of the choice of $\mathfrak{a}$.

(b) For $n \in \mathbb{N}$, we have $M''/\mathfrak{a}^n M'' \cong M/(M' + \mathfrak{a}^n M)$ as R-modules and hence

$$\begin{aligned} S_M^{\mathfrak{a}}(n) &= \ell_R(M/\mathfrak{a}^n M) \\ &= \ell_R(M/(M' + \mathfrak{a}^n M)) + \ell_R((M' + \mathfrak{a}^n M)/\mathfrak{a}^n M) \\ &= S_{M''}^{\mathfrak{a}}(n) + \ell_R(M'/(M' \cap \mathfrak{a}^n M)). \end{aligned}$$

Let $T : \mathbb{N} \to \mathbb{N}$ be the function defined by $T(n) := \ell_R(M'/(M' \cap \mathfrak{a}^n M))$. It follows from (a) that T is polynomial-like; since all terms take only positive values, we also conclude $\deg S_M^{\mathfrak{a}} = \max\{\deg S_{M''}^{\mathfrak{a}}, \deg T\}$. By the Artin-Rees Lemma (1.6.20(b)), there is an $m \in \mathbb{N}$ such that for all $n \in \mathbb{N}_{\geq m}$ we have

$$\mathfrak{a}^n M' \subset M' \cap \mathfrak{a}^n M = \mathfrak{a}^{n-m}(M' \cap \mathfrak{a}^m M) \subset \mathfrak{a}^{n-m} M'$$

and hence $S_{M'}^{\mathfrak{a}}(n) \geq T(n) \geq S_{M'}^{\mathfrak{a}}(n-m)$. Therefore, $\deg T = \deg S_{M'}^{\mathfrak{m}}$, and $S_{M'}^{\mathfrak{m}}$ and T share the same leading coefficient. In particular, the difference $R = T - S_{M'}^{\mathfrak{a}}$ is polynomial like of degree less than $\deg S_{M'}^{\mathfrak{a}} \leq \deg S_M^{\mathfrak{a}}$.

■

2.4 The Main Theorem of Local Dimension Theory

For the rest of this section, let $(R, \mathfrak{m})$ be a Noetherian local ring, and M a finitely generated R-module.

We have three reasonable notions of the *dimension* of M:

(a) The Krull dimension $\dim M := \dim R/\operatorname{Ann} M = \sup_{\mathfrak{p}\in\mathbb{V}(\operatorname{Ann} M)} \operatorname{coht}\mathfrak{p} = \sup_{\mathfrak{p}\in\operatorname{Ass}(M)} \operatorname{coht}\mathfrak{p}$.[7]

(b) The degree of the Hilbert-Samuel function with respect to any ideal of definition: $\mathrm{d}(M) := \deg S_M^{\mathfrak{m}}$.[8]

(c) The *Chevalley dimension* $\delta(M)$, defined to be the minimum number $r \in \mathbb{N}$ of elements $a_1, \ldots, a_r \in \mathfrak{m}$ such that $\dim M/(a_1, \ldots, a_r)M = 0$.[9]

On indication that these three notions are reasonable and comparable is given by

Lemma 2.4.1. The following are equivalent.

(a) $M = 0$.
(b) $\dim M = -1$.
(c) $\mathrm{d}(M) = -1$.
(d) $\delta(M) = -1$.

Similarly, the following conditions on a nonzero M are equivalent.

(a) M is an Artinian R-module, i.e., $\ell_R(M) < \infty$.
(b) $\dim M = 0$.
(c) $\mathrm{d}(M) = 0$.
(d) $\delta(M) = 0$.

Proof. For the first part, the only nontrivial implication is (c) $\Rightarrow$ (a): if $\mathrm{d}(M) = -1$, then for $n \gg 0$ we have $\ell_R(M/\mathfrak{a}^n M) = 0$, so that $M = \mathfrak{a}^n M$, and we are done by 1.5.3(b). For the second part, (a) $\Leftrightarrow$ (b) is 2.3.1 and (a) $\Leftrightarrow$ (d) is clear. For (a) $\Leftrightarrow$ (c), we have $\mathrm{d}(M) = 0$ iff $\Delta^1 S_M^{\mathfrak{m}}(n) = h_{\mathrm{gr}_{\mathfrak{m}}(M)}(n)$ is zero for $n \gg 1$, which by Nakayama (1.5.3) happens iff $\mathfrak{m}^n M = 0$ for $n \gg 0$. This is equivalent to saying that $\operatorname{Ann} M$ is an ideal of definiton, which in turn is equivalent to $\dim M = 0$ by 2.3.3. ■

At this point, the following result is not too surprising.

Theorem 2.4.2. In the above set-up, we always have $\dim M = \mathrm{d}(M) = \delta(M)$.

Proof. By the previous lemma, we may assume $M \neq 0$. We will show $\dim M \leq \mathrm{d}(M) \leq \delta(M) \leq \dim M$.

Step 1. For $\dim M \leq \mathrm{d}(M)$, note that since $\operatorname{Ass}(M)$ is finite and nonempty (2.1.5), there is a prime $\mathfrak{p} \in \operatorname{Ass}(M)$ such that $\dim M = \dim R/\mathfrak{p}$. Since $R/\mathfrak{p} \hookrightarrow M$, we have by 2.3.5 that $\mathrm{d}(R/\mathfrak{p}) \leq \mathrm{d}(M)$. Therefore, it suffices to do the case when $M = R/\mathfrak{p}$ for a prime $\mathfrak{p} \subset R$. For this, we prove by induction on $n \in \mathbb{Z}_{\geq 0}$ that if $\mathfrak{p}_n \subsetneq \cdots \subsetneq \mathfrak{p}_0$ is a chain of primes in R, then $n \leq \mathrm{d}(R/\mathfrak{p}_n)$, with the case $n = 0$ being trivial. When $n \geq 1$, pick an $x \in \mathfrak{p}_{n-1} \smallsetminus \mathfrak{p}_n$, and using 2.1.5 pick a prime $\mathfrak{q}$ associated to the ideal $\mathfrak{p}_n + xR$, so that $\mathfrak{p}_n \subsetneq \mathfrak{p}_n + xR \subset \mathfrak{q} \subset \mathfrak{p}_{n-1}$. By induction, $n - 1 \leq \mathrm{d}(R/\mathfrak{q})$ and by 2.3.5(b) we have

[7] The last equality follows from 2.1.5(e). By convention in this circle of ideas, we define the Krull dimension of the zero ring to be -1.

[8] Recall the convention mentioned in 1.6.9.

[9] By convention, we define $\delta(0) = -1$. Note that $\delta(M)$ is finite because if M is nonzero, then $\dim M/\mathfrak{m}M = \dim R/\mathfrak{m} = 0$, so $\delta(M)$ is less than the embedding dimension of R.

$\mathrm{d}(R/\mathfrak{q}) \leq \mathrm{d}(R/(\mathfrak{p}_n + xR))$. From the short exact sequence

$$0 \to R/\mathfrak{p}_n \xrightarrow{\cdot x} R/\mathfrak{p}_n \to R/(\mathfrak{p}_n + xR) \to 0,$$

it follows again from 2.3.5(b) that $\mathrm{d}(R/(\mathfrak{p}_n + xR)) \leq \mathrm{d}(R/\mathfrak{p}_n) - 1$, finishing the proof.

Step 2. For $\mathrm{d}(M) \leq \delta(M)$, we proceed by induction on $\delta(M)$, with the case $\delta(M) = 0$ being covered by 2.4.1. Suppose now that $\delta(M) = r \in \mathbb{Z}_{\geq 1}$, and pick $a_1, \ldots, a_r \in \mathfrak{m}$ with $\ell_R(M/(a_1, \ldots, a_r)M) < \infty$. For i with $0 \leq i \leq r$, let $M_i := M/(a_1, \ldots, a_i)M$, so that clearly $\delta(M_i) = r - i$. For any $n \in \mathbb{N}$,

$$S^{\mathfrak{m}}_{M_1}(n) = \ell_R(M_1/\mathfrak{m}^n M_1) = \ell_R(M/(a_1 M + \mathfrak{m}^n M)) = S^{\mathfrak{m}}_M(n) - \ell_R(a_1 M/(a_1 M \cap \mathfrak{m}^n M)).$$

When $n \geq 1$, multiplication by a_1 gives a surjection $M/\mathfrak{m}^{n-1}M \twoheadrightarrow a_1 M/(a_1 M \cap \mathfrak{m}^n M)$, so that this last quantity is at most $S^{\mathfrak{m}}_M(n-1)$. In all, we have shown for $n \geq 1$ that

$$S^{\mathfrak{m}}_{M_1}(n) \geq S^{\mathfrak{m}}_M(n) - S^{\mathfrak{m}}_M(n) = \Delta^1 S^{\mathfrak{m}}_M(n-1),$$

so that $\mathrm{d}(M_1) \geq \mathrm{d}(M) - 1$. Therefore, $r - 1 = \delta(M_1) \geq \mathrm{d}(M_1) \geq \mathrm{d}(M) - 1$, as needed.

Step 3. For $\delta(M) \leq \dim M$, again we proceed by induction on $\dim M$ with 2.4.1 dealing with $\dim M = 0$. Now suppose $\dim M > 0$. The set $S := \{\mathfrak{p} \in \mathrm{Ass}(M) : \operatorname{coht} \mathfrak{p} = \dim M\}$ is nonempty and finite. Since $\mathfrak{m} \notin S$, prime avoidance (1.2.14) produces an $x \in \mathfrak{m} \smallsetminus \bigcup S$. Let $N := M/xM$. Since $N_{\mathfrak{p}} = 0$ for all $\mathfrak{p} \in S$, we have $\mathrm{Supp}(N) \subset \mathrm{Supp}(M) \smallsetminus S$, so that $\dim N \leq \dim M - 1$. The proof is finished after noting that $\delta(M) \leq \delta(N) + 1$, which is clear by definition.

■

Let's now look at some fun consequences of this hard work.

Corollary 2.4.3.

(a) Let R be a Noetherian local ring. Every R-module has finite Krull dimension, and $\dim R$ is the minimal number of generators of an ideal of definition of R. In particular, $\dim R \leq \operatorname{edim} R < \infty$.
(b) For any field k and $n \in \mathbb{Z}_{\geq 0}$, we have $\dim k[\![X_1, \ldots, X_n]\!] = n$.
(c) If R is a Noetherian ring, then every prime of R has finite height, and so primes of R satisfy the descending chain condition.

Geometrically, (a) says that for any $n \in \mathbb{Z}_{\geq 0}$, a codimension n closed subscheme of a locally Noetherian scheme can be set-theoretically cut out by precisely n equations. There exist infinite-dimensional Noetherian rings (which must necessarily be non-local); see 10.6.5.

Proof.

(a) The quantity $\delta(R)$ is evidently the minimal number of generators of an ideal of definition of R; taking one such ideal to be $\mathfrak{m}$ and using 1.5.4 finishes the proof.
(b) The inequality $k[\![X_1, \ldots, X_n]\!] \geq n$ was noted above (1.2.17(e)); the other one follows from (a).
(c) Clear from (a).

■

Another classical consequence is the generalized Krull's Hauptidealsatz.

Theorem 2.4.4 (Generalized Krull's Hauptidealsatz)**.** For an integer $n \geq 0$, a prime ideal in a Noetherian ring has height at most n iff it is minimal over an ideal generated by at most n elements.

Geometrically, 2.4.4 says that for any $n \in \mathbb{Z}_{\geq 0}$, a closed subscheme of codimension n in an affine Noetherian scheme (or, by minor modifications, in projective space) is an irreducible component of a subscheme cut out by at most n equations; conversely, any irreducible component of a closed subscheme cut out by at most n equations has codimension at most n. For instance, an affine or projective hypersurface can be cut out by one global equation, and any irreducible component of a subscheme cut out by one equation is a hypersurface (i.e., has codimension 1).

Proof 1. For a Noetherian ring R, prime $\mathfrak{p} \subset R$, and $n \in \mathbb{N}$, we have $\operatorname{ht} \mathfrak{p} = \dim R_{\mathfrak{p}} \leq n$ iff there is an ideal of definition say $\mathfrak{a} \subset R_{\mathfrak{p}}$ generated by at most n elements by 2.4.3(a). The contraction $\mathfrak{a} \cap R$ is also generated by at most n elements; then since $\mathfrak{p}R_{\mathfrak{p}}$ is minimal over $\mathfrak{a}$ (2.3.3(e)), it follows that $\mathfrak{p}$ is minimal over $\mathfrak{a} \cap R$. Conversely, if $\mathfrak{a}$ is an ideal generated by at most n elements and $\mathfrak{p}$ a minimal prime over it, then $\mathfrak{a}R_{\mathfrak{p}}$ is an ideal of definition of $R_{\mathfrak{p}}$ generated by at most n elements, and so we are again done by 2.4.3(a). ■

Another, more elementary proof can be given as follows.

Proof 2. Let R be a Noetherian ring, $\mathfrak{p} \subset R$ a prime.

First suppose $\operatorname{ht} \mathfrak{p} = n \in \mathbb{N}$. If $n = 0$, then $\mathfrak{p}$ is minimal. If $n \geq 1$, then prime avoidance (1.2.14) gives us an $x \in \mathfrak{p}$ not contained in any minimal prime of R. It follows that in the quotient $R/(x)$, we have $\operatorname{ht} \mathfrak{p}/(x) \leq n-1$. By induction, $\mathfrak{p}/(x)$ is minimal over an ideal generated by at most $n-1$ elements; taking preimages and appending x shows that $\mathfrak{p}$ is minimal over a prime generated by at most n elements.

Conversely, let $n \in \mathbb{N}$, and let $\mathfrak{p}$ be minimal over an ideal generated by n elements, say $x_1, \ldots, x_n \in R$; we want to show $\operatorname{ht} \mathfrak{p} \leq n$. The case $n = 0$ is trivial. Let's do $n = 1$, so $\mathfrak{p}$ is minimal over $x = x_1$, and we have to show that if $\mathfrak{q} \subsetneq \mathfrak{p}$ is any prime, then $\operatorname{ht} \mathfrak{q} = 0$. By localizing at $\mathfrak{p}$, we may assume that $(R, \mathfrak{p})$ is local. Since the ring $R/(x)$ has only one prime, namely $\mathfrak{p}/(x)$, it follows that $\dim R/(x) = 0$. From 2.3.2, it follows that $R/(x)$ is Artinian. Therefore, if $\mathfrak{q} \subsetneq \mathfrak{p}$ is any prime, then the sequence $(\mathfrak{q}^{(n)} + (x))/(x)$ of symbolic powers of $\mathfrak{q}$ (2.2.3(c)) taken in $R/(x)$ eventually stabilizes. In particular, there is an integer $n \geq 1$ such that $\mathfrak{q}^{(n)} + (x) = \mathfrak{q}^{(n+1)} + (x)$. We claim that this means that $\mathfrak{q}^{(n)} = \mathfrak{q}^{(n+1)} + x\mathfrak{q}^{(n)}$. Indeed, if $y \in \mathfrak{q}^{(n)}$, then by the above there is a $z \in \mathfrak{q}^{(n+1)}$ and a $w \in R$ such that $y = z + xw$. Since $x \notin \mathfrak{q}$ by minimality of $\mathfrak{p}$, we have $xw = y - z \in \mathfrak{q}^{(n)}$, and $\mathfrak{q}^{(n)}$ is $\mathfrak{q}$-primary (2.2.3(c)), we conclude that $w \in \mathfrak{q}^{(n)}$, finishing the proof of the claim. Since $x \in \mathfrak{p} = \operatorname{Jac}(R)$, we may now apply 1.5.3(c) to conclude that $\mathfrak{q}^{(n)} = \mathfrak{q}^{(n+1)}$. Using 1.1.12(b), we then conclude that $\mathfrak{q}^n R_{\mathfrak{q}} = \mathfrak{q}^{(n)} R_{\mathfrak{q}} = \mathfrak{q}^{(n+1)} R_{\mathfrak{q}} = \mathfrak{q}^{n+1} R_{\mathfrak{q}}$, and so again by 1.5.3(b), this time applied to $R_{\mathfrak{q}}$, we conclude that $\mathfrak{q}^n R_{\mathfrak{q}} = 0$. It then follows from 10.4(b) and 2.3.2 that $R_{\mathfrak{q}}$ is Artinian and that $\operatorname{ht} \mathfrak{q} = \dim R_{\mathfrak{q}} = 0$.

Finally suppose $n \geq 2$. Again by localizing at $\mathfrak{p}$, we may assume that $(R, \mathfrak{p})$ is local. Let $\mathscr{A}$ denote the collection of all primes strictly contained in $\mathfrak{p}$. Since $\mathfrak{p}$ is finitely generated, every chain in $\mathscr{A}$ has an upper bound. If $\mathscr{A}$ is empty, then $\mathfrak{p}$ is minimal and so $\operatorname{ht} \mathfrak{p} = 0$. Else, by Zorn's Lemma, there is a maximal element $\mathfrak{q} \in \mathscr{A}$. By the minimality of $\mathfrak{p}$ over $(x_1, \ldots, x_n)$, this prime $\mathfrak{q}$ cannot contain all the x_i; after reordering if needed, we may assume that $x_1 \notin \mathfrak{q}$. Since every prime containing $\mathfrak{q} + (x_1)$ is between $\mathfrak{q}$ and $\mathfrak{p}$, it follows from 1.2.2 that $\sqrt{\mathfrak{q} + (x_1)} = \mathfrak{p}$. Therefore, for each i with $2 \leq i \leq n$, there is an $n_i \in \mathbb{Z}_{\geq 1}$ and elements $y_i \in \mathfrak{q}$ and $z_i \in R$ such that $x_i^{n_i} = y_i + x_1 z_i$. Now in the quotient ring $\overline{R} := R/(y_2, \ldots, y_n)$, every minimal prime over $\overline{x}_1$ contains all the $\overline{x}_i$'s and is hence $\overline{\mathfrak{p}}$, i.e., that $\overline{\mathfrak{p}}$ is minimal over the principal ideal $(\overline{x}_1)$. It follows by the case $n = 1$ done above that $\operatorname{ht} \overline{\mathfrak{p}} = 1$, so that $\operatorname{ht} \overline{\mathfrak{q}} = 0$, i.e., $\mathfrak{q}$ is minimal over $(y_2, \ldots, y_n)$. It follows by induction that $\operatorname{ht} \mathfrak{q} \leq n-1$. By the maximality of $\mathfrak{q}$ in $\mathscr{A}$, we then conclude that $\operatorname{ht} \mathfrak{p} \leq n$. ■

Corollary 2.4.5. Let R be a Noetherian ring.

(a) If $x \in R$ is not a zero-divisor, then every minimal prime over (x) has height one. If, in addition, R is local and x a non-unit, then $\dim R/(x) = \dim R - 1$.
(b) More generally, if R is local, M a nonzero finitely-generated R-module, and $x \in R$ an element which is neither a unit and nor a zero-divisor for M, then $\dim M \geq 1$ and $\dim M/xM = \dim M - 1$.

Proof.

(a) Any prime containing x cannot have height zero by 1.2.12. For the second statement, since (x) is proper, 1.2.10 combined with the first part tells us that $\dim R \geq 1$ and $\dim R/(x) \leq \dim R - 1$. The other inequality follows immediately from 2.4.3(a).
(b) If $\dim M = 0$, then by 2.3.1 we conclude that $\emptyset \subsetneq \operatorname{Ass}(M) \subset \{\mathfrak{m}\}$, so that by 2.1.5(c) we have $x \in \mathfrak{m} = \bigcup \operatorname{Ass}(M) = \mathscr{Z}(M)$, contrary to hypothesis. Next, $\operatorname{Ann}(M/xM) \supset \operatorname{Ann} M + (x)$, so that

$$\dim M/xM \leq \dim R/(\operatorname{Ann} M + (x)) = \dim(R/\operatorname{Ann} M)/(\overline{x}) = \dim M - 1,$$

by part (a), since $\overline{x} \in R/\operatorname{Ann} M$ is a non-unit non-zero-divisor (because $\mathscr{Z}(M) \supset \mathscr{Z}(R/\operatorname{Ann} M)$). The other inequality follows as above from $\delta(M) \leq \delta(M/xM) + 1$.

■

We end this section by a discussion of systems of parameters. As above, let $(R, \mathfrak{m})$ be a Noetherian local ring and M a nonzero finitely generated R-module of dimension say $n = \dim M \in \mathbb{N}$.

Definition 2.4.6. A *system of parameters* for M is a collection of n elements $a_1, \ldots, a_n \in \mathfrak{m}$ such that $\dim M/(a_1, \ldots, a_n)M = 0$.

Example 2.4.7.

(a) A system of parameters for $M = R$ is a set of generators of an ideal of definition of size $\dim R$ ("the right number of equations which cut out the maximal ideal set-theoretically").
(b) The collection $\{X_1, \ldots, X_n\}$ is a system of parameters for both the rings $k[X_1, \ldots, X_n]_{(X_1, \ldots, X_n)}$ and $k[\![X_1, \ldots, X_n]\!]$.

Theorem 2.4.8. Given any $r \in \mathbb{N}$ and elements $a_1, \ldots, a_r \in \mathfrak{m}$, we have $\dim M/(a_1, \ldots, a_r)M \geq n - r$, with equality iff $\{a_1, \ldots, a_r\}$ can be completed to a system of parameters for M. In particular, if $x \in R$ is neither a unit nor a zero-divisor for M, then x belongs to a system of parameters for M.

Proof. The second statement follows from the first and 2.4.5(b). Let $N := M/(a_1, \ldots, a_r)M$. The inequality $\delta(M) \leq \delta(N) + r$ is clear and gives us the first part when combined with 2.4.2. If $a_1, \ldots, a_r$ can be completed to a system of parameters say $a_1, \ldots, a_n$, then

$$0 = \dim M/(a_1, \ldots, a_n)M = \dim N/(a_{r+1}, \ldots, a_n)N \geq \dim N - (n - r) \geq 0.$$

Conversely, if equality holds, then again by 2.4.2, there are $a_{r+1}, \ldots, a_n \in \mathfrak{m}$ with

$$\dim N/(a_{r+1}, \ldots, a_n)N = 0,$$

and then $a_1, \ldots, a_n$ is a system of parameters for M. ■

2.5 Regular (Local) Rings I

In 2.4.3(a), we saw that the Krull dimension of a Noetherian local ring is bounded above by its embedding dimension. Rings for which equality holds form a particularly nice class of rings; this is one algebraic analog of smoothness of algebraic varieties ([5, 13.2.7]).

Definition 2.5.1. (Regular Rings) Let R be a ring.

(a) Let R be local. We say that R is *regular* iff R is Noetherian and $\dim R = \operatorname{edim} R$.
(b) In general, we say that R is *regular* iff it is Noetherian and for every prime $\mathfrak{p} \subset R$, the localization $R_{\mathfrak{p}}$ is a regular local ring.

Remark 2.5.2. In a regular local ring R, a system of parameters for R is called a *regular system of parameters*. Therefore, if $(R, \mathfrak{m}, k)$ is a regular local ring, then a collection of elements of $\mathfrak{m}$ forms a regular system of parameters for R iff their reductions form a k-basis for $\mathfrak{m}/\mathfrak{m}^2$.

Example 2.5.3.

(a) Let R be a regular local ring. If $\dim R = 0$, then $\mathfrak{m} = 0$, and hence R is a field. If $\dim R = 1$, then R is a DVR (7.1.7).
(b) Let k be a field, $n \in \mathbb{N}$, and let $R := k[\![X_1, \ldots, X_n]\!]$. Then 2.4.3(b) tells us that R is a complete regular local ring of dimension n, with $\{X_1, \ldots, X_n\}$ serving as a regular system of parameters. Conversely, the Cohen Structure Theorem (see [6, 0323]) tells us that these are all the complete regular local rings which contain a field.
(c) Let k be a field, and let $R = k[x, y] := k[X, Y]/(Y^2 - X^3)$, which has dimension one by 5.2.4. If $\mathfrak{p} = (x - 1, y - 1)$, then $R_{\mathfrak{p}}$ is regular; if $\mathfrak{p} = (x, y)$, then $R_{\mathfrak{p}}$ is not.
(d) Let $(R, \mathfrak{m})$ be a regular local ring of dimension $n \geq 1$. For $x \in R$, we have $x \in \mathfrak{m} \smallsetminus \mathfrak{m}^2$ iff the quotient $R/(x)$ is a regular local ring of dimension $n - 1$. Using 1.5.5, we see that if $x \in \mathfrak{m} \smallsetminus \mathfrak{m}^2$, then

$$n - 1 \leq \delta(R/(x)) = \dim R/(x) \leq \operatorname{edim} R/(x) = \operatorname{edim} R - 1 = n - 1.$$

Conversely, if $R/(x)$ is a regular local ring of dimension $n - 1 \geq 0$, then x is not a unit and hence $x \in \mathfrak{m}$, and also $x \notin \mathfrak{m}^2$ because $\operatorname{edim} R/(x) = n - 1$.

Here's one helpful way to check when a ring is regular.

Lemma 2.5.4. (Slicing Criterion for Regularity) Let R be a Noetherian local ring an $x \in R$ a non-unit nonzerodivisor. If $R/(x)$ is regular, then so is R.

Proof. By 2.4.5(a) and 1.5.5, we get $\dim R = \dim R/(x) + 1 = \operatorname{edim} R/(x) + 1 \geq \operatorname{edim} R$. ■

Given 2.5.3(a), the following is not a surprise.

Theorem 2.5.5. A regular local ring is a domain.

Proof. We induct on $n := \dim R$, with $n = 0$ taken care of by 2.5.3(a). Suppose that $n \geq 1$. By prime avoidance (1.2.14), there is an $x \in \mathfrak{m} \smallsetminus \mathfrak{m}^2$ which is not in any of the minimal prime ideals of R. Then $R/(x)$ is a regular local ring of dimension $n - 1$ by 2.5.3(d), and hence a domain by induction. This tells us that $(x) \subset R$ is a prime. Picking a minimal prime of the nonzero ring $R_{(x)}$ gives us a minimal prime $\mathfrak{p}$ of R with $\mathfrak{p} \subset (x)$, which forces $\mathfrak{p} = x\mathfrak{p}$ since $x \notin \mathfrak{p}$. Then Nakayama (1.5.3) tells us that $\mathfrak{p} = 0$, which implies in particular that R is a domain. ■

Generalizing 2.5.3(d), we have

Theorem 2.5.6. Let $(R, \mathfrak{m}, k)$ be a regular local ring of dimension $n \in \mathbb{N}$. Let $r \in \mathbb{N}_{\leq n}$ and $a_1, \ldots, a_r \in \mathfrak{m}$ be arbitrary. The following are equivalent.

(a) The collection $a_1, \ldots, a_r$ is part of a regular system of parameters.
(b) The classes $\overline{a}_1, \ldots, \overline{a}_r$ are k-linearly independent in $\mathfrak{m}/\mathfrak{m}^2$.
(c) The quotient $R/(a_1, \ldots, a_r)$ is regular local of dimension $n - r$.

Proof.

(a) ⇔ (b) Follows from 2.5.2.

(a) ⇒ (c) By 2.4.8, $\dim R/(a_1, \ldots, a_r) = n - r$.[10] If we complete the a_i to a system of parameters by appending $a_{r+1}, \ldots, a_n$, then the images $\overline{a}_{r+1}, \ldots, \overline{a}_n$ generate the maximal ideal of the quotient $R/(a_1, \ldots, a_r)$, whence $\operatorname{edim} R/(a_1, \ldots, a_r) \leq n - r$, and so $R/(a_1, \ldots, a_r)$ is regular.

(c) ⇒ (a) Picking a regular system of parameters for the quotient $R/(a_1, \ldots, a_r)$, lifting to R, and appending to $a_1, \ldots, a_r$ yields a regular system of parameters.

■

Next, we compare the regularity of R with that of $R[X]$. (The corresponding comparison for $R[\![X]\!]$ will be done later in [TODO].)

Theorem 2.5.7. Let $(R, \mathfrak{m})$ be a regular local ring of dimension $n \in \mathbb{N}$. Let $\mathfrak{p}$ be a prime of $R[X]$ lying over $\mathfrak{m}$. Then $R[X]_\mathfrak{p}$ is a regular local ring of dimension either n or $n + 1$.

Proof. ([5, 13.3.7]) Pick a regular system of parameters $a_1, \ldots, a_n$ for R, as well as a chain of primes $0 \subsetneq \mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_n = \mathfrak{m}$ of R of length n. By hypothesis, $\mathfrak{m}R[X] \subset \mathfrak{p}$.

(a) If $\mathfrak{p} = \mathfrak{m}R[X]$, then the sequence $0 \subsetneq \mathfrak{q}_1 R[X]_\mathfrak{p} \subsetneq \cdots \subsetneq \mathfrak{q}_n R[X]_\mathfrak{p}$ is a chain of primes of $R[X]_\mathfrak{p}$ of length n and hence $\dim R[X]_\mathfrak{p} \geq n$. Since the maximal ideal $\mathfrak{p}R[X]_\mathfrak{p}$ is generated by the n elements $a_1, \ldots, a_n$, we conclude that $\operatorname{edim} R[X]_\mathfrak{p} \leq n$ and that $R[X]_\mathfrak{p}$ is a regular local ring of dimension n.

(b) If $\mathfrak{p}$ strictly contains $\mathfrak{m}R[X]$, then our understanding of the primes of $R[X]/\mathfrak{m}R[X] = (R/\mathfrak{m})[X]$ tells us that $\mathfrak{p}$ is of the form $(\mathfrak{m}, f)$ for some monic polynomial $f \in R[X]$ whose reduction in $(R/\mathfrak{m})[X]$ is irreducible. Again, $0 \subsetneq \mathfrak{q}_1 R[X]_\mathfrak{p} \subsetneq \cdots \subsetneq \mathfrak{q}_n R[X]_\mathfrak{p} \subsetneq \mathfrak{p}R[X]_\mathfrak{p}$ is a chain of primes of $R[X]_\mathfrak{p}$ of length $n + 1$, and hence $\dim R_\mathfrak{p} \geq n + 1$. Since the maximal ideal $\mathfrak{p}R[X]_\mathfrak{p}$ is generated by the $n + 1$ elements $a_1, \ldots, a_n, f$, we conclude that $\operatorname{edim} R[X]_\mathfrak{p} \leq n + 1$ and that $R[X]_\mathfrak{p}$ is a regular local ring of dimension $n + 1$.

■

Corollary 2.5.8.

(a) If R is a regular ring, then so is $R[X]$.
(b) If k is a field, then for any $n \in \mathbb{N}$, the ring $k[X_1, \ldots, X_n]$ is regular.

Proof. Clearly, (b) follows from (a). First note that if R is regular, then R is Noetherian, and hence so is $R[X]$ by 1.3.5. Let $\mathfrak{p} \subset R$ be a prime of $R[X]$, and let $\mathfrak{q} := \mathfrak{p} \cap R$. Since $R[X]_\mathfrak{p} = R_\mathfrak{q}[X]_{\mathfrak{p}R_\mathfrak{q}[X]}$, we may assume without loss of generality that R is local and that $\mathfrak{p}$ lies over $\mathfrak{m}$. Then we are done by 2.5.7. ■

Two further results on regular rings we mention now will be proven later: that regular local rings are UFDs ([TODO]), and that a localization of a regular local ring is again regular

[10] Happily there is no clash of notation here: the Krull dimension of the R-module $R/(a_1, \ldots, a_r)$ *is* the Krull dimension of the ring $R/(a_1, \ldots, a_r)$.

([TODO]), which will in turn follow from our homological characterization of regular local rings as those Noetherian local rings with finite global dimension ([TODO]).

2.6 Regular Sequences, Depth, and Cohen-Macaulay Rings

Definition 2.6.1. Let R be a ring and M an R-module.

- A(n) (ordered) sequence $a_1, \dots, a_n \in R$ of elements of R for some $n \in \mathbb{N}$ is said to be *M-regular* or *regular for the module M* iff $(a_1, \dots, a_n)M \neq M$ and for all $i = 1, \dots, n$ we have $a_i \notin \mathscr{Z}(M/(a_1, \dots, a_{i-1})M)$.
- An R-regular sequence is called simply a *regular sequence.*

Example 2.6.2.

(a) For any ring R, an element $x \in R$ forms a regular sequence of length one iff x is a non-unit nonzerodivisor.

(b) Let k be a field and $n \in \mathbb{N}$. If R is either $k[X_1, \dots, X_n]$ or $k[\![X_1, \dots, X_n]\!]$, then $X_1, \dots, X_n$ is a regular sequence.

(c) Order matters: if $R = k[X, Y, Z]$, then $(X, Y(1-X), Z(1-X))$ is a regular sequence, but $(Y(1-X), Z(1-X), X)$ is not. However, see 2.6.4.

Theorem 2.6.3. Let R be a ring, M an R-module, $n \in \mathbb{N}$, and $a_1, \dots, a_n \in R$ an M-regular sequence. Then for any positive integers $r_1, \dots, r_n \in \mathbb{Z}_{\geq 1}$, the sequence $a_1^{r_1}, \dots, a_n^{r_n}$ is still M-regular.

Proof. ([7, Theorem 16.1]) We start with an observation: if $a_1, \dots, a_n \in R$ is an M-regular sequence, and if $m_1, \dots, m_n \in R$ are such that $\sum_{i=1}^n a_i m_i = 0$, then for all $i = 1, \dots, n$, we have $m_i \in (a_1, \dots, a_n)M$. Indeed, since $a_n \notin \mathscr{Z}(M/(a_1, \dots, a_{n-1})M)$, we conclude that $m_n \in (a_1, \dots, a_{n-1})M$, from which the result follows immediately by induction on n.

Returning to the main proof, we note that it suffices to treat the case $r_2 = \cdots = r_n = 1$, which we do by induction on $r := r_1$, with $r = 1$ being obvious. Suppose $r \geq 2$. That $a_1^r \notin \mathscr{Z}(M)$ is clear. If for some $i \geq 2$ and $m \in M$ we have $a_i m \in (a_1^r, \dots, a_{i-1})M$, say $a_i m = a_1^r m_1 + a_2 m + \cdots + a_{i-1} m_{i-1}$ for $m_j \in M$, then by regularity of $a_1^{r-1}, \dots, a_{i-1}, a_i$, we conclude that there are $n_j \in M$ such that $m = a_1^{r-1} n_1 + a_2 n_2 + \cdots + a_{i-1} n_{i-1}$. Then from the equation

$$a_1^{r-1}(a_1 m_1 - a_i n_1) + a_2(m - a_i n_2) + \cdots + a_{i-1}(m_{i-1} - a_i n_{i-1}) = 0,$$

we conclude by the observation above that $a_1 m_1 - a_i n_1 \in (a_1^{r-1}, a_2, \dots, a_{i-1})M$, from which we get $a_i n_1 \in (a_1, \dots, a_{i-1})M$. By the regularity of $a_1, \dots, a_i$, this forces $n_1 \in (a_1, \dots, a_{i-1})M$, and hence that $m \in (a_1^r, \dots, a_{i-1})M$ as required.

■

Theorem 2.6.4. Let R be a Noetherian ring and M a finitely generated R-module. If $n \in \mathbb{N}$ and $a_1, \dots, a_n \in R$ is a regular sequence for M such that $(a_1, \dots, a_n) \subset \operatorname{Jac}(R)$, then every permutation of $a_1, \dots, a_n$ is regular. In particular, this always holds if R is a Noetherian local ring.

For a short argument using spectral sequences, see [5, 9.5.6]. Here we give an elementary proof.

Proof. It suffices to do the case $n = 2$, so suppose $a, b \in R$ form an M-regular sequence. We wish to show two things: that $b \notin \mathscr{Z}(M)$ and $a \notin \mathscr{Z}(M/bM)$.

Step 1. Let $N := (0 :_M b) = M[b]$. By Nakayama (1.5.3), it remains to show that $N \subset aN$. Let $n \in N$. Then $bn = 0 \in aM$, and so $b \notin \mathscr{Z}(M/aM)$ tells us $n \in aM$. Write $n = am$ for $m \in M$. Then $0 = bn = a(bm)$ and $a \notin \mathscr{Z}(M)$ tells us $bm = 0$, i.e., that $m \in N$.

Step 2. If $m \in M$ is such that $am \in bM$, then we want to show that $m \in bM$. If we write $am = bm_1$ for $m_1 \in M$, then $b \notin \mathscr{Z}(M/aM)$ tells us that $m_1 \in aM$, say $m_1 = am_2$ for $m_2 \in M$. Then $a(m - bm_2) = 0$ along with $a \notin \mathscr{Z}(M)$ tells us that $m = bm_2$ as needed.

■

We now define an important algebraic invariant associated to a finitely generated module over a Noetherian local ring. For this, we start with a simple observation.

Lemma 2.6.5. Let R be a Noetherian local ring and M a finitely generated R-module. If $n \in \mathbb{N}$, and $a_1, \ldots, a_n \in R$ is an M-regular sequence, then $n \leq \dim M$, and $a_1, \ldots, a_n$ can be extended to a system of parameters for M.

Proof. Follows immediately using induction from 2.4.5(b) and 2.4.8. ■

Definition 2.6.6. Let R be a Noetherian ring, $\mathfrak{a} \subset R$ an ideal, and M an R-module such that $M \neq \mathfrak{a}M$.

- The *depth of M with respect to* $\mathfrak{a}$, denoted $\operatorname{depth}_{\mathfrak{a}} M$, is the maximal length of an M-regular sequence contained in $\mathfrak{a}$.

If R is further local with maximal ideal $\mathfrak{m}$, then for any nonzero finitely generated R-module M we define the *depth of M* to be $\operatorname{depth} M := \operatorname{depth}_{\mathfrak{m}} M$. By 2.6.5, we have $\operatorname{depth} M \leq \dim M$.

- In the local case, the module M is said to be *Cohen-Macaulay* iff $\operatorname{depth} M = \dim M$. The ring R is said to be *Cohen-Macaulay* if it is Cohen-Macaulay as a module over itself.

Given a ring R, we say that R is *Cohen-Macaulay* R is Noetherian and for every prime $\mathfrak{p} \subset R$, the localization $R_{\mathfrak{p}}$ is Cohen-Macaulay.

We will show later [TODO] that $\operatorname{depth} M$ is the length of *any* maximal regular sequence for M. We will also show later [TODO] that a localization of a Cohen-Macaulay local ring at a prime is again Cohen-Macaulay, so there is no disagreement between the a priori different definitions of a local Cohen-Macaulay ring above. Before we give some examples, we record one easy lemma.

Lemma 2.6.7. Let R be a Noetherian local ring and M a nonzero finitely generated R-module. The following conditions on M are equivalent.

(a) $\operatorname{depth} M = 0$.
(b) $\mathfrak{m} \subset \mathscr{Z}(M)$.
(c) $\mathfrak{m} \in \operatorname{Ass}(M)$.

Proof. The equivalence (a) $\Leftrightarrow$ (b) is clear by definition, (b) $\Rightarrow$ (c) follows from 2.1.6, and (c) $\Rightarrow$ (b) from 2.1.2(c). ■

Example 2.6.8.

(a) An Artinian local ring is Cohen-Macaulay.
(b) A one-dimensional Noetherian local domain is Cohen-Macaulay; this follows from 2.6.7.
(c) We will show in 2.6.9 that regular local rings are Cohen-Macaulay.

The converse to (c) is clearly not true, as, for instance any Artinian local ring that is not a field shows. For a one-dimensional example, take any non-DVR one-dimensional Noetherian local domain (e.g., for a field k, consider the localization of $R := k[x, y] := k[X, Y]/(Y^2 - X^3)$ at the prime $\mathfrak{p} = (x, y)$). For a two-dimensional example, see 2.15.

The relationship of this notion with regularity as in the previous section is given by

Proposition 2.6.9. If $(R, \mathfrak{m})$ is a Noetherian local ring, then R is regular iff $\mathfrak{m}$ can be generated by a regular sequence. In this case, the length of any regular sequence generating $\mathfrak{m}$, and hence any maximal regular sequence, is precisely $\dim R$. In particular, regular local rings are Cohen-Macaulay.

Proof. That a regular system of parameters is a regular sequence follows immediately from 2.5.5 and 2.5.6. Conversely, if $\mathfrak{m}$ is generated by a regular sequence of length $r \in \mathbb{N}$, then 2.6.5 tells us that $r \leq \dim R \leq \operatorname{edim} R \leq r$. In particular, R is regular, and $r = \dim R$. Finally, any regular sequence can be extended to a system of parameters by 2.6.5, and a regular system of parameters is a regular sequence as noted above; therefore, a maximal regular sequence is a system of parameters, and hence has length $\dim R$. ■

In all, in a regular local ring, a (regular) system of parameters is the same thing as a maximal regular sequence. We will revisit local dimension theory using homological methods at the end of the course ([TODO]).

2.7 Serre's Conditions R and S

Definition 2.7.1. Let R be a Noetherian ring. Let $n \in \mathbb{N}$. We say that R satisfies condition

R_n iff for every prime $\mathfrak{p} \subset R$ with $\operatorname{ht} \mathfrak{p} \leq n$, the localization $R_{\mathfrak{p}}$ is a regular local ring; and

S_n iff for every prime $\mathfrak{p} \subset R$, we have $\operatorname{depth} R_{\mathfrak{p}} \geq \min\{n, \operatorname{ht}(\mathfrak{p})\}$.

Clearly, R satisfies S_n for all $n \in \mathbb{N}$ iff it is Cohen-Macaulay.

2.8 Exercises

Exercise 2.1. Let $\varphi : R \to S$ be a morphism of rings with S Noetherian. Show that if $\mathfrak{p}$ is a prime associated to the ideal $\ker\varphi$ (i.e., $\mathfrak{p} \in \operatorname{Ass}(R/\ker\varphi)$), then there is a $\mathfrak{q} \in \operatorname{Ass}_S(S)$ such that $\varphi^{-1}(\mathfrak{q}) = \mathfrak{p}$.

Exercise 2.2. Let R be a UFD.

(a) Suppose $f \in R$ is a prime element. Show that for each $n \in \mathbb{Z}_{\geq 1}$, the ideal $(f)^n$ is (f)-primary, and conversely that these are all the (f)-primary ideals.
(b) Let $\mathfrak{m} \subset R$ be a maximal ideal and $\mathfrak{a} \subset R$ an $\mathfrak{m}$-primary ideal. For any $f \in R$, the prime $\mathfrak{m}$ is an embedded prime of $R/((f) \cap \mathfrak{a})$ iff $f \notin \mathfrak{a}$.
(c) If R is Noetherian, and $0 \neq f \in R$, then every prime associated to $R/(f)$ has height one in R.

Exercise 2.3.

(a) Let R be a UFD and $0 \neq f \in R$. Show that the primes associated to $R/(f)$ are exactly the principal ideals generated by the prime factors of f. Conclude that, in this case, there are no embdded primes associated to $R/(f)$.
(b) Show that a Noetherian domain R is a UFD iff for each $f \in R$, the isolated primes associated to $R/(f)$ are principal ideals in R.

Exercise 2.4. Show that in a PID, nonzero primary ideals are exactly the powers of prime ideals.

Exercise 2.5. Let k be a field, $R = k[x, y, z] := k[X, Y, Z]/(XY - Z^2)$, and $\mathfrak{p} = (x, z)$.

(a) Show that R is a domain and $\mathfrak{p} \subset R$ a prime ideal such that $\mathfrak{p}^2$ is not a primary ideal.
(b) For each integer $n \geq 1$, describe the n^{th} symbolic power $\mathfrak{p}^{(n)}$.

Exercise 2.6. Consider the following conditions on a ring R.

(a) R has a unique minimal prime ideal.
(b) The nilradical $\operatorname{Nil}(R)$ is prime.
(c) The reduction R^{red} is an integral domain.
(d) Every zero-divisor of R is nilpotent.
(e) R is nonzero, and the ideal $(0) \subsetneq R$ is primary.
(f) There is a unique prime associated to the zero ideal $(0) \subset R$.

Show that (a)-(e) are equivalent and immply (f), and if R is Noetherian, then all conditions are equivalent. A ring satisfying equivalent conditions (a)-(e) is said to be *primary* or *irreducible.*[11] Check that a subring or a localization of an irreducible (resp. reduced) ring is irreducible (resp. reduced), and that a ring is an integral domain iff it is reduced and irreducible. Is the quotient of an irreducible ring also always irreducible?

Exercise 2.7. Let R be a primary ring such that $\operatorname{Ass}(R)$ is nonempty (e.g., R is Noetherian). Show that $\mathscr{Z}(R) = \operatorname{Nil}(R)$, i.e., the zero-divisors of R are precisely the nilpotent elements. Show that the hypothesis on $\operatorname{Ass}(R)$ is necessary.

Exercise 2.8. Let R be a primary ring and $S \subset R$ a multiplicative subset. Show that the localization $S^{-1}R$, if not zero, is primary. Does the converse hold in general?

Exercise 2.9. Let R be a Noetherian ring and $\mathfrak{a} \subset R$ a proper ideal. Show directly (i.e., using Noetherian induction and without using primary decomposition) that there is an integer $n \geq 1$

[11] This latter terminology is due to the fact that, geometrically, this corresponds to the affine scheme $\operatorname{Spec} R$ being irreducible. We will use both interchangeably.

and not necessarily distinct primes $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subset R$ such that $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subset \mathfrak{a}$.

The next few exercises (2.10, 2.11, and 2.12) are based on [4, Chapter 8, Exercise 1].

Exercise 2.10. Let R be a Noetherian ring. Suppose $\mathfrak{a} \subset R$ is a $\mathfrak{p}$-primary ideal for some prime $\mathfrak{p}$. Show that there is an $n \in \mathbb{Z}_{\geq 1}$ such that $\mathfrak{p}^{(n)} \subset \mathfrak{a}$.

Exercise 2.11. Let R be a Noetherian ring and $\mathfrak{p} \subset R$ a prime that is *not minimal.* Show that the symbolic powers $\mathfrak{p}^{(n)}$ for $n \in \mathbb{Z}_{\geq 1}$ are all distinct. What happens when $\mathfrak{p}$ is minimal?

Exercise 2.12. Let R be a Noetherian ring. Suppose $(0) = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_r$ is a minimal primary decomposition of (0) in R for some $r \in \mathbb{Z}_{\geq 1}$ with corresponding primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$. Show that if say $\mathfrak{p}_1$ is an isolated prime associated to R, then for all $N \gg 1$, we have $\mathfrak{a}_1 = \mathfrak{p}_1^{(N)}$. (This gives another proof of 2.2.13 in the case of primary decompositions of ideals.) Show that if $\mathfrak{p}_1$ is instead embedded, then in the above primary decomposition we may replace $\mathfrak{a}_1$ with $\mathfrak{p}_1^{(N)}$ for $N \gg 1$ to get infinitely many *distinct* primary components corresponding to the prime $\mathfrak{p}_1$, i.e., infinitely many distinct primary decompositions of (0).

Exercise 2.13. Let R be a ring and M an R-module. Consider the following conditions:

(a) We have $\ell_R(M) < \infty$.
(b) For any multiplicative $S \subset R$, we have $\ell_{S^{-1}R}(S^{-1}M) < \infty$.
(c) For any prime ideal $\mathfrak{p} \subset R$, we have $\ell_{R_p}(M_{\mathfrak{p}}) < \infty$.
(d) For any maximal ideal $\mathfrak{m} \subset R$, we have $\ell_{R_{\mathfrak{m}}}(M_{\mathfrak{m}}) < \infty$.

Show that (a) ⇒ (b) ⇒ (c) ⇒ (d), and that when R is Noetherian and M finitely generated, all conditions are equivalent.

Exercise 2.14. Let R be a Noetherian ring with no embedded primes (e.g., a reduced Noetherian ring). Give a natural isomorphism $\mathrm{Quot}(R) \to \prod_{\mathfrak{p} \in \mathrm{Ass}(R)} R_{\mathfrak{p}}$ of R-algebras. What happens when R has embedded primes?

Exercise 2.15. [Move later, with slicing criterion.] Let k be a field. Show that the localization of the ring

$$R := k[x, y, z] := k[X, Y, Z]/(XZ - Y^2),$$

(the "coordinate ring of the quadric cone in $\mathbb{A}_k^3$") at the prime (x, y, z) (at the "cone point") is Cohen-Macaulay but not regular.

Chapter 3

Integrality and Cohen-Seidenberg Theory

3.1 Fundamentals of Integrality

Definition 3.1.1. Let $R \subset S$ be a ring extension. We say that an element $s \in S$ is

(a) *algebraic* over R if there is an integer $n \geq 1$ and $a_0, \dots, a_n \in R$ with $a_0 \neq 0$ such that

$$a_0 s^n + a_1 s^{n-1} + \cdots + a_n = 0,$$

(b) *integral* over R if it is algebraic and in the above we can take $a_0 = 1$, and more generally

(c) *integral over an ideal* $\mathfrak{a} \subset R$ if it is algebraic and in the above we can take $a_0 = 1$ and $a_1, \dots, a_n \in \mathfrak{a}$.

If R is a field, then the notions of algebraicity and integrality over R coincide.

Definition 3.1.2 (Integral Closure/Normalization)**.**

(a) If $R \subset S$ is a ring extension, then the subset of elements of S that are integral over R is called the *relative integral closure* or the *relative normalization* of R in S. We denote it by $\mathrm{Cl}_S(R)$.

(b) On the one hand, the subring R is said to be *integrally closed* or *relatively normal* in S if $R = \mathrm{Cl}_S(R)$. On the other hand, we say that the extension $S \subset R$ is *integral* iff $\mathrm{Cl}_S(R) = S$.

(c) If R is an integral domain, then the normalization $\mathrm{Cl}_{\mathrm{Frac}(R)}(R)$ of R in its fraction field is called the *absolute integral closure* or *absolute normalization* of R.

(d) A domain R is said to be *integrally closed* or *normal* if $R = \mathrm{Cl}_{\mathrm{Frac}(R)}(R)$.

Theorem 3.1.3 (Robust Characterizations of Integrality)**.** Let $R \subset S$ be a ring extension and $s \in S$ an element. Then the following are equivalent:

(a) The element s is integral over R.

(b) The subring $R[s]$ of S generated over R by s is a finitely generated R-module.

(c) The subring $R[s]$ of S is contained in a subring $R' \subset S$ which is a finitely generated R-module.

(d) There is a faithful $R[s]$-module M that is finitely generated as an R-module.

Proof. It is clear that (a) ⇒ (b) ⇒ (c) ⇒ (d). For (d) ⇒ (a), apply 1.5.2 with $\mathfrak{a} = (1)$. ■

Corollary 3.1.4 (Properties of Integral Extensions)**.** Let $R \subset S \subset T$ be ring extensions.

(a) If $s_1, \dots, s_n \in S$ are any elements over R, then the subalgebra $R[s_1, \dots, s_n] \subset S$ is a finitely generated R-module iff all the s_i are integral over R.

(b) The normalization $\mathrm{Cl}_S(R)$ is a subring of S containing R.

(c) (Transitivity) If T/S and S/R are integral, then so is T/R.

(d) (Idempotence) We have $\mathrm{Cl}_S(\mathrm{Cl}_S R) = \mathrm{Cl}_S R$, i.e., $\mathrm{Cl}_S R$ is integrally closed in S.

Proof.

(a) The "only if" direction follows from 3.1.3(c). For the "if", proceed by induction on n; when $n = 1$, this follows from 3.1.3(b). When $n \geq 2$, define $R' := R[s_1, \dots, s_{n-1}]$; by induction, this is a finitely generated R-module. Since s_n is integral over R, it is also integral over R' and so by the $n = 1$, we have $R'[s_n]$ is a finitely generated R'-module. By transitivity of module-finiteness, we conclude that $R[s_1, \dots, s_n]$ is a finitely generated R-module.

(b) If $s, t \in S$ are integral, then $R[s, t]$ is a finitely generated R-module by (a), and so the inclusions $R[s - t], R[st] \subset R[s, t]$ imply by 3.1.3(c) that $s - t, st \in \mathrm{Cl}_S(R)$.

(c) Suppose that $t \in T$ satisfies $t^n + s_1 t^{n-1} + \cdots + s_n = 0$ with $s_i \in S$. By (a), $S' := R[s_1, \ldots, s_n]$ is a finitely generated R-module. Since t is integral over S', we conclude that $S'[t]$ is a finitely generated S'-module. Again, by transitivity of module finiteness, we conclude that $S'[t]$ is a finitely generated R-module, so 3.1.3(c) shows that t is integral over R.

(d) This follows immediately from (c) because $\operatorname{Cl}_S(R)/R$ is integral by definition.

■

Example 3.1.5. The Rational Root Theorem asserts that a UFD is normal.

Example 3.1.6 (Algebraic Integers)**.** Let $K/\mathbb{Q}$ be any field extension (e.g. a number field). Then the integral closure $\operatorname{Cl}_K(\mathbb{Z}) =: \mathcal{O}_K$ of $\mathbb{Z}$ in K is called the *ring of algebraic integers* in K. It is easy to see that if $K/\mathbb{Q}$ is algebraic, then $K = (\mathbb{Z} \smallsetminus \{0\})^{-1}\mathcal{O}_K = \operatorname{Frac}\mathcal{O}_K$. By idempotence, $\mathcal{O}_K$ is normal but in general is not a UFD (e.g. for $K := \mathbb{Q}[\sqrt{-23}]$). When K is any algebraically closed field, this construction returns the ring $\mathcal{O}_{\overline{\mathbb{Q}}}$ of all algebraic integers.

Example 3.1.7 (Plane Cuspidal Cubic)**.** The coordinate ring of a planar cuspidal curve is a domain that is not normal. Let k be a field and look at $R := k[X,Y]/(Y^2 - X^3)$. Since $Y^2 - X^3 \in k[X,Y]$ is irreducible and $k[X,Y]$ is a PID, R is an integral domain; let $K := \operatorname{Frac} R$. Let x and y denote the classes of X and Y respectively in R, so $y^2 = x^3$. Then $0 \neq x, y \in R$ and so we may look at the element $t := y/x \in K$. Then $t^2 - x = 0$, so $t \in \operatorname{Cl}_K(R)$, but $t \notin R$: else $Y = FX + G(Y^2 - X^3)$ for some $F, G \in k[X,Y]$, which is impossible. In fact, it is easy to see that $K = k(t) \cong k(\mathbb{P}^1)$ and $\operatorname{Cl}_K(R) = k[t]$.

Lemma 3.1.8. Let $R \subset S$ be an integral ring extension.

(a) If $\mathfrak{b} \subset S$ is an ideal and $\mathfrak{a} := \mathfrak{b} \cap R$, then $S/\mathfrak{b}$ is integral over $R/\mathfrak{a}$.
(b) If $U \subset R$ is a multiplicative system, then $U^{-1}S$ is integral over $U^{-1}R$.
(c) If S is a domain, then R is a field iff S is.
(d) If $\mathfrak{p} \subset R$ and $\mathfrak{q} \subset S$ are primes such that $\mathfrak{q} \cap R = \mathfrak{p}$, then $\mathfrak{p}$ is maximal iff $\mathfrak{q}$ is.

Proof. The statements in (a) and (b) are clear, and (d) follows from (a) and (c) applied to $R/\mathfrak{p} \subset S/\mathfrak{q}$. For (c), first assume that R is a field and let $0 \neq s \in S$. There is an $n \geq 1$ and $a_i \in R$ such that $s^n + a_1 s^{n-1} + \cdots + a_n = 0$. Since S is a domain, we can assume that $a_n \neq 0$, so since R is a field $a_n^{-1} \in R$. Then $-a_n^{-1}(s^{n-1} + a_1 s^{n-2} + \cdots + a_{n-1}) \in S$ is a multiplicative inverse for s. Conversely, if S is a field and $0 \neq r \in R$, then there is an $r^{-1} \in S$ and so there is an $n \geq 1$ and $a_i \in R$ such that $r^{-n} + a_1 r^{-n+1} + \cdots + a_n = 0$. Multiplying by r^{n-1} gives us $r^{-1} = -(a_1 + a_2 r + \cdots + a_n r^{n-1}) \in R$. ■

Note that part (c) of 3.1.8 needs S to be a domain; consider $k \subset k[x]/(x^2)$. Next, we briefly discuss integrality over an ideal.

Lemma 3.1.9. Let $R \subset S$ be a ring extension, and let $\mathfrak{a} \subset R$ be an ideal.

(a) The collection $\operatorname{Cl}_S(\mathfrak{a})$ of elements of S integral over $\mathfrak{a}$ is $\sqrt{\mathfrak{a}\operatorname{Cl}_S(R)}$.
(b) Suppose that S is a domain, and let $K := \operatorname{Frac} R$. Given an $s \in \operatorname{Cl}_S(\mathfrak{a})$, if the minimal polynomial of s over K is $\mu_s(X) = X^n + a_1 X^{n-1} + \cdots + a_n \in K[X]$, then for each i we have $a_i \in \operatorname{Cl}_K(\mathfrak{a})$. In particular, if R is normal, then the coefficients $a_i \in \sqrt{\mathfrak{a}}$.

Proof.

(a) If x is integral over $\mathfrak{a}$ and $n \geq 1, a_i \in \mathfrak{a}$ are such that $x^n + a_1 x^{n-1} + \cdots + a_n = 0$, then $x^n \in \mathfrak{a}\operatorname{Cl}_S(R)$ so $x \in \sqrt{\mathfrak{a}\operatorname{Cl}_S(R)}$. Conversely, if $x \in \sqrt{\mathfrak{a}\operatorname{Cl}_S(R)}$, then $x^n = \sum_j \alpha_j x_j$ for some $n \geq 1$ and elements $\alpha_j \in \mathfrak{a}, x_j \in \operatorname{Cl}_S(R)$. Since each x_j is integral over R, the ring $M := R[x_j]_j$ is a finitely generated R-module and $x^n M \subset \mathfrak{a}M$. By 1.5.1, we have that

$x^n + a_1 x^{n-1} + \cdots + a_n = 0 \in \operatorname{End}_R(M)$ for some $a_i \in \mathfrak{a}$, but since $1 \in M$, we have this identity in S.

(b) Let $L := \operatorname{Frac} S$ and look at the roots s_j of μ_s in some extension of L. These also satisfy the same equation of integral dependence and so belong to $\operatorname{Cl}_S(\mathfrak{a})$; since the coefficients a_i are polynomials in the s_i, they belong to $\operatorname{Cl}_S(\mathfrak{a})$ as well. Therefore, they belong to

$$\operatorname{Cl}_S(\mathfrak{a}) \cap K = \operatorname{Cl}_K(\mathfrak{a}) = \sqrt{\mathfrak{a}\operatorname{Cl}_K(R)} = \sqrt{\mathfrak{a}},$$

where equality at the last two steps holds by (a) and the normality of R respectively.

■

Corollary 3.1.10. Let R be a normal domain, $K = \operatorname{Frac} R$ be its fraction field, L/K an algebraic extension and $S = \operatorname{Cl}_L(R)$. An $\alpha \in L$ is in S iff the minimal polynomial $\mu_\alpha(X) \in K[X]$ of α over K is in $R[X]$.

This corollary reduces the check of integrality to that of identifying the minimal polynomial; some applications of this can be found in 3.1 and 3.2.

Proof. The "if" implication is clear; for the "only if", take $\mathfrak{a} = R$ in 3.1.9(b). ■

Next, we discuss how integrality behaves under localization.

Lemma 3.1.11. Suppose $R \subset S$ is a ring extension.

(a) If $U \subset R$ is a multiplicative subset, then $\operatorname{Cl}_{U^{-1}S}(U^{-1}R) = U^{-1}\operatorname{Cl}_S(R) \subset U^{-1}S$.[1]

(b) When R is a domain, the following are equivalent:

  (i) R is normal.

  (ii) $U^{-1}R$ is normal for every multiplicative $U \subset R$.

  (iii) $R_\mathfrak{p}$ is normal for all $\mathfrak{p}$.

  (iv) $R_\mathfrak{m}$ is normal for all $\mathfrak{m}$.

Proof.

(a) By 3.1.8(b) we have $U^{-1}\operatorname{Cl}_S(R) \subset \operatorname{Cl}_{U^{-1}S}(U^{-1}R)$. The converse follows from clearing denominators in an equation exhibiting integrality; the details are straightforward and left to the reader.

(b) The implication (i) ⇒ (ii) follows from (a). The implications (ii) ⇒ (iii) ⇒ (iv) are clear. For (iv) ⇒ (i), if an element of $K = \operatorname{Frac}(R)$ is integral over R, then it is integral over $R_\mathfrak{m}$ for all $\mathfrak{m}$ and hence it belongs to $\bigcap_\mathfrak{m} R_\mathfrak{m} = R$ (1.15).

■

Finally, we discuss how integrality behaves under purely transcendental ring extensions. In what follows, let $X = (X_i)_{i\in I}$ denote an abritrary collection of variables, and for a ring R, let $R[X]$ denote the polynomial ring obtained by adjoining this collection.

Lemma 3.1.12. Let $R \subset S$ be a ring extension.

(a) We have $\operatorname{Cl}_{S[X]}(R[X]) = (\operatorname{Cl}_S(R))[X] \subset S[X]$.

(b) In particular, R is integrally closed in S iff $R[X]$ is integrally closed in $S[X]$.

(c) If R is a domain, then R is normal iff $R[X]$ is normal.

[1] Here we are implicitly using that if $R \subset S$ is a ring extension and $U \subset R$ a multiplicative subset, then the natural map $U^{-1}R \to U^{-1}S$ is also injective, so that we may identify $U^{-1}R$ with a subring of $U^{-1}S$.

Proof. Parts (b) and (c) follow immediately from (a) (along with the fact that if $K = \operatorname{Frac} R$ is a field, then $K[X]$ is normal–this is 3.1.5). In showing (a), we can immediately reduce to the case of finite and then singleton I, so we may assume that $R[X]$ just denotes the usual polynomial ring in one variable over R (and similarly for S etc.). The inclusion $(\mathrm{Cl}_S(R))[X] \subset \mathrm{Cl}_{S[X]}(R[X])$ is clear, since the latter is a ring. We give two proofs of the other inclusion.

(a) (Following [8, Exercise 4.17].) Let $f \in S[X]$ be integral over $R[X]$; we show by induction on the degree of f that $f \in (\mathrm{Cl}_R(S))[X]$. If $\deg f = 0$, the result is clear: simply evaluate at $X = 0$, or equivalently take constant terms, in an equation of integral dependence. Suppose now that $\deg(f) > 0$; then it suffices to show (using 3.1.4(b)) that the leading coefficient α of f is in $\mathrm{Cl}_R(S)$. By considering only the coefficients involved, we are immediately reduced to the case in which $\mathbb{Z} \to R \to S$ are of finite type, so that in particular R is Noetherian, which we assume hence. Now let $M := R[X, f] \subset S[X]$, and let $\operatorname{coef}(M) \subset S$ be the R-submodule generated by the coefficients of elements of M. Since M is a finitely generated R-module, $\operatorname{coef}(M)$ is a finitely generated R-module. Since α is the *leading coefficient* of f, we have that $R[\alpha] \subset M \subset S$. Since R is Noetherian, we conclude that $R[\alpha]$ is finitely generated as an R-module, and so we are done by Theorem 3.1.3(b).

(b) (Following [4, Exercises 5.8-9].) This proceeds in three steps:

(1) Let S be a ring and $f \in S[X]$ be a monic polynomial of degree $n \in \mathbb{Z}_{\geq 1}$. Then there is a ring extension $S \subset T$ and elements $\alpha_1, \dots, \alpha_n \in T$ such that $f = \prod_{i=1}^n (X - \alpha_i) \in T[X]$. Induct on n, with $n = 1$ clear. Now suppose $n \geq 2$, and we have shown the result for $n - 1$. First take $T' := S[X]/(f(X))$, and let $\alpha_1 \in T'$ be the image of X, so that $f(\alpha_1) = 0 \in T'$. It is easy to check by degree considerations that the natural map $S \to T'$ is injective. Now performing long division on f to write $f(X) = (X - \alpha_1) f_1(X)$ for some $f_1(X) \in T'[X]$ of degree $n - 1$. The result follows from applying the inductive hypothesis to T' in place of S.

(2) Let $R \subset S$ be a ring extension. If $f, g \in S[X]$ are monic polynomials such that $fg \in (\mathrm{Cl}_S(R))[X]$, then $f, g \in (\mathrm{Cl}_S(R))[X]$. Pick a ring T as in (1) such that $S \subset T$ and f and g split into linear factors in $T[X]$, say $f(X) = \prod_i (X - \alpha_i)$ and $g(X) = \prod_j (X - \beta_j)$. Then in T, each α_i and β_j is a root of $fg \in (\mathrm{Cl}_S(R))[X]$ and is hence integral over $\mathrm{Cl}_S(R)$, and hence over R (by 3.1.4(c)). Therefore, the coefficients of f (resp. g), which are elementary symmetric polynomials in the α_i (resp. β_j) are integral over R as well (by 3.1.4(b)) as needed.

(3) Suppose $f \in S[X]$ is integral over $R[X]$, and pick $n \in \mathbb{Z}_{\geq 1}$ and elements $a_1, \dots, a_n \in R[X]$ such that $f^n + a_1 f^{n-1} + \cdots + a_n = 0$. Let $N \gg 1$ be a large integer; specifically, we need $N > \max\left(\{n\} \cup \{\deg a_i\}_{i=1}^n\right)$. Set $g := f - X^N$. Replacing f by $g + X^N$ in the above equation of integral dependence yields a new one, say $g^n + b_1 g^{n-1} + \cdots + b_n = 0$, where $b_n = X^{Nn} + a_1 X^{N(n-1)} + \cdots + a_n \in R[X]$. Note in particular that b_n is monic (by our choice of N). Since $b_n = -g(g^{n-1} + \cdots + b_{n-1})$ and $-g$ is monic as well, we conclude that so is $g^{n-1} + \cdots + b_{n-1}$. Then step (2) applied to the monic polynomials $-g$ and $g^{n-1} + \cdots + b_{n-1}$ in $S[X]$ gives the required result.

■

3.2 Cohen-Seidenberg Theory

In this section, we develop the basic Cohen-Seidenberg theory of primes in integral extensions, which allow us to relate the Krull dimensions of two rings in an integral extension.

Theorem 3.2.1. Let $R \subset S$ be an integral extension and $\mathfrak{p} \subset R$ be a prime.

(a) (Lying Over) There is a prime $\mathfrak{q} \subset S$ such that $\mathfrak{q} \cap R = \mathfrak{p}$.
(b) (Incomparability) There are no inclusions between distinct primes $\mathfrak{q}$ of S lying over $\mathfrak{p}$.

Proof. For (a), by 1.1.13, it suffices to show that $\mathfrak{p}S \cap R \subset \mathfrak{p}$. If $x \in \mathfrak{p}S \cap R$, then $x \in \sqrt{\mathfrak{p}S}$, so by 3.1.9(a), we have $x \in \mathrm{Cl}_S(\mathfrak{p})$ and so $x^n \in \mathfrak{p}$ for some $n \geq 1$, from which we get $x \in \sqrt{\mathfrak{p}} = \mathfrak{p}$. For an alternative proof which also shows (b), localize both sides at $U := R \smallsetminus \mathfrak{p}$ and use 3.1.8(b) to conclude that $S_\mathfrak{p} := (R \smallsetminus \mathfrak{p})^{-1}S$ is integral over $R_\mathfrak{p}$. Then prime ideals of S lying over $\mathfrak{p}$ are in canonical bijection with prime ideals of $S_\mathfrak{p}$ lying over $\mathfrak{p}R_\mathfrak{p}$, and so we reduce to the case that R is local with $\mathfrak{p} = \mathfrak{m}$ the maximal ideal. For (a), note that if $\mathfrak{n} \subset S$ is any maximal ideal, then $\mathfrak{n} \cap R$ is maximal by 3.1.8(d) and so $\mathfrak{n} \cap R = \mathfrak{m}$ and $\mathfrak{n}$ lies over $\mathfrak{m}$. Conversely, if $\mathfrak{n} \subset S$ is a prime that satisfies $\mathfrak{n} \cap R = \mathfrak{m}$, then again by 3.1.8(d), $\mathfrak{n}$ is maximal; in particular, there are no inclusions between distinct such $\mathfrak{n}$. ■

Remark 3.2.2. Geometrically, 3.2.1 is saying that if $\varphi : R \to S$ is an injective integral morphism, then $\operatorname{Spec} \varphi$ is surjective with zero-dimensional fibers.

Example 3.2.3. Let $K/\mathbb{Q}$ be a number field, and $\mathcal{O}_K = \mathrm{Cl}_K(\mathbb{Z})$ its ring of integers. Given any prime $\mathfrak{p} \subset \mathcal{O}_K$, there is a prime $\mathfrak{P} \subset \mathcal{O}_{\overline{\mathbb{Q}}}$ in the ring of all algebraic integers such that $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$, and no two such primes $\mathfrak{P}, \mathfrak{P}'$ are comparable. Can you locate the hidden use of Zorn's Lemma in this proof?

Definition 3.2.4. A ring extension $R \subset S$ satisfies

(a) *the going up property* if given any $n \geq 1$ and chain $\mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n$ of primes in R and $\mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_m$ in S for some $1 \leq m < n$ such that $\mathfrak{q}_i \cap R = \mathfrak{p}_i$ for $1 \leq i \leq m$, the ascending chain of ideals can be completed: there are primes $\mathfrak{q}_{m+1} \subset \cdots \subset \mathfrak{q}_n$ in S such that $\mathfrak{q}_i \cap R = \mathfrak{p}_i$ for all i; and
(b) *the going down property* if given any $n \geq 1$ and chain $\mathfrak{p}_1 \supset \cdots \supset \mathfrak{p}_n$ of primes in R and $\mathfrak{q}_1 \supset \cdots \supset \mathfrak{q}_m$ in S for some $1 \leq m < n$ such that $\mathfrak{q}_i \cap R = \mathfrak{p}_i$ for $1 \leq i \leq m$, the descending chain of ideals can be completed: there are primes $\mathfrak{q}_{m+1} \supset \cdots \supset \mathfrak{q}_n$ in S such that $\mathfrak{q}_i \cap R = \mathfrak{p}_i$ for all i.

Theorem 3.2.5 (Cohen-Seidenberg)**.**

(a) (Going Up) If $R \subset S$ is integral, then $R \subset S$ satisfies the going up.
(b) (Going Down) If $R \subset S$ is integral with S a domain and R normal, then $R \subset S$ satisfies going down.

Proof. By Lying Over (3.2.1(a)) and induction, we are reduced to the case $n = 2, m = 1$.

(a) By 3.1.8(a), $S/\mathfrak{q}_1$ is integral over $R/\mathfrak{p}_1$, so by Lying Over (3.2.1(a)), there is a prime $\overline{\mathfrak{q}}_2$ of $S/\mathfrak{q}_1$ lying over $\mathfrak{p}_2/\mathfrak{p}_1$. Lifting to S, we get a prime $\mathfrak{q}_2$ of S lying over $\mathfrak{p}_2$.
(b) It suffices to show using 1.1.12(d) and 1.1.13 that $\mathfrak{p}_2 S_{\mathfrak{q}_1} \cap R \subset \mathfrak{p}_2$. If $x \in \mathfrak{p}_2 S_{\mathfrak{q}_1}$, then $sx = y$ for some $s \in S \smallsetminus \mathfrak{q}_1$ and $y \in \mathfrak{p}_2 S$. If the minimal polynomial of y over $K := \operatorname{Frac} R$ is $\mu_y(X) = X^n + a_1 X^{n-1} + \cdots + a_n \in K[X]$ then each $a_i \in \mathfrak{p}_2$ by 3.1.9(b). If further $x \in \mathfrak{p}_2 S_{\mathfrak{q}_1} \cap R \smallsetminus 0$, then $s = yx^{-1}$ with $x^{-1} \in K$, so the minimal polynomial of s over K is given by $\mu_s(X) = X^n + b_1 X^{n-1} + \cdots + b_n \in K[X]$ with $b_i = x^{-i} a_i$. But s is integral

over R, so by 3.1.10, $b_i \in R$ for each i. If $x \notin \mathfrak{p}_2$, then $x^i b_i = a_i \in \mathfrak{p}_2 \Rightarrow b_i \in \mathfrak{p}_2$ for all i so that $s^n \in \mathfrak{p}_2 S \subset \mathfrak{p}_1 S \subset \mathfrak{q}_1$, which is a contradiction to $s \notin \mathfrak{q}_1$.

■

For a different proof of Going Down using a little Galois Theory, see [8, Theorem 13.9]. Cohen and Seidenberg's very readable original paper [9] treats the slightly more general case where R is assumed to be a normal domain and no zero-divisors of S lie in R. Then also give counterexamples to show that the hypotheses cannot be easily weakened. A reader interested in this aspect of the theory is highly encouraged to read this paper. Finally, we note that Going Down also holds under the assumption that the extension $R \subset S$ is *flat*; see [8, Lemma 10.11]. This (along with Chevalley's Theorem) is the key ingredient in the proof that flat morphisms locally of finite presentation are open.

The Cohen-Seidenberg Theorems enable use to relate the dimensions of rings related by an integral extension. This comparison result is

Corollary 3.2.6. Let $R \subset S$ be an integral extension. Then

(a) $\dim R = \dim S$.

If $\mathfrak{p} \subset R$ and $\mathfrak{q} \subset S$ are primes with $\mathfrak{q} \cap R = \mathfrak{p}$, then

(b) $\operatorname{coht} \mathfrak{p} = \operatorname{coht} \mathfrak{q}$,
(c) $\operatorname{ht} \mathfrak{p} \geq \operatorname{ht} \mathfrak{q}$, and
(d) equality holds in (c) whenever $R \subset S$ further satisfies going down.

Proof.

(a) Going up and incomparability (3.2.5(a) and 3.2.1(b)) give us a canoncial bijection between (strict) chains of primes in R and S.
(b) The ring $S/\mathfrak{q}$ is integral over $R/\mathfrak{p}$ by 3.1.8(a), and so we are done by (a).
(c) If we have a chain of primes contained in $\mathfrak{q}$ of length n, then by intersecting with R we get a chain of length n in $\mathfrak{p}$ (where the inclusions are strict again by incomparability, 3.2.1(b)).
(d) Apply going down to go the other way.

■

3.3 Extensions of Homomorphisms to Algebraically Closed Fields

In this section, we discuss some general results on when homomorphisms to an algebraically closed field extend across ring extensions. These results will be very helpful when we return to dimension questions later.

Theorem 3.3.1. Let $R \subset S$ be a ring extension and Ω be an algebraically closed field. Let $\varphi : R \to \Omega$ be a homomorphism; we ask when it extends to a homomorphism $\hat{\varphi} : S \to \Omega$.

(a) If $R \subset S$ is integral, then φ extends to homomorphism $\hat{\varphi} : S \to \Omega$.

(b) (Lang's Lemma) If S is a domain and finitely generated R-algebra, φ extends to a $\hat{\varphi} : S \to \Omega$. In fact, given any $0 \neq s \in S$ there is a $0 \neq r \in R$ depending on s such if $\varphi(r) \neq 0$, then $\hat{\varphi}$ can be chosen to satisfy $\hat{\varphi}(s) \neq 0$.

(c) If S is a field, then given any $0 \neq \alpha \in S$, we have that φ extends to either $R[\alpha] \to \Omega$ or $R[\alpha^{-1}] \to \Omega$.

Proof.

(a) Let $\mathfrak{p} := \ker \varphi$. Replacing R by $R_{\mathfrak{p}}$ and S by $S_{\mathfrak{p}} := (R \smallsetminus \mathfrak{p})^{-1}S$ and using 3.1.8(b), we can reduce to the case when $(R, \mathfrak{m}, k)$ is local and $\ker \varphi = \mathfrak{m}$ is maximal. By 3.2.1(a) and 3.1.8(d), there is a maximal $\mathfrak{n} \subset S$ such that $\mathfrak{n} \cap R = \mathfrak{m}$. Then $S/\mathfrak{n}$ is an algebraic extension of the field k and Ω is an algebraically closed field containing $F := \varphi(k)$, so by the well-known case of algebraic extensions of fields, there is an extension $S/\mathfrak{n} \to \Omega$ extending $\varphi : k \to F$. Then $\hat{\varphi} : S \twoheadrightarrow S/\mathfrak{n} \to \Omega$ is the required extension of φ.

(b) By inducting on the minimal number of generators of S as an R-algebra, we are reduced to the case $S = R[x]$. Suppose that x is transcendental over R and let $s = a_0x^n + \cdots + a_n$ for some $n \in \mathbb{Z}_{\geq 0}$ and $a_0, \ldots, a_n \in R$ with $a_0 \neq 0$. Define $r := a_0$. If $\varphi : R \to \Omega$ has $\varphi(a_0) \neq 0$, then there is an $\alpha \in \Omega$ such that $\varphi(a_0)\alpha^n + \cdots + \varphi(a_n) \neq 0$, since Ω is infinite. Then define $\hat{\varphi} : R[x] \to \Omega$ by sending $x \mapsto \alpha$. Now suppose that x is algebraic; then so is s. Write down equations $a_0x^n + \cdots + a_n = 0$ and $b_0s^m + \cdots + b_m = 0$ satisfied by x and s with $n, m \geq 1$ and $a_i, b_j \in R$ with $a_0, b_m \neq 0$, and set $r := a_0b_m$. (That $r \neq 0$ uses that S is domain.) Then $S[r^{-1}] = R[r^{-1}][x]$ is integral over $R[r^{-1}]$. If $\varphi(r) \neq 0$, then φ extends to a map $R[r^{-1}] \to \Omega$ and hence by (a) to a $\hat{\varphi} : S[r^{-1}] \to \Omega$; the restriction of this to S gives the required extension. This extension satisfies $\hat{\varphi}(s) \neq 0$ because if $\hat{\varphi}(s) = 0$, then $\varphi(b_m) = 0$ and so $\varphi(r) = 0$ as well.

(c) As in (a) we may assume that $(R, \mathfrak{m}, k)$ is local and $\ker \varphi = \mathfrak{m}$ is maximal and we may let $F = \varphi(k)$ as before, so $\varphi : k \xrightarrow{\sim} F$. Let $\mathfrak{a} := \{f(X) \in R[X] : f(\alpha) = 0\} \subset R[X]$ and let $\mathfrak{b} := (\varphi(\mathfrak{a})) \subset F[X]$. Since $F[X]$ is a PID, we have $\mathfrak{b} = (\mu(X))$ for some $\mu(X) \in F[X]$. If $\mu(X)$ is either constantly 0 or nonconstant, then there is a $\beta \in \Omega$ such that $\mu(\beta) = 0$; then $\alpha \mapsto \beta$ gives an extension $R[\alpha] \to \Omega$. If $\mu(X)$ is a nonzero constant, then $\mathfrak{b} = (1)$. Since $\varphi : k \xrightarrow{\sim} F$, this implies that there is an $f(X) \in R[X]$ such that $\varphi(f)(X) = 1$, which is to say that there is an integer $n \geq 1$ and elements $a_0, \ldots, a_n \in R$ such that $a_0\alpha^n + \cdots + a_n = 0$ and $\varphi(a_0) = \varphi(a_1) = \cdots = \varphi(a_{n-1}) = \varphi(a_n) - 1 = 0$, and we can choose n to be the smallest integer with this property, and by replacing a_i by $a_ia_n^{-1}$, we may assume that $a_n = 1$. (This last step is justified by the fact that $1 - a_n \in \ker \varphi = \mathfrak{m} = \operatorname{Jac} R \Rightarrow a_n \in R^\times$.) The claim is that this latter case cannot hold for both α and α^{-1}; indeed, suppose that $m \geq 1$ is the smallest integer for which there are $b_0, \ldots, b_{m-1} \in R$ and $b_0\alpha^{-m} + \cdots + b_{m-1}\alpha^{-1} + 1 = 0$ with $\varphi(b_0) = \cdots = \varphi(b_{m-1}) = 0$. We may assume without loss of generality that $n \geq m$. Multiplying throughout by $a_0\alpha^n$, we get the relation $a_0\alpha^n + a_0b_{m-1}\alpha^{n-1} + \cdots + a_0b_0\alpha^{n-m} = 0$. Here we have two cases. If $n = m$, then subtracting the two and multiplying by $(1 - a_0b_0)^{-1}$ gives us $(a_1 - a_0b_{m-1})(1 - a_0b_0)^{-1}\alpha^{n-1} + \cdots + 1 = 0$. If $n \geq 2$, we have contradicted the minimality of n; if $n = 1$, then we have concluded the absurdity $1 = 0$.

■

3.4 Krull-Akizuki Theorem

In this section, we give another application of the theory developed so far that is often useful. The following proof and discussion has been taken from [10, §4.9].

Theorem 3.4.1 (Krull-Akizuki)**.** Let R be a Noetherian domain of dimension at most 1, and let $K = \operatorname{Frac} R$. If L is a finite extension of K, then every subring S of L containing R is Noetherian of dimension at most 1. Further, for every nonzero ideal $\mathfrak{a}$ of S, the quotient $S/\mathfrak{a}$ is a finite R-module.

Proof. We first reduce to the case of $L = K$. For this, first note that we have $R \subset S \subset K[S]$, so we may certainly assume without loss of generality that $L = K[S]$. Pick a basis say $x_1, \ldots, x_n$ of L/K lying in S, where $n = [L : K]$. For each i, the element $x_i \in S$ is integral over K, and so there is a nonzero $r_i \in R$ such that $r_i x_i \in S$ is integral over R. Then the ring $R' = R[r_1x_1, \ldots, r_nx_n]$ is a Noetherian domain (1.3.5) of dimension at most one (3.2.6(a)), and further $R' \subset S \subset L = \operatorname{Frac} R'$.

Therefore, we may assume that $L = K$. If $\dim R = 0$, then $R = K$ and there is nothing to show; hence assume that $\dim R = 1$. If S is a field, we are done; else, we may pick a proper nonzero ideal $\mathfrak{a} \subset S$. Pick a nonzero $x \in \mathfrak{a} \cap R$, and for $n \in \mathbb{Z}_{\geq 0}$, let $\mathfrak{a}_n := x^n S \cap R + xR$. Since $R/(x)$ is a zero-dimensional Noetherian ring, it is Artinian (2.3.2), and so there is an $N \in \mathbb{Z}_{\geq 1}$ such that for all $n > N$, we have $\mathfrak{a}_n = \mathfrak{a}_{n+1}$.

We claim next that this means that $x^N S \subset x^{N+1}S + R$ as R-submodules of K. Indeed, this property can be established locally, and so we may assume without loss of generality that R is local with maximal ideal $\mathfrak{m}$. If x is a unit, there is nothing to show; hence assume that $x \in \mathfrak{m}$. Let $0 \neq s \in S$. We first claim that there is an $n \in \mathbb{Z}_{\geq 1}$ with $n \geq N$ such that $\mathfrak{m}^{n+1} \subset s^{-1}R$. Indeed, it suffices to show this when $s = r^{-1}$ for some $r \in \mathfrak{m}$, but then (r) is an ideal of definition for R by 2.3.3(f), so we conclude by 2.3.3(b). It then follows that $x^{n+1}s \in x^{n+1}S \cap R \subset \mathfrak{a}_{n+1} = \mathfrak{a}_{n+2}$, so that $x^n s \in x^{n+1}S + R$. If the smallest $n \geq N$ for which this last property holds is greater than N, then

$$x^n s \in x^{n+1}S + (x^n S \cap R) \subset x^{n+1}S + \mathfrak{a}_n = x^{n+1}S + \mathfrak{a}_{n+1} = x^{n+1}S + xR,$$

whence $x^{n-1}s \in x^n S + R$, contradicting the minimality of n. Therefore, $n = N$, and hence $x^N s \in x^{N+1}S + R$. This is true for any $0 \neq s \in S$, and so we conclude that $x^N S \subset x^{N+1}S + R$.

Therefore, we have that

$$S/xS \cong x^N S/x^{N+1}S \subset (x^{N+1}S + R)/x^{N+1}S \cong R/(x^{N+1}S \cap R)$$

as R-modules. In particular,

$$\ell_{S/xS}(S/xS) \leq \ell_R(S/xS) \leq \ell_R(R/(x^{N+1}S \cap R)) \leq \ell_R(R/x^{N+1}R) = \ell_{R/x^{N+1}R}(R/x^{N+1}R) < \infty,$$

where again we are using that $R/(x^{N+1}R)$ is an Artinian ring (2.3.2). Therefore, S/xS is an Artinian ring, and hence in particular Noetherian (1.3.10); from this it follows that S is Noetherian as well. Since $\dim S/xS = 0$, it follows that $\dim S = 1$. Finally, if $\mathfrak{a} \subset S$ is a nonzero ideal, then either $\mathfrak{a} = S$, in which case $S/\mathfrak{a} = 0$, or $\mathfrak{a}$ is nonzero proper ideal, in which case for any nonzero $x \in \mathfrak{a} \in R$, we have the surjection $S/xS \twoheadrightarrow S/\mathfrak{a}$ of R-modules. Since, by the above, S/xS is a finite-length and hence finite R-module, so is $S/\mathfrak{a}$. ∎

Note that, in general, S is not a finite R-module, and that the obvious generalization to higher dimensional R is false; see again [10, §4.9].

3.5 Exercises

Exercise 3.1. Let $d \in \mathbb{Z}$ be a squarefree integer. Show that

$$\mathcal{O}_{\mathbb{Q}[\sqrt{d}]} = \begin{cases} \mathbb{Z}[\sqrt{d}], & \text{if } d \equiv 2, 3 \pmod 4, \text{ and} \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right], & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

Exercise 3.2. Let k be a field and $f(X) \in k[X]$ be a nonconstant separable polynomial. Let $R := k[X]$ and $K := \operatorname{Frac} k[X] = k(X)$.

(a) Show that $Y^2 - f(X) \in K[Y]$ is irreducible.

Let $L = K[\sqrt{f}] := K[Y]/(Y^2 - f(X))$; this is an algebraic field extension of K. Let $S := \mathrm{Cl}_L(R)$.

(b) Show that if $\operatorname{char} k \neq 2$, then $S = R[\sqrt{f}]$.

(c) Show by example that the result of (b) is false in general if $\operatorname{char} k = 2$. Can this result be salvaged?

Chapter 4

Derivations

4.1 Derivations and Kähler Differentials

Definition 4.1.1. Suppose R is a ring, S an R-algebra, and M an S-module. An *R-linear derivation (or simply an R-derivation) from S to M* is an R-module homomorphism $D : S \to M$ that satisfies the *Liebniz Rule* that for all $f, g \in S$ we have

$$D(fg) = f \cdot Dg + g \cdot Df.$$

The set of all R-linear derivations from S to M is naturally an S-module denoted by $\mathrm{Der}_R(S, M)$.

Remark 4.1.2.

(a) Every ring S is a $\mathbb{Z}$-algebra. A $\mathbb{Z}$-derivation is simply called a *derivation*, and in that case the module of derivations is written $\mathrm{Der}(S, M) := \mathrm{Der}_{\mathbb{Z}}(S, M)$.

(b) If $\phi : M \to M'$ is an S-module homomorphism and $D : S \to M$ an R-derivation, then it is immediate that the map $\phi \circ D : S \to M'$ is also an R-derivation. This gives an S-module homomorphism $\phi_* : \mathrm{Der}_R(S, M) \to \mathrm{Der}_R(S, M')$. It is immediate to check that this construction is functorial, so that taking R-derivations gives a covariant functor

$$\mathrm{Der}_R(S, -) : S\text{-}\mathsf{Mod} \to S\text{-}\mathsf{Mod}.$$

We shall see momentarily that this functor is representable.

(c) The case $M = S$ deserves special attention: we define $\mathrm{Der}_R(S) := \mathrm{Der}_R(S, S)$. If $D, D' \in \mathrm{Der}_R(S)$ then we can compose them to get another map $DD' : S \to S$ which is not in general a derivation. However, the bracket $[D, D'] = DD' - D'D$ is indeed a derivation, and this turns $\mathrm{Der}_R(S)$ into a Lie algebra over R.

Lemma 4.1.3 (Basic Properties of Derivations)**.**

(a) If $e \in S$ is an idempotent, then $D(e) = 0$ for any R-derivation $D \in \mathrm{Der}_R(S, M)$. In particular, $D(1) = 0$ for any R-derivation $D \in \mathrm{Der}_R(S, M)$.

(b) If $i : R \to S$ denotes the canonical map, then a derivation $D \in \mathrm{Der}(S, M)$ is R-linear iff $D \circ i = 0$. In this sense, $\mathrm{Der}_R(S, M) \subset \mathrm{Der}(S, M)$ is the submodule of derivations that vanish on R.

(c) For any $f, g \in S$, R-derivation $D \in \mathrm{Der}_R(S, M)$ and integer $n \geq 1$ we have that

$$D(f^n) = nf^{n-1}Df.$$

If, $M = S$, then we also have

$$D^n(fg) = \sum_{i=0}^{n} \binom{n}{i} D^i f \cdot D^{n-i} g.$$

(d) If $n = 0 \in S$ for some $n \geq 1$, then for any element $f \in S$ and $D \in \mathrm{Der}_R(S, M)$ we have $D(f^n) = 0$. If $n = p$ is prime, then if $D \in \mathrm{Der}_R(S)$ then $D^p \in \mathrm{Der}_R(S)$ too.

Proof.

(a) This follows from $D(e) = D(e^2) = 2e \cdot D(e) \Rightarrow (2e-1)D(e) = 0 \Rightarrow D(e) = (2e-1)^2 D(e) = 0$.

(b) If D is R-linear, then $D(r) = D(r \cdot 1) = r \cdot D(1) = 0$; the converse follows from the Liebniz Rule.

(c) Clear by induction on n.

(c) Clear from (d).

■

Example 4.1.4. If $S = R[X_\lambda]_{\lambda\in\Lambda}$ is the polynomial ring, then a derivation $D \in \operatorname{Der}_R(S, M)$ is completely determined by the family $D(X)_\lambda \in M$, since by the Leibniz rule we have for $F \in S$ that

$$DF = \sum_\lambda \frac{\partial F}{\partial X_\lambda} DX_\lambda,$$

where $\partial F/\partial X_\lambda$ is the usual formal derivative of F with respect to X_λ. In particular, we have $\operatorname{Der}_R(S) \cong \bigoplus_\lambda S\langle \mathrm{d}X_\lambda\rangle$ is the free S-module on the symbols $\mathrm{d}X_\lambda$ for $\lambda \in \Lambda$, and $\operatorname{Der}_R(S, M) \cong \operatorname{Der}_R(S) \otimes_S M$ for any S-module M.

Theorem 4.1.5 (Kähler Differentials)**.** The functor $\operatorname{Der}_R(S, -) : S\text{-}\mathsf{Mod} \to S\text{-}\mathsf{Mod}$ is representable. In other words, there is an S-module $\Omega_{S/R}$, called the *module of Kähler differentials* of S over R, and a derivation $\mathrm{d} : S \to \Omega_{S/R}$, called the *universal derivation*, such that if M is any S-module and $D \in \operatorname{Der}_R(S, M)$ any R-derivation, then there is a unique S-module homomorphism $\widetilde{D} : \Omega_{S/R} \to M$ such that $D = \widetilde{D} \circ \mathrm{d}$; in other words, such that the following diagram commutes:

$$\begin{tikzcd}
S \arrow[r, "\mathrm{d}"] \arrow[dr, "D"'] & \Omega_{S/R} \arrow[d, dashed, "\exists!\, \widetilde{D}"] \\
 & M
\end{tikzcd}$$

From this it follows that we have a natural isomorphism of functors

$$\operatorname{Der}_R(S, -) \cong \operatorname{Hom}_S(\Omega_{S/R}, -) : S\text{-}\mathsf{Mod} \to S\text{-}\mathsf{Mod}.$$

Proof. The universal property determines $\Omega_{S/R}$ upto unique isomorphism preserving d; therefore, it suffices to show existence. We give two constructions:

(a) Consider the quotient of the free S-module generated by all symbols of the form $\{\mathrm{d}f : f \in S\}$ by the relations

$$-\,\mathrm{d}(fg) + f\,\mathrm{d}g + g\,\mathrm{d}f \text{ and } -\,\mathrm{d}(rf + sg) + r\,\mathrm{d}f + s\,\mathrm{d}g,$$

for all $f, g \in S$ and $r, s \in R$. The quotient $\Omega_{S/R}$ along with the map $\mathrm{d} : S \to \Omega_{S/R} : f \mapsto [\mathrm{d}f]$ satisfies the universal property.

(b) Firstly, define $\mu : S \otimes_R S \to S$ by $\mu(f \otimes g) := fg$; then μ is an R-algebra homomorphism. Set $I := \ker\mu$ and $\Omega_{S/R} := I/I^2$, with the map $\mathrm{d} : S \to \Omega_{S/R}$ given by $f \mapsto 1 \otimes f - f \otimes 1 \pmod{I^2}$.[1] Now given an R-derivation $D : S \to M$, we get an R-module homomorphism $\delta : S \otimes_R S \to M$ given on pure tensors by $f \otimes g \mapsto f \cdot Dg$. This satisfies the property that for $x, y \in S \otimes_R S$ we have

$$\delta(xy) = \mu(x)\delta(y) + \mu(y)\delta(x),$$

and so vanishes on I^2. From this we get the map $\tilde{D} : \Omega_{S/R} \to M$, which is easily seen to be an S-module homomorphism with $\tilde{D} \circ d = D$. Finally, since for $f \otimes g \in S \otimes_R S$ we have

$$f \otimes g = (f \otimes 1)(1 \otimes g - g \otimes 1) + fg \otimes 1,$$

it follows that if $x = \sum_i f_i \otimes g_i \in I$ then $x \equiv \sum_i f_i \mathrm{d}g_i \pmod{I^2}$, so that $\Omega_{S/R}$ is generated as an S-module by the ds, showing uniqueness of $\tilde{D}$.

[1] Note that $S \otimes_R S/I \cong S$ and the S-module structure on $\Omega_{S/R}$ comes from noting that it (being a quotient of I) is an $S \otimes_R S$-module annihilated by I, and hence an $S \otimes_R S/I \cong S$-module; equivalently, S-module structure on $\Omega_{S/R}$ given by multiplication on either the right or the left is the same.

■

Remark 4.1.6. For $i \geq 0$, define $\Omega^i_{S/R} := \Lambda^i \Omega_{S/R}$; then the derivation $\mathrm{d} : S = \Omega^0_{S/R} \to \Omega^1_{S/R} = \Omega_{S/R}$ is the first step in a complex of R-modules

$$\Omega^\bullet_{S/R} : 0 \to \Omega^0_{S/R} \xrightarrow{\mathrm{d}=\mathrm{d}^0} \Omega^1_{S/R} \xrightarrow{\mathrm{d}^1} \cdots \to \Omega^i_{S/R} \xrightarrow{\mathrm{d}^i} \Omega^{i+1}_{S/R} \to \cdots ,$$

where the map $\mathrm{d}^i : \Omega^i_{S/R} \to \Omega^{i+1}_{S/R}$ satisfies

$$\mathrm{d}^i(f \mathrm{d}\eta_1 \wedge \cdots \wedge \mathrm{d}\eta_i) = \mathrm{d}f \wedge \mathrm{d}\eta_1 \wedge \cdots \wedge \mathrm{d}\eta_i.$$

The complex $\Omega^\bullet_{S/R}$ is called the *de Rham complex* of S relative to R, and its cohomology $H^\bullet_{\mathrm{dR}}(S; R)$ is called the *de Rham cohomology* of S relative to R.

To define it we simply set $\mathrm{d}'(b/s) = (1/s)\mathrm{d}b - (1/s^2)b\mathrm{d}s$. To see that this is well-defined, note that if $b/s = b'/s'$ in $S^{-1}B$, then there is a $t \in S$ such that $t(s'b - b's) = 0$. Differentiating $t^2(s'b - b's) = 0$ and using the Leibniz Rule then yields that $t^2(s'\mathrm{d}b + b\mathrm{d}s' - b'\mathrm{d}s - s\mathrm{d}b') = 0$. Therefore,

$$\begin{aligned} & t^2 \left(s^2(s'\mathrm{d}b' - b'\mathrm{d}s') - (s')^2(s\mathrm{d}b - b\mathrm{d}s)\right) \\ =& t^2 \left(ss'(s\mathrm{d}b' - s'\mathrm{d}b) - (s^2b'\mathrm{d}s' - (s')^2 b\mathrm{d}s)\right) \\ =& t^2 \left(ss'(b\mathrm{d}s' - b'\mathrm{d}s) - (s^2b'\mathrm{d}s' - (s')^2 b\mathrm{d}s)\right) \\ =& t^2(s'b - b's)(s'\mathrm{d}s' + s'\mathrm{d}s) = 0, \end{aligned}$$

whence $\mathrm{d}'(b/s) = \mathrm{d}'(b'/s')$. The linearity of d' and the Leibniz Rule follow immediately from it being well-defined and the corresponding properties of d. Finally, d' evidently vanishes on A because d does, and hence defines an A-derivation, finishing the proof.

4.2 Fundamental Exact Sequences

4.3 Smoothness

Chapter 5

Field Theory

5.1 Linear Disjointness

In this section, we study the basic condition of abstract linear disjointness. To set this notion up, consider first the case of a large embedding field. Let Ω/k be a field extension, and let $k \subset K/L \subset \Omega$ be two subextensions. In this setting, we let $K[L] = L[K]$ denote the smallest subring of Ω containing K and L, and let KL denote the compositum of K and L in Ω, i.e., the smallest sub*field* of Ω containing both K and L, so that $KL = \operatorname{Frac} K[L]$ with $KL = K[L]$ if either K or L is algebraic over k (see Exercise 5.1).

Proposition/Definition 5.1.1. Let Ω/k be a field extension, and let $k \subset K, L \subset \Omega$ be two subextensions. The following conditions are equivalent:

(a) If a collection $\{x_\lambda\}$ of elements of K is linearly independent over k, then the same collection considered in Ω is linearly independent over L.
(b) The same as (a) with K and L interchanged.
(c) If $\{x_\lambda\}$ (resp. $\{y_\mu\}$) is a collection of elements of K (resp. L) linearly independent over k and $c_{\lambda\mu} \in k$ are elements, all but finitely many zero, such that $\sum c_{\lambda\mu} x_\lambda y_\mu = 0 \in \Omega$, then each $c_{\lambda\mu} = 0$.
(d) The natural map $K \otimes_k L \to \Omega$ is injective.
(e) The natural map $K \otimes_k L \to K[L]$ is an isomorphism.

When one of K and L is finite over k, say L, then these conditions are also equivalent to

(f) We have $[KL : K] = [L : k]$.

When these equivalent conditions are satisfied, we say that K and L are *linearly disjoint over* k *in* Ω. Further,

(g) If $\Lambda \subset \Omega$ is any field containing the compositum KL, then K and L are linearly disjoint over k in Ω iff they are so in Λ; in particular, this holds for $\Lambda = KL$.
(h) In this setting, K and L are linearly disjoint over k in Ω iff for all finitely generated subextensions $K' \subset K$ and $L' \subset L$, the fields K' and L' are linearly disjoint over k in Ω.
(i) If K and L are linearly disjoint over k in Ω, then $K \cap L = k$.

Proof. Note that the natural map $K \otimes_k L \to K[L]$ is surjective, so an isomorphism iff it is injective. The equivalence of (a)-(e) is clear from the properties of tensor product over a field k. When L is finite over k, then $K[L] = KL$ is the compositum of K and L in Ω (Exercise 5.1), so that (e) and (f) are equivalent for dimension reasons. The claims (g) and (h) are clear; for (i), if $\theta \in K \cap L \setminus k$, then $1 \otimes \theta - \theta \otimes 1 \in K \otimes_k L$ is a nonzero element of the kernel of the map to Ω. ■

When K and L are both finite over k, the condition (f) is clearly equivalent also to $[KL : k] = [K : k][L : k]$. The converse of (i) is not true; see Theorem 5.1.3 and Remark 5.1.4. Let us now immediately study the dependence of this notion on Ω, or equivalently the notion of "abstract" linear disjointness of two field extensions; the original source for the following very clear treatment is [11].

Proposition/Definition 5.1.2. Let k be a field, and $K, L \supset k$ two field extensions, not necessarily embedded in any larger field.

(a) The field extensions K and L are said to be *somewhere linearly disjoint over* k if there is a field extension $\Omega \supset k$ and k-embeddings $i : K \hookrightarrow \Omega$ and $j : L \hookrightarrow \Omega$ such that $i(K)$ and $j(L)$ are linearly disjoint over k in Ω; this is equivalent to $K \otimes_k L$ being a domain.
(b) The field extensions K and L are said to be *everywhere linearly disjoint over* k if for every field extension $\Omega \supset k$ and k-embeddings $i : K \hookrightarrow \Omega$ and $j : L \hookrightarrow \Omega$, the fields $i(K)$ and

$j(L)$ are linearly disjoint over k in Ω; this is equivalent to $K \otimes_k L$ being a field.

(c) If either K or L is algebraic over k, then conditions (a) and (b) are equivalent, i.e., if K, L are somewhere linearly disjoint over k, then they are everwhere linearly disjoint over k. In this case, we say that K and L are *(abstractly) linearly disjoint over k*.

See also Exercise 5.10.

Proof.

(a) If there is such a field extension Ω, then $K \otimes_k L \cong i(K) \otimes_k j(L) \xrightarrow{\sim} i(K)[j(L)] \subset \Omega$ is a domain; conversely, if $K \otimes_k L$ is a domain, taking $\Omega = \operatorname{Frac} K \otimes_k L$ suffices.

(b) If $K \otimes_k L$ is a field, then for any field Ω, the natural map $K \otimes_k L \to \Omega$ must be injective; conversely, if $K \otimes_k L$ is *not* a field, then it has a nontrivial maximal ideal $\mathfrak{m} \subset K \otimes_k L$, and taking $\Omega := K \otimes_k L/\mathfrak{m}$ gives us a field extension in which K and L are *not* linearly disjoint over k.

(c) In light of Exercise 5.4, the implication (b) $\Rightarrow$ (a) always holds, and if K or L is algebraic (i.e., integral) over k, the implication (a) $\Rightarrow$ (b) follows from the stability of integrality under base-change and Lemma 3.1.8(c). Alternatively, suppose there is a field extension $\Omega \supset k$ containing K and L such that K and L are linearly disjoint over k in Ω. Then by Proposition/Definition 5.1.1(e), the natural map $K \otimes_k L \to K[L]$ is an isomorphism. By Exercise 5.1, if either K or L is algebraic over k, then $K[L] = KL$ is the compositum of K and L in Ω, and hence in this case $K \otimes_k L$ is a field, whence K and L are everywhere linearly disjoint over k.

■

Here is a good illustration of these definitions.

Theorem 5.1.3. Let k be a field and $K, L \supset k$ be two algebraic extensions such that at least one of K and L is normal over k and at least one of K and L is separable over k. Then K and L are (abstractly) linearly disjoint over k iff for some further field extension Ω containing K and L we have $K \cap L = k$.

By Proposition/Definitions 5.1.2 if this condition holds, then $K \cap L = k$ in *any* Ω.

Proof. One direction was shown in Propositions/Definitions 5.1.1(i) and 5.1.2(c) above; for the other, suppose that we are given such an Ω, and further that K is separable over k; then in light of Proposition 5.1.2(c), we only need to show that $K \cap L = k$ implies that K and L are linearly disjoint over k in Ω.

First suppose that K is also normal, so that K/k is Galois; this result is then called the "Theorem on Natural Irrationalities." By Proposition/Definition 5.1.1(h), we may assume that $K, L/k$ are finite, and by replacing K by its normal closure we may assume further that K is finite Galois. By the Primitive Element Theorem, K is the splitting field of a single separable polynomial over k, in which case KL is the splitting field of the same polynomial over L and hence KL/L is Galois as well. Since $K \cap L = k$, there is a restriction map $\operatorname{Gal}(KL/L) \to \operatorname{Gal}(K/k)$, which is easily seen to be an isomorphism, giving us $[KL : L] = [K : k]$. Then we are done by Proposition/Definition 5.1.1(f).

Now suppose only that K is separable, but L is normal over k. As in the previous step, we may assume that K and L are both finite over k. Let S (resp. I) denote the separable (resp. purely inseparable) closure of k in L, so that S/k is Galois and so, by the case already shown, we have $[KS : K] = [S : k]$. Now KS/k is separable and I/k purely inseparable, so that by Exercise 5.11, KS and I are linearly disjoint over k in Ω; in particular, $[KL : KS] = [KSI : KS] = [I : k]$.

Then the result follows again from Proposition/Definition 5.1.1(f) along with the computation

$$[KL:K] = [KL:KS][KS:K] = [I:k][S:k] = [I:k][L:I] = [L:k],$$

where we are using in the second-to-last step that $I = L^{\mathrm{Aut}(L/k)}$, whence L/I is Galois with Galois group $\mathrm{Aut}(L/k) \cong \mathrm{Gal}(S/k)$, and so in particular $[L:I] = [S:k]$. ■

Remark 5.1.4. There is no easy way to strengthen the preceding theorem, in the following sense.

(a) Taking $k = \mathbb{Q}$, $K = \mathbb{Q}[\sqrt[3]{2}]$, and $L = \mathbb{Q}[\omega\sqrt[3]{2}]$ inside say $\Omega = \mathbb{C}$ (where $\omega^2 + \omega + 1 = 0$) gives us an example where both K and L are separable over k and $K \cap L = k$ in Ω, but K and L are not linearly disjoint over k, since $KL = \mathbb{Q}[\sqrt[3]{2}, \omega]$ has degree 6 over k. Note that neither K nor L is normal over k.

(b) Given a prime $p > 0$, taking $k = \mathbb{F}_p(s,t)$, $K = k[X]/(X^{p^2} + sX^p + t)$, and $L = k^{1/p^\infty}$ inside an algebraic closure Ω of k gives us an example where L/k is normal and $K \cap L = k$ in Ω, but K and L are not linearly disjoint over k. Note that neither K nor L is separable over k. See §5.3 and [12] for details, and also Exercise 5.7 for a similar example.[1]

Finally, one result that is used quite often is

Theorem 5.1.5 (Transitivity of Linear Disjointness)**.** Let $k \subset \Omega$ be a field extension, and let $k \subset K' \subset K \subset \Omega$ and $k \subset L \subset \Omega$ be subextensions. Then K and L are linearly disjoint over k in Ω iff K' and L are linearly disjoint over k in Ω and K and $K'L$ are linearly disjoint over K' in Ω.

Proof. Consider the sequence of maps

$$K \otimes_k L \overset{\sim}{\to} K \otimes_{K'} (K' \otimes_k L) \twoheadrightarrow K \otimes_{K'} K'[L] \twoheadrightarrow K[L].$$

If K and L are linearly disjoint over k in Ω, then clearly so are K' and L; further, the composite map $K \otimes_k L \to K[L]$ above is an isomorphism, forcing the map $K \otimes_{K'} K'[L] \to K[L]$ to be an isomorphism as well, which implies that K and $K'[L]$ are linearly disjoint over K', and then so are K and $K'L$ since $K'L = \mathrm{Frac}\, K'[L]$ (Exercise 5.3).

$$\begin{tikzcd}
 & \Omega \\
K \arrow[r] & KL \arrow[u] \\
K' \arrow[u] \arrow[r] & K'L \arrow[u] \\
k \arrow[u] \arrow[r] & L \arrow[u]
\end{tikzcd}$$

Conversely, if K' and L are linearly disjoint over k in Ω, then the natural map $K' \otimes_k L \to K'[L]$ is injective, and hence, since tensoring over a field is exact, so is $K \otimes_{K'} (K' \otimes_k L) \to K \otimes_{K'} K'[L]$. If further K and $K'L$ are linearly disjoint over K' in Ω, then so are K and $K'[L]$ (again see Exercise 5.3), and hence the map $K \otimes_{K'} K'[L] \to K[K'[L]] = K[L]$ is injective as well. These two facts combined then imply that the map $K \otimes_k L \to K[L]$ is also injective, so that K and L are linearly disjoint over k. ■

[1] I would be interested in seeing an example where both K and L are normal but Theorem 5.1.3 fails. I also suspect that this result needs a suitable p-dimension to be at least 2 (so, e.g., that there is no counterexample with $k = \mathbb{F}_p(s)$).

5.2 Some Dependence Relations Involving Fields

We use the abstract study of dependence relations (§10.3) to some more sophisticated concrete examples: that of algebraic dependendence, p-dependence, and differential dependence.

5.2.1 Algebraic Dependence

Theorem/Definition 5.2.1. Let $k \subset K$ be a field extension. The map $\mathscr{D} : 2^K \to 2^K$ defined by sending X to the integral closure of $k(X)$ in K, i.e.,

$$\mathscr{D}X = \mathrm{Cl}_K(k(X))$$

is a dependence relation on K, called *algebraic dependence* over k.

A basis for this dependence relation is called a *transcendence basis* for K/k, and the dependency of K with respect to this relation is called the *transcendence degree of K over k*, written $\operatorname{trdeg}_k K$. More generally, if R is a domain containing k, we define its *transcendence degree over k*, written $\operatorname{trdeg}_k R$ to be $\operatorname{trdeg}_k R := \operatorname{trdeg}_k \operatorname{Frac} R$.

Proof. Conditions (a), (b), and (d) in Definition 10.3.1 are clear, and (c) follows from transitivity of integral closure: for any X, the set $\mathscr{D}X$ is a field by Lemma 3.1.8(c) and so

$$\mathscr{D}^2 X = \mathrm{Cl}_K\, k(\mathscr{D}X) = \mathrm{Cl}_K\, \mathscr{D}X = \mathrm{Cl}_K(\mathrm{Cl}_K\, k(X)) = \mathrm{Cl}_K\, k(X) = \mathscr{D}X,$$

where in the second to last step have used Corollary 3.1.4(d). It remains to show (e). Suppose that $x \in X \subset K$ and $y \in \mathscr{D}X \smallsetminus \mathscr{D}(X \smallsetminus \{x\})$; then for some $n \geq 1$ and $a_0, \ldots, a_n \in k(X)$ with $a_0 \neq 0$ we have $a_0 y^n + \cdots + a_n = 0$. Clearing denominators, we may assume that each $a_i \in k[X]$. Rearrange the terms in this identity to write it out in powers of x, i.e.,write it as $b_0 x^m + \cdots + b_m = 0$ for some $m \geq 0$ with $b_0 \neq 0$ and each $b_i \in k[(X \smallsetminus \{x\}) \cup \{y\}]$. If $m = 0$, then $b_0 = 0$ still has a nonzero power of y and then shows that $y \in \mathscr{D}(X \smallsetminus \{x\})$, a contradiction; therefore $m \geq 1$ and we have shown that $x \in \mathscr{D}((X \smallsetminus \{x\}) \cup \{y\})$ as needed. ■

The fundamental set of this relation is the field $\mathrm{Cl}_K(k)$, i.e., the algebraic closure of k in K. An element $x \in K$ is said to be *transcendental* over k iff $\{x\}$ is algebraically independent over k, which is equivalent to saying that $x \notin \mathrm{Cl}_K(k)$. It is a straightforward consequence of the definition that a family of elements $\{x_\lambda\}$ in K is algebraically independent over k iff the natural map $k[X_\lambda] \to K$ taking $X_\lambda \mapsto x_\lambda$ is injective, and hence extends to an isomorphims $k(X_\lambda) \to k(x_\lambda)$. This family is, in addition, a transcendence basis for K/k iff K is in addition algebraic over $k(x_\lambda)$. In particular, K/k is algebraic iff $\operatorname{trdeg}_k K = 0$, and $\operatorname{trdeg}_k k(X_1, \ldots, X_n) = n$ for any $n \geq 0$. Finally, it is easy to see that if $k \subset K \subset L$ is a tower of extensions, then $\operatorname{trdeg}_k L = \operatorname{trdeg}_k K + \operatorname{trdeg}_K L$ (Exercise 5.8), and that any finitely generated field extension has finite transcendence degree–indeed, if $K = k(a_1, \ldots, a_n)$, then there is a subset of $\{a_1, \ldots, a_n\}$ that is a transcendence basis for K over k.

Remark 5.2.2. It is not necessarily true that if K/k has finite transcendence degree then it is finitely generated; indeed, consider $k = \mathbb{Q}$ and $K = \overline{\mathbb{Q}}$.

Example 5.2.3. Let Ω be a field of characteristic zero and uncountable cardinality, say $|\Omega| = \mathfrak{c}$ (e.g., $\Omega = \mathbb{R}, \mathbb{C}, \mathbb{Q}_p, \overline{\mathbb{Q}_p}, \mathbb{C}_p$, etc.). We show that $\operatorname{trdeg}_{\mathbb{Q}} \Omega = \mathfrak{c}$. For that, first note that if k is a countable field, then so is $k[X]$ by separating by degree and then so is $k(X) = \operatorname{Frac} k[X]$ because it injects into $k[X] \times k[X]$. If K/k is an algebraic extension of a countable field, then $K = \bigcup_{0 \neq f \in k[X]} \{\alpha \in K : f(\alpha) = 0\}$ being a countable union of finite sets is countable as well. Given this, if $X = \{x_n\}_{n \geq 1}$ is an at most countable transcendence basis of Ω over $\mathbb{Q}$, then if we let $K_0 := \mathbb{Q}$ and $K_n := K_{n-1}(x_n)$ for $n \geq 1$, then $\mathbb{Q}(X) = \bigcup_{n\geq 0} K_n$ is a countable union of countable sets and so countable; and then the algebraicity of Ω over $\mathbb{Q}(X)$ would show that Ω is countable as well, which is false. The Lefschetz principle (as well as another proof of the Nullstellensatz for $k = \Omega$ when algebraically closed, see [13, Lecture 5]) makes use of this observation.

Example 5.2.4. Let k be a field, $n \geq 1$ an integer, and $f \in k[X_1, \dots, X_n]$ be an irreducible polynomial. Then $R := k[X_1, \dots, X_n]/(f)$ is an integral domain; we claim that $\operatorname{trdeg}_k R = n-1$. Indeed, let $K := \operatorname{Frac} R$. Write $f = a_0 X_n^m + a_1 X^{m-1} + \cdots + a_m$ for some $m \geq 0$ and each $a_i \in k[X_1, \dots, X_{n-1}]$ with $a_0 \neq 0$. By relabelling the X_i if necessary, we may assume that $m \geq 1$. If $x_1, \dots, x_n$ denote the classes of $X_1, \dots, X_n$ in R (and so K) respectively, then we claim that $\{x_1, \dots, x_{n-1}\}$ form a transcendence basis for K over k. Indeed, the equation $\overline{f} = 0$ in K shows that x_n is algebraically dependent on $\{x_1, \dots, x_{n-1}\}$, so these elements form an algebraic spanning set. To show that they are algebraically independent, suppose that there is a polynomial $g \in k[X_1, \dots, X_{n-1}]$ such that $g(x_1, \dots, x_{n-1}) = 0$. Then $g \in k[X_1, \dots, X_{n-1}] \cap (f) = (0) \subset k[X_1, \dots, X_n]$ as needed.[2]

One further idea that we will use is that of

Definition 5.2.5. Let L/k be a field extension.

(a) A *separating transcendence basis for* L/k is a transcendence basis X for L/k such that the algebraic extension $L/k(X)$ is separably algebraic.

(b) The extension L/k is said to be *separably generated* if it admits a separating transcendence basis.

Note that in characteristic zero, any transcendence basis is a separating transcendence basis and every field extension is separably generated. In positive characteristic, this is no longer true: if p is a prime and $k = \mathbb{F}_p$ with $L = \mathbb{F}_p(t)$, then the set $\{t^p\}$ is a transcendence basis for L/k but not a separating transcendence basis, although L/k *is* separably generated. An algebraic field extension is separably generated iff it is separable algebraic, and so an inseparable algebraic extension is an example of a field extension that is not separably generated. This notion will appear frequently in discussions below.

5.2.2 p-dependence

Next up is a phenomenon special to characteristic $p > 0$, due to Teichmüller from 1936.

Theorem/Definition 5.2.6. Let $k \subset L$ be a field extension in characteristic $p > 0$. The map $\mathscr{D} : 2^K \to 2^K$ defined by sending X to the smallest subfield of K containing k, K^p and X, i.e.,

$$\mathscr{D}X = k(K^p, X)$$

is a dependence relation on K, called *p-dependence* over k.

A basis for this dependence relation is called a *p-basis* for K/k, and the dependency of K with respect to this relation is called the *p-dimension* of K over k, written $p\text{-}\dim_k K$.

Proof. Conditions (a)-(d) are clear; again, we have to show (e). Suppose $x \in X \subset K$ and $y \in \mathscr{D}X \smallsetminus \mathscr{D}(X \smallsetminus \{x\})$. Let $L := \mathscr{D}(X \smallsetminus \{x\})$ for convenience, so that $\mathscr{D}X = L(x)$ and

[2] Note that a sort of converse of this observation is also true: if $\mathfrak{p} \subset k[X_1, \dots, X_n]$ is a prime ideal such that $R := k[X_1, \dots, X_n]/\mathfrak{p}$ has $\operatorname{trdeg}_k R = n-1$, then $\mathfrak{p}$ is principal. This follows from combining Theorem 6.2.8 and Theorem/Definition 1.4.3, along with the fact that the polynomial ring $k[X_1, \dots, X_n]$ is a UFD, which itself follows from Corollary 1.4.10.

$y \in L(x) \smallsetminus L$. Note that since $x^p \in L$ but $x \notin L$, it follows that $[L(x) : L] = p$.[3] Now $L \subsetneq L(y) \subset L(x)$ and the primality of p forces $L(x) = L(y)$, whence $x \in L(y)$, as needed. ■

The fundamental set of this relation is the field $k(K^p)$. A family of elements $B = \{x_\lambda\}$ in K is p-indepedent over k iff for any finite subset $B' \subset B$ of cardinality $n \geq 0$, we have $[k(K^p, B') : k(K^p)] = p^n$, or equivalently iff the set Γ_B of p-monomials

$$\Gamma_B := \left\{ x^e = \prod_\lambda x_\lambda^{e_\lambda} \right\}$$

in B (where $e = (e_\lambda)$ runs over the set of tuples indexed by B such that $0 \leq e_\lambda \leq p-1$ for each λ and $e_\lambda = 0$ for all but finitely many λ) is linearly independent over $k(K^p)$. This family B is further a p-basis if in addition we have $k(K^p, B) = K$, or equivalently iff Γ_B is a $k(K^p)$-basis of K.

Example 5.2.7. Let p be a prime, $n \geq 0$ an integer and $K := \mathbb{F}_p(X_1, \dots, X_n)$ and let $k = K^p$. Then $\{X_1, \dots, X_n\}$ is a p-basis for K/k, so $p\text{-dim}_k K = n$. Conversely, if K/k is any extension field generated by m-elements (i.e., $K = k(a_1, \dots, a_m)$), then there is a subset of $\{a_1, \dots, a_n\}$ that is a p-basis for K/k, and in particular $p\text{-dim}_k K \leq m$. In particular, $\mathbb{F}_p(X, Y)/\mathbb{F}_p(X^p, Y^p)$ is not a simple extension, illustrating the necessity of the separability hypothesis in the Primitive Element Theorem.

5.2.3 Differential Dependence

Finally, here is a more sophisticated notion of dependence that we shall use in these notes.

Definition 5.2.8. Let $k \subset K$ be a field extension. Then the module $\Omega_{K/k}$ of Kähler differentials is an K-vector space and so has a linear dependence relation LD_K. If $\mathrm{d} : K \to \Omega_{K/k}$ is the universal differential, then the pullback dependence relation (Exercise 10.6) $\mathrm{d}^*\mathrm{LD}_K$ on K is called the relation of *k-differential dependence* on K.

It follows from the definition that a collection $\{x_\lambda\}$ of elements k-differentially spans K (resp. is k-differentially independent, is a k-differential basis) iff the collection $\{\mathrm{d}x_\lambda\}$ of its differentials K-linearly spans $\Omega_{K/k}$ (resp. is K-linearly independent, is a K-linear basis). Consequently, $\operatorname{dep} \mathrm{d}^*\mathrm{LD}_K = \dim_K \Omega_{K/k}$.

[3] This uses Exercise 5.13.

5.3 Separability

In this section, we talk about separability of algebras and non-algebraic field extensions. In this section, all algebras are commutative.

Definition 5.3.1. Given a field k, a k-algebra A is called *separable* (over k) if $A_L := A \otimes_k L$ is a reduced ring for every field extension L/k.

Remark 5.3.2. If a k-algebra A is separable, then every k-subalgebra of A is also separable. Since reducedness can be detected at the element level and tensoring over k is exact, we see that A is separable over k iff all of its finitely generated subalgebras are, iff $A \otimes_k L$ is reduced for every finitely generated extension L/k, and iff for any extension K/k, the algebra A_K is separable over K. In the language of algebraic geometry, separability corresponds to geometric reducedness.

For future use, we record one elementary but important fact here as a lemma.

Lemma 5.3.3. Let k be a field, $n \geq 1$ an integer, and $A_1, \dots, A_n$ be k-algebras. The direct product k-algebra $A_1 \times \cdots \times A_n$ is separable iff each A_i for $i = 1, \dots, n$ is.

Proof. If the product is separable, then so is each A_i because each A_i is (isomorphic to) a k-subalgebra of the product. For the other direction, check that the tensor product over a field k commutes with taking finite direct product of k-algebras, i.e. for every field extension L/k, the natural map $(A_1 \times \cdots \times A_n)_L \to (A_1)_L \times \cdots \times (A_n)_L$ is an isomorphism of L-algebras. ■

Now let us understand the field extensions which satisfy this definition a little better.

Theorem/Definition 5.3.4 (Separable Field Extensions)**.** For a field extension K/k, the following are equivalent.

(a) The field K is separable as a k-algebra, i.e. for every extension L/k, the ring $K \otimes_k L$ is reduced.
(b) For every finite purely inseparable extension L/k, the ring $K \otimes_k L$ is reduced.
(c) There is a perfect extension L/k such that $K \otimes_k L$ is reduced.
(d) Let $\overline{k}$ be an algebraic closure of k. Then $K \otimes_k \overline{k}$ is reduced.
(e) For every algebraically closed extension Ω of k and for all $n \geq 1$ and k-linearly independent elements $a_1, \dots, a_n$ of Ω, there are $\sigma_1, \dots, \sigma_n \in \mathrm{Aut}_k(\Omega)$ such that $\det(\sigma_i(a_j))_{i,j} \neq 0$.
(f) If $\operatorname{char} k = p > 0$, then K and k^{1/p^∞} are linearly disjoint over k.
(g) If $\operatorname{char} k = p > 0$, then K and $k^{1/p}$ are linearly disjoint over k.
(h) Every finitely generated subextension of K is separably generated.
(i) For any subfield $k' \subset k$ the map $K \otimes_k \Omega_{k/k'} \to \Omega_{K/k'}$ is injective.
(j) The map $K \otimes_k \Omega_k \to \Omega_K$ is injective.
(k) Any derivation of k to an arbitrary K-vector space M extends to a derivation of K to M.

An extension satisfying these equivalent conditions is said to be a *separable* field extension. Further,

(h) Suppose that $K = k(a_1, \dots, a_n)$ is finitely generated and separable. Then there is a subset of $\{a_1, \dots, a_n\}$ that is a separating transcendence basis for K/k.
(i) If K/k is separably generated, then it is separable.
(j) If K/k is algebraic, then the above definition agrees with the usual definition of algebraic separability, i.e. K/k is separable iff the minimal polynomial over k of any element of K is a separable polynomial.

(k) If K/k is finite, then K/k is separable iff it is étale over k iff the trace pairing on K is perfect (or equivalently nondegenerate).

Remark 5.3.5. From the above theorem, it is clear that in characteristic zero every field extension is separable. It is not true that with the finitely generated hypothesis that a separable extension is separably generated (i.e. that (j) holds); see Example 10.6.7.

Proof.

(a) ⇒ (b) Suppose $\operatorname{char} k = p > 0$. It suffices to show that if $L \subset k^{1/p^\infty}$ is any finitely generated subextension, then K and L are linearly disjoint over k. For that, note that L/k is a finite purely inseparable extension and pick an $N \gg 1$ such that $L^{p^N} \subset k$. Since $A := K \otimes_k L$ is a finite-dimensional K-algebra, it is an Artinian ring; since $A^{p^N} \subset K$, it follows that every non-unit of A is nilpotent and hence A is local (Proposition/Definition 1.2.7); since, addition, it is reduced by hypothesis, it follows from Theorem 1.3.9(a) that A is a field, and hence K and L are linearly disjoint over k.

(b) ⇒ (c) Clear, since $k^{1/p} \subset k^{1/p^\infty}$.

(c) ⇒ (d) If $\operatorname{char} k = 0$, we are done. If $\operatorname{char} k = p > 0$, replace K by this finitely generated extension to assume that K is finitely generated; then we will show (h) using the definition (c) for separability. After relabelling, assume that $a_1, \dots, a_r \in K$ are a transcendence basis for K/k, $a_{r+1}, \dots, a_s \in K$ are separably algebraic over $k(a_1, \dots, a_r)$. We induct on $n - s$. If $n - s = 0$, we are done. Now suppose that $s \le n - 1$ and $y := a_{s+1}$ is not separably algebraic over $k(a_1, \dots, a_r)$. Let $f(Y^p) \in k(a_1, \dots, a_r)[Y]$ be the minimal polynomial of a_{s+1} over $k(a_1, \dots, a_r)$, and minimally clear denominators to get a polynomial $F(X, Y^p) \in k[X, Y] := k[X_1, \dots, X_m, Y]$ such that $F(a_1, \dots, a_r, a_{s+1}^p) = 0$. Now if $\partial F/\partial X_i = 0$ for $1 \le i \le r$, then there is a polynomial $G(X, Y) \in k^{1/p}[X, Y]$ such that $F = G^p$; then

$$k[a_1, \dots, a_r, a_{s+1}] \otimes_k k^{1/p} \cong k[X, Y]/(F) \otimes_k k^{1/p} \cong k^{1/p}[X, Y]/(G^p)$$

is a nonreduced subring of $K \otimes_k k^{1/p}$, so $K \otimes_k k^{1/p}$ cannot be a domain, contradicting the linear disjointness hypothesis. Therefore, $\partial F/\partial X_i \ne 0$ for some $1 \le i \le r$; after further relabelling, we may assume $\partial F/\partial X_1 \ne 0$. Then a_1 is separable algebraic over $k(a_2, \dots, a_r, a_{s+1})$, and so are $a_{r+1}, \dots, a_s$. For transcendence degree reasons, $a_2, \dots, a_r, a_{s+1}$ must be a transcendence basis for K/k. Setting $a_1' := a_{s+1}$, $A_{s+1} = a_1$ and $a_j' = a_j$ for all $j \ne 1, s+1$. we have reduced $n - s$ by 1, finishing the proof.

(d) ⇒ (a) It suffices to assume that K is finitely generated; then it suffices to show (i) using definition (a), i.e. that if K is a separably generated field extension, then K is separable as a k-algebra. Let Γ be a separating transcendence basis for K over k. Now $k(\Gamma) \otimes_k L$ is a ring of fractions of the domain $k[\Gamma] \otimes_k L \cong L[\Gamma]$ and is hence a domain with field of fractions $L(\Gamma)$. Thus

$$K \otimes_k L \cong K \otimes_{k(\Gamma)} (k(\Gamma) \otimes_k L) \hookrightarrow K \otimes_{k(\Gamma)} L(\Gamma),$$

and we are reduced to the case where K/k is separably algebraic. Again we may assume that K is finitely generated, so that K is then finite separable. By the Primitive Element Theorem, $K \cong k[X]/(f)$ for some separable $f \in k[X]$, and then $K \otimes_k L \cong L[X]/(f)$. Now $f \in L[X]$ is still separable, although no longer necessarily irreducible; say $f = \prod_{i=1}^n f_i$ for distinct irreducibles f_i which are pairwise coprime. Then the Chinese Remainder Theorem gives us

$$L[x]/(f) \cong \prod_{i=1}^{n} L[X]/(f_i),$$

which is a finite product of fields and hence reduced.

(c) ⇒ (e)

(e) ⇒ (f) Take k' to be the prime subfield of k.

(f) ⇔ (g) Both are equivalent to the surjectivity of $\operatorname{Hom}_K(\Omega_K, M) \to \operatorname{Hom}_K(K \otimes_k \Omega_k, M)$ for each M.

(f) ⇒ (c)

(h) This was shown in the proof of the implication (c) ⇒ (d).

(i) This was shown in the proof of the implication (d) ⇒ (a).

(j) Clear from (d) or (h); one direction of this was also shown in the proof of (d) ⇒ (a).

(k) Immediate from Theorem/Definitions 5.3.4 and 5.4.1 below.

■

Corollary 5.3.6. Let $k \subset K \subset L$ be a tower of field extensions.

(a) If L/k is separable, then so is K/k. If, in addition, K/k is algebraic, then L/K is separable as well.

(b) If K/k and L/K are separable, then so is L/k.

Proof.

(a) The separability of K/k is an immediate consequence of Theorem/Definition 5.3.4(c). Suppose now that K/k is algebraic as well.

■

One simple consequence of the above definition is the characterization of fields with only separable extensions.

Theorem/Definition 5.3.7 (Perfect Fields)**.** Let k be a field. Then the following are equivalent:

(a) Either $\operatorname{char} k = 0$ or $\operatorname{char} k = p > 0$ and $k = k^{1/p}$, i.e. every element of k is a p^{th} power.

(b) Every field extension of k is separable.

(c) Every algebraic extension of k is separable.

(d) Every finite extension of k is separable.

Fields satisfying these equivalent conditions are called *perfect fields*.

Proof. The implication (a) ⇒ (b) follows from Theorem 5.3.4(c), and (b) ⇒ (c) ⇒ (d) are clear. For (d) ⇒ (a), suppose $\operatorname{char} k = p > 0$. If $x \in k^{1/p} \smallsetminus k$, then the finite extension $k(x)$ of k is not separable. ■

Example 5.3.8. Note that all fields of characteristic zero, all algebraically closed fields, all finite fields, and all algebraic extensions of perfect fields are perfect (the last by Corollary 5.3.6(a)). A simple example of a field that is not perfect is $\mathbb{F}_p(t)$.

Theorem 5.3.9. Let k be a field and X be a geometrically integral k-scheme. Then the field extension $k(X)/k$ is a separable extension and k is algebraically closed in $k(X)$. If X is locally of finite type over k, then $k(X)$ is also finitely generated.

Proof. Replace X by an affine open to assume $X = \operatorname{Spec} A$ for a domain A. It follows from geometric integrality of X that if k'/k is any algebraic extension field, then $A_{k'} = A \otimes_k k'$ is still a domain, and hence so is the localization $k(X) \otimes_k k'$, showing that $k(X)$ and k' are (abstractly) linearly disjoint over k. Applying this to $k' = k^{1/p}$ shows that $k(X)$ is separable over k (Theorem 5.3.4(c)); applying this to $k' = \operatorname{Cl}_{k(X)}(k)$ shows that k is algebraically closed in $k(X)$. If X is locally of finite type over k, then A can be taken to be a finitely generated k-algebra, and then $k(X) = \operatorname{Frac} A$ is a finitely generated extension of k. ■

Remark 5.3.10. Let k be a field and X an integral k-scheme. Consider the following conditions:

(a) X is geometrically integral over k.
(b) The function field $k(X)$ and an algebraic closure $\overline{k}$ are linearly disjoint over k.
(c) The field k is algebraically closed in the function field $k(X)$.

Then (a) $\Leftrightarrow$ (b) $\Rightarrow$ (c). If k is perfect, then all conditions are equivalent.

Indeed, (a) $\Rightarrow$ (b) was proven in Theorem 5.3.9, (b) $\Rightarrow$ (a) is standard algebraic geometry [TOCITE Liu], (b) $\Rightarrow$ (c) is clear from the definitions, and the implication (c) $\Rightarrow$ (b) when k is perfect is Exercise 5.6. Finally, Exercise 5.7 shows that these conditions are not always equivalent if k is not perfect.

Theorem 5.3.11. *Let K/k be a finitely generated field extension. Then*

$$\operatorname{trdeg}_k K \leq \dim_K \Omega_{K/k} < \infty$$

with equality in the former iff K/k is separable. In this last case, a collection $x_1, \ldots, x_n \in K$ of elements is a separating transcendence basis of K/k iff $\mathrm{d}x_1, \ldots, \mathrm{d}x_n$ form a K-linear basis of $\Omega_{K/k}$.

5.4 Étale Algebras and Grothendieck's Reformulation of Galois Theory

In this section, we study Grothendieck's reformulation of infinite Galois theory over a field k as the computation of the étale fundamental group $\pi_1^{\text{ét}} \operatorname{Spec} k$. For this, the fundamental objects of interest are étale algebras. Again, all algebras in this section are assumed to be commutative.

Theorem/Definition 5.4.1 (Étale Algebras)**.** Let k be a field and $\overline{k}$ a fixed algebraic closure of k with a given embedding $k \hookrightarrow \overline{k}$. For a finite-dimensional algebra A over k, consider the following conditions.

(a) There is an isomorphism of k-algebras $A \cong k[X]/(f)$ for some separable $f \in k[X]$.
(b) A is a finite direct product of finite separable field extensions of k.
(c) A is separable as a k-algebra.
(d) $A_{\overline{k}}$ is a reduced ring.
(e) $A_{\overline{k}}$ is a finite direct product of copies of $\overline{k}$.
(f) The discriminant of one (and hence any) basis of A/k is nonzero.
(g) The trace pairing on A is perfect (or equivalently nondegenerate).

The conditions (b)-(g) are equivalent and implied by (a). If $\dim_k A \leq \#k$ (in particular, if k is infinite), then all conditions are equivalent. A k-algebra A is said to be *étale* over k if it is finite-dimensional, commutative, and satisfies the equivalent conditions (b)-(g).

Proof.

(a) ⇒ (b) The irreducible factors of f are all distinct and separable, and hence pairwise coprime; we are done by the Chinese Remainder Theorem.

(b) ⇒ (c) Apply Theorem 5.3.4 and Lemma 5.3.3.

(c) ⇒ (b) A is Artinian since it is finite-dimensional over k. If A is local, then by Theorem 1.3.9(a), A is a field, and then we are done by Theorem 5.3.4. In general, by Theorem 1.3.9(e), A is a finite direct product of Artinian local rings, and it is easy to see from the proof of that result that if A is a k-algebra, then so is each factor. By Lemma 5.3.3, each factor is separable, and so we are done by the local case.

(c) ⇒ (d) Clear from the definition.

(d) ⇒ (e) Again, since $A_{\overline{k}}$ is a reduced Artinian ring, we are done by the same argument as in (c) ⇒ (b).

(e) ⇒ (f) The discriminant is stable under base change, and the discriminant of a finite direct product of copies of $\overline{k}$ is clearly nonzero (take a basis of idempotents).

(f) ⇔ (g) Clear from the definition of the discriminant and the trace pairing.

(f) ⇒ (c) Again, since the discriminant is stable under base change, it suffices to show that if A is a finite-dimensional algebra over a field with nonzero discriminant, then A is reduced. Suppose $n := \dim_k A$ and let $r := \dim_k \sqrt{0A}$; suppose instead that $1 \leq r \leq n$. Pick an (ordered) k-basis $\alpha_1, \ldots, \alpha_n$ of A such that $\alpha_1, \ldots, \alpha_r$ form a basis for $\sqrt{0A}$. Then if either $i \leq r$ or $j \leq r$, then the k-linear map $\alpha_i\alpha_j : A \to A$ is nilpotent, and hence has zero trace. Therefore, the matrix $[\operatorname{Tr}_k^A(\alpha_i\alpha_j)]_{ij}$ has its first r rows and columns identically zero, so if $r \geq 1$, it cannot have nonzero determinant.

(b) ⇒ (a), when $\dim_k A \leq \#k$. Find an integer $n \geq 1$ and finite separable field extensions $K_1, \ldots, K_n$ of k such that $A \cong \prod_{i=1}^n K_i$. For each $i = 1, \ldots, n$, use the Primitive Element Theorem to pick monic irreducible $f_i \in k[X]$ so that $K_i \cong k[X]/(f_i)$, ensuring that each new f_i is not equal to f_j for $j < i$. This can be achieved by replacing $f_j(X)$ by $f_j(X + a)$ for $a \in k^\times$ if necessary; here we use that there are at least $(n-1)$ different choices for a by hypothesis and that if $f \in k[X]$ is irreducible, then the $\{f(X+a)\}_{a \in k^\times}$ are irreducible and pairwise coprime. Then the polynomials f_i are irreducible, separable, and pairwise coprime, and we may take $f = \prod_{i=1}^n f_i$.

■

The hypothesis that $\dim_k A \leq \#k$ in the implication (b) ⇒ (a) is necessary; see Exercise 5.14.

Finally, we want to mention that the ddecomposition of an étale algebra as a product of field extensions is essentially unique; this is a consequence of the following general observation.

Lemma 5.4.2. Let k be a field, $n \geq 1$ an integer and $K_1, \dots, K_n$ field extensions of k. Let $A := \prod_{i=1}^n K_i$ be their product.

(a) Given a k-algebra B and a surjective k-algebra morphism $\varphi : A \to B$, the map φ can be decomposed as a projection onto a subproduct followed by an isomorphism.

(b) Further, if B is a field extension of k, then the projection map is a projection onto a single factor. In particular, we have

$$\mathrm{Hom}_k(A, B) \cong \coprod_{i=1}^n \mathrm{Hom}_k(K_i, B).$$

(c) If $m \geq 1$ is another integer and $L_1, \dots, L_m$ field extensions of k with $B = \prod_{j=1}^m L_j$, then

$$\mathrm{Hom}_k(A, B) \cong \coprod_{i,j} \mathrm{Hom}_k(K_i, L_j).$$

(d) In particular, $A \cong B$ iff $n = m$ and there is a permutation $\sigma : [n] \to [n]$ such that $K_i \cong L_{\sigma(i)}$ as k-algebras for $i = 1, \dots, n$.

Proof.

(a) The projection of the kernel to each K_i is an ideal of K_i.

(b) The image of A in B is a k-subalgebra of a field, and hence an integral domain.

(c) Follows from $\mathrm{Hom}_k(A, B) \cong \prod_{j=1}^m \mathrm{Hom}_k(A, L_j)$ combinted with (b).

(d) Clear from (c): note that n is determined as the number of inequivalent idempotents of A, and projections $\prod_i K_i \twoheadrightarrow L_j$ and $\prod_j L_j \twoheadrightarrow K_i$ show that each K_i is isomorphic to some L_j.

■

Now suppose k is a field, and we fix an embedding $k \hookrightarrow \overline{k}$ as above. Let k^s denote the separable closure of k in $\overline{k}$, so $k \subset k^s \subset \overline{k}$. If L/k is any finite separable extension, then $\# \mathrm{Hom}_{k\text{-}\mathsf{Alg}}(L, k^s) = [L : k]_s = [L : k] < \infty$, and so $X_L := \mathrm{Hom}_{k\text{-}\mathsf{Alg}}(L, k^s)$ is a finite set.[4] The absolute Galois group $G_k = \mathrm{Gal}(k^s/k)$ acts on X_L by postcomposition, and for each $\varphi \in X_L$, the stabilizer $(G_k)_\varphi = \mathrm{Gal}(k^s/\varphi(L))$ is an open subgroup of G_k by the Fundamental Theorem of Infinite Galois Theory, and so X_L is a discrete G_k-set (see Exercise 5.16). Finally, this action is transitive by the extension property of homomorphisms from algebraic extensions to algebraically closed fields. In conclusion, X_L is a left coset space for some open subgroup in G_k. When L/k is Galois, X_L is isomorphic to a quotient of G_k by an open normal subgroup, namely $\mathrm{Gal}(k^s/\varphi(L))$ for one (and hence any) $\varphi \in X_L$. If K and L are two finite separable extensions and $\theta : K \to L$ a k-homomorphism, then we get a pullback map $\theta^* : X_L \to X_K$, which is clearly a G_k-set morphism.

[4] In the terminology of algebraic geometry, this is the set $X_L = \mathrm{Spec}(L)(k^s)$ of k^s-valued points of the geometrically reduced separated finite-type k-scheme (i.e. k-variety) $\mathrm{Spec}(L)$ in the category of k-schemes.

Theorem 5.4.3. In the above set-up, the association $L \mapsto X_L$ gives an antiequivalence between the categories of finite separable extensions L/k and transitive finite (left) G_k-sets. Further, Galois extensions correspond to finite quotients of G_k.

Proof. For essential surjectivity, let X be a transitive finite left G_k-set, and pick an $x \in X$. By Exercise 5.16, the stabilizer of x in G_k is an open subgroup, and so by the Fundamental Theorem of Infinite Galois Theory is of the form $\mathrm{Gal}(k^s/L)$ for some finite separable subextension L/k of k^s. Let $\iota : L \hookrightarrow k^s$ be the inclusion; then the map $X_L \to X$ given by $g\iota \mapsto gx$ is an isomorphism of G_k-sets.

It remains to show that if $K, L/k$ are finite separable extensions, then the map

$$-^* : \mathrm{Hom}_k(K, L) \to \mathrm{Hom}_{G_k}(X_L, X_K)$$

is a bijection. For this, we construct an inverse. Fix an $\iota \in X_L$; then a G_k-homomorphism $\eta : X_L \to X_K$ determines and is determined by the element $\eta(i) \in X_K$ by transitivity. If η is a G_k-homomorphism, then $\mathrm{Gal}(k^s/\iota(L)) = (G_k)_\iota \subset (G_k)_{\eta(\iota)} = \mathrm{Gal}(k^s/\eta(\iota)(K))$, so by the Fundamental Theorem we get $\iota(L) \supset \eta(\iota)(K)$. The composite $\theta_\eta : K \xrightarrow{\eta(\iota)} \iota(L) \xrightarrow{\iota^{-1}} L$ is a k-algebra homomorphism with $\theta_\eta^* = \eta$. Checking that this construction gives inverse bijections is left to the reader. ■

We can now ask what all the finite left G_k-sets are, not necessarily transitive ones. Note that if A is an étale k-algebra, then $X_A := \mathrm{Hom}_{k\text{-}\mathsf{Alg}}(A, k^s)$ is also a left G_k-set. If we pick n and K_i as in Lemma 5.4.2 as given by Theorem/Definition 5.4.1(b), the decomposition in Lemma 5.4.2(b) of the form

$$X_A \cong \coprod_{i=1}^{n} X_{K_i}$$

is an isomorphism of G_k-sets. In particular, X_A is a finite left G_k set. The main theorem we are after here says exactly that these are, in fact, all.

Theorem 5.4.4 (Fundamental Theorem of Galois Theory, Grothendieck's Version)**.** The association $A \mapsto X_A$ gives an antiequivalence between the categories of étale algebras A/k and finite left G_k-sets. Further,

(a) separable field extensions correspond to transitive finite left G_k-sets, and
(b) Galois extensions correspond to finite quotients of G_k.

Proof. Again, for essential surjectivity, let X be a finite left G_k-set, and decompose it into its G_k-orbits: pick an integer $n \geq 1$ and G_k-invariant subsets $X_1, \dots, X_n \subset X$ such that $X = \coprod_{i=1}^n X_i$ and the action of G_k on each X_i is transitive. For each $i = 1, \dots, n$, by Theorem 5.4.3, there is a finite separable extension K_i/k and a G_k-set isomorphism $X_{K_i} \to X_i$. Taking $A = \prod_{i=1}^n K_i$, it follows that the composition

$$X_A \cong \coprod_{i=1}^{n} X_{K_i} \xrightarrow{\sim} \coprod_{i=1}^{n} X_i = X$$

is a G_k-set isomorphism. Similarly, to show full faithfulness, suppose we have étale k-algebras A, B, and we pick n, m, K_i and L_j as in Lemma 5.4.2 so $A \cong \prod_{i=1}^n K_i$ and $B \cong \prod_{j=1}^m L_j$. Then we get G_k-set isomorphisms

$$\mathrm{Hom}_{k\text{-}\mathsf{Alg}}(A, B) \cong \coprod_{i,j} \mathrm{Hom}_k(K_i, L_j) \xrightarrow{\sim} \coprod_{i,j} \mathrm{Hom}_{G_k}(X_{L_j}, X_{K_i}) \cong \mathrm{Hom}_{G_k}(X_B, X_A),$$

where we are using Lemma 5.4.2(c), Theorem 5.4.3, and that a G_k-set morphism $X_B \to X_A$ must preserve the decomposition into G_k-orbits. Everything else is clear from Theorem 5.4.3. ■

As remarked earlier, this theorem amounts to the computation $\pi_1^{\text{ét}} \operatorname{Spec}(k) \cong G_k$.

5.5 Exercises

Exercise 5.1. Suppose we have field extensions $k \subset K, L \subset \Omega$ as in Proposition/Definition 5.1.1. Show that if either K or L is algebraic over k, then $K[L] = KL$, i.e. that the smallest subring of Ω containing K and L is a field. Come up with an example of fields k, K, L, and Ω as above for which $K[L] \subsetneq KL$.

Exercise 5.2.

(a) Let K, L be finite extensions of a field k such that $[K : k]$ and $[L : k]$ are relatively prime. Show that K and k are linearly disjoint over k.

(b) Show that $f(X) := X^5 + 4X^3 + 6X + 14 \in \mathbb{Q}[\sqrt{5}, \cos(2\pi/7)][X]$ is irreducible.

Exercise 5.3. Suppose $k \subset \Omega$ is a field extension, and that $k \subset K, L \subset \Omega$ intermediate *domains*. We say that K and L are linearly disjoint over k in Ω iff the natural map $K \otimes_k L \to \Omega$ is injective. Show that K and L are linearly disjoint over k in Ω iff their fraction fields $\operatorname{Frac} K$ and $\operatorname{Frac} L$ are .

Exercise 5.4. Show that if k is a field and $K, L \supset k$ two extension fields, then there is a field extension of k containing k-isomorphic copies of K and L.

Exercise 5.5. Let k be a field and Ω/k an extension field. Show that if K/k is a purely inseparable extension, then there is at most one k-embedding $K \to \Omega$.

Exercise 5.6. Partially generalize Theorem 5.1.3 as follows. Let k be a field and K/k be any extension such that k is algebraically closed in K. If L/k is a Galois extension (e.g. if k is perfect and L is an algebraic closure of k), then K and L are linearly disjoint over k.

Exercise 5.7. Let $\mathbb{F}$ be any imperfect field, so that $p := \operatorname{char} \mathbb{F} > 0$, and pick an $s \in \mathbb{F} \setminus \mathbb{F}^p$. Let $k := \mathbb{F}(t)$.

(a) Show that $X^p + sY^p + t \in k[X, Y]$ is irreducible.

Let $K := \operatorname{Frac} k[X, Y]/(X^p + sY^p + t)$. Let $k \to L$ be an algebraic closure of k, let $K \to \Omega$ be an algebraic closure of K, and extend the natural map $k \to K \to \Omega$ to an inclusion $L \to \Omega$. In what follows, identify k, K, and L with their images in Ω.

(b) Show that $K \cap L = k$ (i.e. k is algebraically closed in K), but that K and L are not linearly disjoint over k in Ω. In particular, K and $L \cong \overline{k}$ are not abstractly linearly disjoint over k.

Exercise 5.8. Let $k \subset K \subset L$ be a tower of field extensions. Show that $\operatorname{trdeg}_k L = \operatorname{trdeg}_k K + \operatorname{trdeg}_K L$.

Exercise 5.9. Let k be a field and $m, n \in \mathbb{Z}_{\geq 1}$ with $m > n$. Show that any collection of m polynomials say $f_1, \ldots, f_m$, in $k[X_1, \ldots, X_n]$ is algebraically dependent, i.e., satisfies a nontrivial algebraic relation.

Exercise 5.10. Let k be a field, and $K, L \supset k$ be two extension fields of k. Show that if K and L are everywhere linearly disjoint over k, then one of K or L is algebraic over k.

Exercise 5.11. Let k be a field and $K, L \supset k$ be two algebraic extensions of k. Show directly (i.e. without quoting Theorem 5.1.3) that if K is separable and L is purely inseparable, then K and L are linearly disjoint over k.

Exercise 5.12. For a field K and a collection of independent transcendental indeterminates $X = \{X_i\}_{i \in I}$, let $K(X)$ denote the purely transcendental extension of K obtained by adjoining the X_i.

(a) Show that if $K \subset L$ is an algebraic extension, then so is $K(X) \subset L(X)$ for any X.
(b) Show that if $K \subset L$ is any extension, then $\operatorname{trdeg}_K L = \operatorname{trdeg}_{K(X)} L(X)$.

Exercise 5.13. Let k be a field and $f(X) \in k[X]$ be a polynomial such that for every field extension K of k, if f has a root in K then f splits over K. Show that all irreducible factors of f have the same degree. In particular, if in addition f has prime degree and does not have a root in k, then f is irreducible over k.

Exercise 5.14. Show that the étale $\mathbb{F}_2$-algebra $A = \mathbb{F}_2^3$ is not isomorphic to $\mathbb{F}_2[X]/(f)$ for any $f \in \mathbb{F}_2[X]$.

Exercise 5.15. Let G be a profinite group and $n \geq 1$ an integer. Show that any continuous homomorphism $\rho : G \to \mathrm{GL}_n \mathbb{C}$ factors through a finite quotient of G.

Exercise 5.16. Let G be a topological group acting on a set X. Show that the following are equivalent:

(a) The action of G on X is continuous for the discrete topology on X.
(b) For each $x \in X$, the stabilizer $G_x \subset G$ of x in G is an open subgroup of G.
(c) Every element $x \in X$ is stabilized by some open subgroup $U_x \subset G$, i.e. $X = \bigcup_{U \leq G} X^U$, where the union is over open subgroups $U \leq G$.

In this situation, we call X a *discrete G-set*.

Chapter 6

Global Dimension Theory

6.1 Noether Normalization and Zariski's Lemma

The main theorem of this section is:

Theorem 6.1.1 (Noether Normalization)**.** Let k be a field and R be a finitely generated k-algebra. Then there exists an integer $r \geq 0$ and elements $z_1, \ldots, z_r \in R$ such that:

(a) The z_i's are algebraically independent over k, i.e. the map $k[Z_1, \ldots, Z_r] \to R$ given by $Z_j \mapsto z_j$ for $j = 1, \ldots, r$, is injective.

(b) R is integral over the image $k[z_1, \ldots, z_r]$.

Finally, if k is infinite, and we express R as $R \cong k[x_1, \ldots, x_n] = k[X_1, \ldots, X_n]/\mathfrak{a}$ for some integer $n \geq 0$ and ideal $\mathfrak{a} \subset k[X_1, \ldots, X_n]$, then the z_i can be chosen to be linear combinations of the x_i.

Proof. Start with a set $\{z_j\}_{j=1}^r$ for some $r \geq 0$ with R integral over $k[z_j]_{j=1}^r$ (e.g. we can start with any generating set, say $\{x_i\}_{i=1}^n$ if we are in the second situation). Either the z_i are algebraically independent, and we are done; or, $r \geq 1$ and there is a $0 \neq f \in k[Z_1, \ldots, Z_r]$ such that $f(z_1, \ldots, z_r) = 0$. As explained below, we can replace Z_j for $1 \leq j < r$ by Z'_j such that $k[Z_1, \ldots, Z_r] = k[Z'_1, \ldots, Z'_{r-1}, Z_r]$ and such that the polynomial f when written in these new variables is monic in Z_r (possibly after rescaling); and further, we can ensure that if k is infinite then the Z'_j are linear combinations of the Z_j. Having done this, we would conclude that z_r is integral over $k[z'_1, \ldots, z'_{r-1}]$, where each z'_j is the image of Z'_j, and then by 3.1.4(c), R would be integral over $k[z'_1, \ldots, z'_{r-1}]$. We have now reduced r by 1. Therefore, by repeating this process finitely many times we will arrive at an algebraically independent collection of the sort required.

For the transformation steps, first assume that k is infinite. Set $Z'_j := Z_j - \alpha_j Z_r$ for $1 \leq j < r$ for $\alpha_1, \ldots, \alpha_{r-1} \in k$ to be determined later. Let $\sum_I c_I Z^I$ be the sum of monomials of highest total degree $|I| =: N$ in f (so $c_I \neq 0$ for at least one I), and look at $\sum_I c_I \left(\prod_{j=1}^{r-1} (Z'_j + \alpha_j Z_r)^{i_j}\right) Z_r^{i_r}$. The coefficient of Z_r^N in this expansion is $c := \sum_I c_I \prod_{j=1}^{r-1} \alpha_j^{i_j}$. Since this is a nonzero polynomial in $k[\alpha_j]_{j=1}^{r-1}$ and k is infinite, we can choose $\alpha_1, \ldots, \alpha_{r-1}$ such that $c \neq 0$. Clearly, none of the the homogenous terms of f of total degree less than N can contribute to the coefficient of Z_r^N, so scaling by c^{-1}, we are done.

In the general case, consider integers ("weights") $w_1, \ldots, w_{r-1} \geq 0$ to be specified later, and set $w_r = 1$. Set $Z'_j := Z_j - Z_r^{w_j}$ for $1 \leq j < r$. In a typical monomial $c_I Z^I$ in f after substitution, we get a term of the form $c_I \left(\prod_{j=1}^{r-1} (Z'_j + Z_r^{w_j})^{i_j}\right) Z_r^{i_r}$. This has term of highest degree in Z_r that looks like Z_r to the power $\sum_{j=1}^r i_j w_j$. If we can pick the w_j in such a way that all of these sums over varying I are distinct, then we could pick a unique highest order term of power of Z_r in the changed polynomial, so after scaling we would be done. This is always possible because of 6.1.2 below. ■

Lemma 6.1.2. Suppose that $r \geq 1$ is an integer, and $\mathscr{I} = \{(i_1, \ldots, i_r) : i_1, \ldots, i_r \geq 0\}$ a *finite* set of ordered r-tuples of nonnegative integers. Then there are nonnegative integers $w_1, \ldots, w_{r-1}, w_r$, such that $w_r = 1$ and if $I \neq I' \in \mathscr{I}$ then $\sum_{j=1}^r i_j w_j \neq \sum_{j=1}^r i'_j w_j$.

Proof. Proceed by induction on r, with $r = 1$ clear. If $r \geq 2$, then by induction choose integers $w_2, \ldots, w_{r-1}, w_r \geq 0$ with $w_r = 1$ such that $\sum_{j=2}^r i_j w_j = \sum_{j=2}^r i'_j w_j \Rightarrow I = I'$. Now choose $w_1 > \max_{I \in \mathscr{I}} \{\sum_{j=2}^r i_j w_j\}$. ■

Remark 6.1.3. Geometrically, the Normalization Theorem says that every affine variety admits a finite surjective map to an affine space of its dimension. If the base field is infinite (as are usually the fields we work with in algebraic geometry), then in fact we can take this map to be a linear projection.

Corollary 6.1.4. If, in addition, R is an integral domain, then $r = \operatorname{trdeg}_k R$.

Proof. Let $K := \operatorname{Frac} R$. In the above notation, the integral closure $\operatorname{Cl}_K(k(z_1, \ldots, z_r)) \subset K$ is a field by 3.1.8(c) and contains R, so it must be K. In particular, K is algebraic over $k(z_1, \ldots, z_r)$, and hence $\operatorname{trdeg}_k R := \operatorname{trdeg}_k \operatorname{Frac} R = r$. ■

Remark 6.1.5. We will show below (6.2.8) that for $r \in \mathbb{Z}_{\geq 0}$, we have that $\dim k[Z_1, \ldots, Z_r] = r$. It will then follow from 3.2.6(a) that $\dim R = r$ as well. In all, this will show that if R is a finitely generated commuative k-algebra for some field k that is an integral domain, then $\dim R = \operatorname{trdeg}_k R$.

Now we derive plenty of delicious consequences. We begin with useful lemma.

Lemma 6.1.6 (Artin-Tate Lemma)**.** Let $R \subset S \subset T$ be rings. Suppose that R is Noetherian, T is a finitely generated R-algebra, and that T is integral over S (equivalently, T is a finite S-module). Then S is a finitely generated R-algebra.

Proof. Let $m, n \geq 1$ be integers such that e indcan pick generators $x_1, \ldots, x_m$ of T as an R-algebra, and $y_1, \ldots, y_n$ of T as an S-module. Then there are expressions of the form $x_i = \sum_j s_{ij} y_j$ and $y_i y_j = \sum_k s_{ijk} y_k$ for $s_{ij}, s_{ijk} \in S$. Let $S' := R[s_{ij}, s_{ijk}]_{i,j,k}$. Since R is Noetherian, so is S', being a finitely-generated R-algebra (1.3.5). Any element of T is a polynomial in the x_i with coefficients in R; substituting the above, we see that T is generated as an S'-module by the y_j; in particular, it is module-finite over S'. Since S' is Noetherian and S is a submodule of the finitely generated S'-module T, the ring S is module-finite over S'. Since S' is a finitely-generated R algebra, it follows that S is a finitely generated R-algebra as well. ■

Remark 6.1.7. Here is one historically significant application of the Artin-Tate Lemma: the construction of quotient varieties. Let k be a field, $n \geq 1$ an integer and G a finite group acting on a finitely generated k-algebra T, and we are interested in studying the G-invariants T^G. Lemma 6.1.6 applied to $R = k$ and $S = T^G$ says that the ring S of invariants is finitely generated.[1] A closer examination of the proof, however, reveals that it is not constructive; a variant of this proof in this special case, essentially due to Noether and Hilbert, was the impetus behind the development of a lot of commutative algebra (including the definition of Noetherian ring and the Hilbert Basis Theorem), and initially got Hilbert under fire (Gordan denounced this proof as "theology, not mathematics!") [TOCITE]. It was a long time before this proof technique, and nonconstructive techniques in commutative algebra, became mainstream.

We now come to one of the most fundamental results of the theory, of which we give six proofs.

Theorem 6.1.8 (Zariski's Lemma)**.** Let $k \subset K$ be a field extension. If K is a finitely generated k-algebra, then it is a finite algebraic extension.

Proof 1. Induct on $n \in \mathbb{Z}_{\geq 0}$, the minimal number of generators of K as a k-algebra, the case $n = 0$ being trivial. Suppose $n \geq 1$ and $K = k[x_1, \ldots, x_n]$ for some $x_1, \ldots, x_n \in K$. If K is not algebraic over k, at least one of the x_i, say x_1, is not algebraic over k. Then $k(T) \cong k(x_1) \subset K$,

[1] In modern algebraic geometry, this is saying that the quotient of the finitely generated affine k-scheme $\operatorname{Spec}(T)$ by the action of G is still of the same type, i.e., a geometric quotient of $\operatorname{Spec}(T)$ by G exists in this category. It is also clear that if T is reduced, then so is T^G: the quotient of an affine k-variety by a finite group G is also one.

and K is generated as a $k(x_1)$ algebra by $x_2, \ldots, x_n$, so by induction $x_2, \ldots, x_n$ are algebraic over $k(x_1)$. By clearing out denominators in equations of algebraic dependence, we can find an $f \in k[x_1]$ such that $fx_2, \ldots, fx_r$ are integral over $k[x_1]$. Now let $g \in k[x_1]$ be an irreducible not dividing f; this is possible, since $k[x_1]$ is a PID with infinitely many irreducibles.[2] Then $1/g \in k(x_1) \subset K = k[x_1, \ldots, x_n]$ implies that there is an $N \gg 1$ such that $f^N/g \in k[x_1, fx_2, \ldots, fx_n]$. Then $f^N/g \in k(x_1)$ is integral over $k[x_1]$. But $k[x_1]$ is a UFD and hence normal (3.1.5), so $f^N/g \in k[x_1]$, i.e. $f^N = gh$ for some $h \in k[x_1]$, a contradiction. ■

Proof 2. Let $K = k[x_1, \ldots, x_n]$. If K is not algebraic over k, then $n \geq 1$ we may reorder the x_i to arrange that $x_1, \ldots, x_r$ are algebraically independent over k for some $r \geq 1$ and that each of $x_{r+1}, \ldots, x_n$ are algebraic over $k(x_1, \ldots, x_r)$. Applying 6.1.6 to $R = k, S = k(x_1, \ldots, x_r), T = K$, it follows that the purely transcendental extension $k(x_1, \ldots, x_r)$ is a finitely generated k-algebra, say $k(x_1, \ldots, x_r) = k[y_1, \ldots, y_s]$ for some $s \geq 1$. Then each $y_i = f_j/g_j$ for some polynomials f_j, g_j in $x_1, \ldots, x_r$. Since there are infinitely many irreducible polynomials in $k[x_1, \ldots, x_n]$, we may pick an irreducible $g \in k[x_1, \ldots, x_n]$ that does not divide $g_1 \cdots g_s$. Then the element $g^{-1} \in k[y_1, \ldots, y_s]$ implies that g^{-1} is polynomial in $y_1, \ldots, y_s$, which is not possible; this contradiction shows that K is algebraic over k. ■

Proof 3. From Noether Normalization (6.1.1), we can write $k \subset k[z_1, \ldots, z_r] \subset K$ where the first extension is polynomial and the second extension is integral. But from 3.1.8(c), we get that since K is a field, so must be $k[z_1, \ldots, z_r]$. This is only possible if $r = 0$. ■

Proof 4. Taking $R = k$, $S = K$, and $\varphi : k \hookrightarrow \Omega$ an algebraic closure of k, in Lang's Lemma (3.3.1(b)) gives an extension $\hat{\varphi} : K \to \Omega$. Since K is a field, this last homomorphism is injective, and so K is algebraic over k. Since it is a finitely generated k-algebra, it is finite algebraic. ■

Finally, we record two more proofs that use tools beyond our discussion so far.

Proof 5. By 6.2.8(a) below, we have $0 = \dim K = \operatorname{trdeg}_k K$, so that K/k is algebraic. ■

Proof 6. If K is not algebraic over k, then there is an inclusion $k[X] \hookrightarrow K$ of the polynomial ring $k[X]$ into K. This gives rise to a dominant morphism $\pi : \operatorname{Spec} K \to \mathbb{A}^1_k$ of finite-type k-schemes. By Chevalley's Theorem, the image of π is constructible, but the image of π is the generic point of $\mathbb{A}^1_k$, which is *not* constructible. ■

[2] For instance, by the same argument as the infinitude of primes.

6.2 Some Classical Algebraic Geometry

6.2.1 The Classical Nullstellensatz

In classical algebraic geometry, we look at the vanishing loci of polynomials in affine space.

Definition 6.2.1. For an integer $n \geq 1$ and ring k, the *k-points of affine n-space* is the set

$$\mathbb{A}^n(k) = \{(a_1, \dots, a_n) : a_i \in k\}$$

of ordered n-tuples of elements of k.

In what follows, we fix an $n \in \mathbb{Z}_{\geq 1}$. In modern algebraic geometry, this is the set of k-points of the universal affine n-space $\mathbb{A}^n_{\mathbb{Z}} = \operatorname{Spec} \mathbb{Z}[X_1, \dots, X_n]$. In classical algebraic geometry, in the absence of the notion of Spec, this was the geometric space on which algebraic geometry was done. Here's a version that we will set up.

Fix a field k and an algebraic closure $\overline{k}$ of k. Associate to each subset $\mathfrak{a} \subset k[X_1, \dots, X_n]$ its vanishing locus $\mathbb{V}(\mathfrak{a}) \subset \mathbb{A}^n(\overline{k})$, and to each subset $X \subset \mathbb{A}^n(\overline{k})$ the ideal $\mathbb{I}(X) \subset k[X_1, \dots, X_n]$ of polynomials over k vanishing on it. Then with this notation we have

Theorem 6.2.2 (Hilbert's Nullstellensatz)**.**

(a) If $\mathfrak{a} \subset k[X_1, \dots, X_n]$ is a proper ideal, then $\mathbb{V}(\mathfrak{a}) \neq \emptyset$.
(b) If $\mathfrak{a} \subset k[X_1, \dots, X_n]$ is any ideal, then $\mathbb{I}(\mathbb{V}(\mathfrak{a})) = \sqrt{\mathfrak{a}}$.

Proof.

(a) Since $\mathfrak{a}$ is proper, there is a maximal ideal $\mathfrak{m} \subset k[X_1, \dots, X_n]$ containing $\mathfrak{a}$. Then $\mathbb{V}(\mathfrak{m}) \subset \mathbb{V}(\mathfrak{a})$. Therefore, it suffices to do the case when $\mathfrak{a}$ is maximal. In this case, the quotient $K := k[X_1, \dots, X_n]/\mathfrak{a}$ is a field extension which is a finitely generated k-algebra, and hence by Zariski's Lemma 6.1.8, it is a finite algebraic extension. In particular, there is a k-embedding $\varphi : K \to \overline{k}$, and then the point $(\varphi(\overline{X}_1), \dots, \varphi(\overline{X}_n)) \in \mathbb{V}(\mathfrak{a}) \subset \mathbb{A}^n(\overline{k})$.

(b) The inclusion $\sqrt{\mathfrak{a}} \subset \mathbb{I}(\mathbb{V}(\mathfrak{a}))$ is clear. For the other direction, we use the *Rabinowitsch trick*: if $f \in \mathbb{I}(\mathbb{V}(\mathfrak{a}))$, then in $k[X_1, \dots, X_{n+1}]$, the ideal $\mathfrak{b} := (\mathfrak{a}, f \cdot X_{n+1} - 1)$ has the property that $\mathbb{V}(\mathfrak{b}) = \emptyset$. By (a), $\mathfrak{b} = (1)$. Therefore,

$$\begin{aligned} 0 &= k[X_1, \dots, X_n]/\mathfrak{b} \\ &\cong (k[X_1, \dots, X_n]/\mathfrak{a})\, [X_{n+1}]/(\overline{f} \cdot X_{n+1} - 1) \\ &\cong (k[X_1, \dots, X_n]/\mathfrak{a})\, [\overline{f}^{-1}], \end{aligned}$$

which by 1.1.4 gives us that $\overline{f} \in \operatorname{Nil}(k[X_1, \dots, X_n]/(\mathfrak{a}))$ as needed.

■

Corollary 6.2.3. Suppose that $k = \overline{k}$, i.e., that k is algebraically closed. Then there is a bijection between $\mathbb{A}^n(k)$ and the maximal ideals of $k[X_1, \dots, X_n]$, given by sending a point $(a_1, \dots, a_n)$ to the ideal $(X_1 - a_1, \dots, X_n - a_n)$.

Proof. This map is clearly well-defined and injective. For any maximal ideal $\mathfrak{m} \subset k[X_1, \dots, X_n]$, 6.2.2(a) tells us that there is an $(a_1, \dots, a_n) \in \mathbb{A}^n(k)$ such that $\mathfrak{m} \supset (X_1 - a_1, \dots, X_n - a_n)$; but the latter is already a maximal ideal. ■

In fact, the above set-up can be used to give an antitone Galois connection between the k-subvarieties of $\mathbb{A}^n(\overline{k})$ and radical ideals in $k[X_1, \dots, X_n]$; but that belongs properly to a course on classical algebraic geometry. This observation is also the starting point of modern algebraic geometry, which systematically studies not only maximal ideals of polynomial rings over a field but rather all prime ideals of arbitrary rings as its “points”.

Remark 6.2.4. It is true the statement of 6.2.2(a) would also have been true if $\overline{k}$ were to denote only a *separable* closure of k. Indeed, this is immediate when k has characteristic zero, and in characteristic $p > 0$, the extension k^{alg}/k^s is purely inseparable.

6.2.2 Jacobson Rings

The Nullstellensatz implies that (when k is algebraically closed) for any ideal $\mathfrak{a} \subset k[X_1, \dots, X_n]$ we have $\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{m} \supset \mathfrak{a}} \mathfrak{m}$ (check!). We call rings with this property *Jacobson rings*; this is developed systematically in

Theorem/Definition 6.2.5 (Jacobson Rings)**.** The following conditions on a ring R are equivalent:

(a) In every quotient ring of R, the nilradical equals the Jacobson radical.
(b) Every radical ideal in R is the intersection of maximal ideals.
(c) Every prime ideal in R is the intersection of maximal ideals.
(d) If S is a domain quotient of R and there is a $0 \neq x \in S$ such that $S[x^{-1}]$ is a field, then S is a field.
(e) Every finitely generated algebra over R that is a field is finitely generated as an R-module.

A ring satisfying the above equivalent conditions is said to be a *Jacobson ring.* In this situation:

(f) If S is a finitely generated R-algebra by $\varphi : R \to S$, then S is also Jacobson. Further, if $\mathfrak{m} \subset S$ is maximal, then so is $\varphi^{-1}\mathfrak{m} \subset R$ and hence $S/\mathfrak{m}$ is a finite algebraic extension of $R/\varphi^{-1}\mathfrak{m}$.

Remark 6.2.6. Geometrically, a morphism of Jacobson schemes which is locally of finite type (e.g., that of varieties over a field) maps closed points to closed points; this fact enabled classical algebraic geometers to stick to closed points in their interpretation of the *geometry* of algebraic geometry. The statement (f) above is often called the generalized Nullstellensatz.

Proof.

(a) ⇒ (b) Let $\mathfrak{a} \subset R$ be a radical ideal. Then in $R/\mathfrak{a}$ we have $0 = \mathrm{Nil}(R/\mathfrak{a}) = \mathrm{Jac}(R/\mathfrak{a}) = \bigcap_{\mathfrak{m} \subset R/\mathfrak{a}} \mathfrak{m}$, so in R we have $\mathfrak{a} = \bigcap_{\mathfrak{m} \supset \mathfrak{a}} \mathfrak{m}$.

(b) ⇒ (c) Clear.

(c) ⇒ (a) If $\mathfrak{a} \subset R$ is any ideal, then $\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{p} \supset \mathfrak{a}} \mathfrak{p} = \bigcap_{\mathfrak{m} \supset \mathfrak{a}} \mathfrak{m}$, where the first statement is 1.2.2, and the second uses the hypothesis (c). Therefore, $\mathrm{Nil}(R/\mathfrak{a}) = \sqrt{0(R/\mathfrak{a})} = \bigcap_{\mathfrak{m} \subset R/\mathfrak{a}} \mathfrak{m} = \mathrm{Jac}(R/\mathfrak{a})$.

(c) ⇒ (d) Let $\mathfrak{p} := \ker(R \to S)$, and lift x to an $\tilde{x} \in R \setminus \mathfrak{p}$. By hypothesis, there is a maximal ideal $\mathfrak{m}$ containing $\mathfrak{p}$ but not $\tilde{x}$; this corresponds to a maximal ideal of S not containing x and hence by 1.1.12(d) a proper prime ideal of $S[x^{-1}]$, which must be (0); therefore, $\mathfrak{p} = \mathfrak{m}$.

(d) ⇒ (c) We have to show that given a prime $\mathfrak{p}$ and $x \notin \mathfrak{p}$, there is a maximal $\mathfrak{m}$ containing $\mathfrak{p}$ such that $x \notin \mathfrak{m}$. In this case, $(R/\mathfrak{p})[x^{-1}]$ is not the zero ring and therefore has a maximal ideal $\mathfrak{m}_0$; then $\mathfrak{m} := \varphi^{-1}\mathfrak{m}_0$ is a prime in R containing $\mathfrak{p}$ and not containing x, where $\varphi : R \twoheadrightarrow R/\mathfrak{p} \xrightarrow{\eta} (R/\mathfrak{p})[x^{-1}]$. We claim that $\mathfrak{m}$ is maximal. Indeed, the composite $R \twoheadrightarrow R/\mathfrak{p} \xrightarrow{\eta} (R/\mathfrak{p})[x^{-1}] \twoheadrightarrow (R/\mathfrak{p})[x^{-1}]/\mathfrak{m}_0 := K$ has kernel exactly $\mathfrak{m}$ and so gives an injection $R/\mathfrak{m} \hookrightarrow K$; since $x \notin \mathfrak{m}$, this extends to a map $(R/\mathfrak{m})[x^{-1}] \hookrightarrow K$. But by construction of K this map is also clearly surjective, and so an isomorphism. By (d) applied to $S = R/\mathfrak{m}$, we conclude that $\mathfrak{m}$ is maximal.

(d) $\Rightarrow$ (e) Suppose that K is a field and a finitely generated R-algebra via $\varphi : R \to K$. Replacing R by $R/\ker\varphi$, we may assume that R is a domain; let $k := \operatorname{Frac} R$. Since K is a finitely generated R-algebra, it is also a finitely generated k-algebra, so by Zariski's Lemma (6.1.8), K/k is finite algebraic. For the finitely many generators of x_i of K/k, write down equations of algebraicity and take a large common denominator $0 \neq x \in R$ of the coefficients so that $R[x^{-1}] \hookrightarrow K$ is an integral extension. By 3.1.8(c), $R[x^{-1}]$ is a field, so that by hypothesis $R = k$. Since K/k is finite, we are done.

(e) $\Rightarrow$ (d) Let S and x be as given. Since $S[x^{-1}]$ is a finitely generated R-algebra that is a field, by (e) it is integral over R. Writing an equation of integral dependence of x^{-1} of degree $n \geq 1$ and multiplying throughout by x^n shows then that $x^{-1} \in S$ and hence $S = S[x^{-1}]$ is a field.

(f) The ring S clearly satisfies (e). Finally, if $\mathfrak{m} \subset S$ is maximal, then $S/\mathfrak{m}$ is a finitely generated R-algebra that is a field, so by (e) again $S/\mathfrak{m}$ is integral over R. Then $R/\varphi^{-1}\mathfrak{m} \subset S/\mathfrak{m}$ is an integral extension of domains with $S/\mathfrak{m}$ a field, so by 3.1.8(d), $\varphi^{-1}\mathfrak{m}$ is maximal.

■

Example 6.2.7.

(a) Fields and hence finitely generated algebras over fields are Jacobson; this is the classical Nullstellensatz.
(b) A Dedekind domain is Jacobson iff it has infinitely many prime ideals (7.2). In particular, if K is a number field, then $\mathcal{O}_K$ is a Jacobson ring.
(c) A local domain that is not a field is not Jacobson; see also 6.1.

6.2.3 Dimension of Affine Varieties

Let us now return to a little bit of dimension theory. The key result we are after is

Theorem 6.2.8. Let k be a field and R be a finitely generated k-algebra which is a domain.

(a) We have $\dim R = \operatorname{trdeg}_k R$.
(b) For $n \in \mathbb{Z}_{\geq 0}$, we have $\dim k[X_1, \ldots, X_n] = n$.
(c) If S is any finitely generated k-algebra (that is not necessarily a domain), then $\dim S < \infty$.
(d) For any prime $\mathfrak{p} \subset R$, equality holds in $\operatorname{ht}\mathfrak{p} + \operatorname{coht}\mathfrak{p} \leq \dim R$. In particular, if $\mathfrak{p} = \mathfrak{m}$ is maximal, the $\operatorname{ht}\mathfrak{m} = \dim R$.

In fact, the length of any maximal chain of primes in R is exactly $\dim R$ (i.e., R is "(universally) catenary", although establishing that needs a little more work, e.g., a refined version of the normalization lemma [TOCITE]). The statements (b) and (c) follow immediately from (a), and by previous discussion (6.1.5), to show (a), it suffices to show (b), and indeed only that $\dim k[X_1, \ldots, X_n] \leq n$, since the other inequality is obvious. Let's first isolate this bit of the proof.

Proof of 6.2.8(a)-(c). We induct on $n = \operatorname{trdeg}_k R$, and, as above, reduce to showing $\dim k[X_1, \ldots, X_n] \leq n$. This is clearly true for $n = 0$. Suppose $n \geq 1$, and we have shown the result for all R' with $\operatorname{trdeg}_k R' \leq n - 1$. Suppose there is a chain of primes $(0) = \mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_m$ of length $m \in \mathbb{Z}_{\geq 1}$ in $k[X_1, \ldots, X_n]$. Replace $\mathfrak{p}_1$ by (f) for some irreducible $f \in k[X_1, \ldots, X_n]$. In the quotient $R' := R/(f)$, we get a chain of length $m - 1$, so that $m - 1 \leq \dim R'$. But 5.2.4 tells us that $\operatorname{trdeg}_k R' = n - 1$, so that by the inductive hypothesis, $\dim R' = n - 1$, finishing the proof. ■

Finally, let's prove statement (d).

Proof of 6.2.8(d). If $\operatorname{ht}\mathfrak{p} = 0$, then $\mathfrak{p} = (0)$ (since R is a domain) and the result is clear. Assuming first the result when $\operatorname{ht}\mathfrak{p} = 1$, we show it for general $\mathfrak{p}$ by induction on height. Therefore, suppose now that $h := \operatorname{ht}\mathfrak{p} \geq 2$, and suppose that $0 = \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_h = \mathfrak{p}$ is a chain of primes of height h. In the quotient $R/\mathfrak{p}_1$, the prime $\mathfrak{p}/\mathfrak{p}_1$ has height $h-1$, and so by induction we conclude that

$$h - 1 + \dim R/\mathfrak{p} = \dim R/\mathfrak{p}_1.$$

Now by the case of height 1 applied to $\mathfrak{p}_1$, we conclude that $1 + \dim R/\mathfrak{p}_1 = \dim R$, and hence the result.

It remains to deal with the case when $\operatorname{ht}\mathfrak{p} = 1$, i.e., when $\mathfrak{p}$ is a minimal nonzero prime; then we want to show that $\dim R/\mathfrak{p} \geq \dim R - 1$. Suppose that $\dim R = r$, and using Noether Normalization (6.1.1) pick an injective integral morphism $\varphi : k[Z_1, \ldots, Z_r] \to R$. If $\varphi^{-1}(\mathfrak{p}) = (0)$, then we get an injective integral morphism $k[Z_1, \ldots, Z_r] \hookrightarrow R/\mathfrak{p}$ and hence that $\dim R/\mathfrak{p} = r$ as well (3.2.6(a)), contradicting the inequality $\dim R/\mathfrak{p} \leq r - 1$ which we knew already; therefore, we may pick a nonzero irreducible $f \in \varphi^{-1}(\mathfrak{p})$. If $(f) \subsetneq \varphi^{-1}(\mathfrak{p})$, then by Going Down (3.2.5(b)) applied to the extension $k[Z_1, \ldots, Z_r] \subset R$, there would be a nonzero prime $\mathfrak{q} \subset \mathfrak{p}$ such that $\varphi^{-1}(\mathfrak{q}) = (f)$, contradicting that $\operatorname{ht}\mathfrak{p} = 1$; therefore, $\varphi^{-1}(\mathfrak{p}) = (f)$ is principal. This gives us an injective integral morphism $k[Z_1, \ldots, Z_r]/(f) \hookrightarrow R/\mathfrak{p}$, and so again 3.2.6(a) reduces us to showing that $\dim k[Z_1, \ldots, Z_r]/(f) = r - 1$, which was done above. ■

6.3 Exercises

Exercise 6.1. Show that a local ring is a Jacobson ring iff it has Krull dimension zero.

Exercise 6.2. Let k be a field and R an Artinian ring that is a finitely generated k-algebra. Show that R is a finite dimensional k-vector space. Show that R can be written as a finite direct product of Artinian local rings R_i which are all finitely generated k-algebras; let k_i denote the residue field of R_i. Show that, in this case, each k_i is a finite extension of k, and that $\dim_k(R) = \sum_i \dim_k(R_i)$ and $\ell_R(R) = \sum_i \dim_k(R_i) \cdot [k_i : k]^{-1}$. Conclude that if k is algebraically closed, then $\ell_R(R) = \dim_k(R)$. Give an explicit example to show that this last result fails if k is not algebraically closed.

Exercise 6.3. Let $(R, \mathfrak{m}, k)$ be a Noetherian local ring and $f \in m$ a nonzerodivisor in R. Show that if $R/(f)$ is regular, then so is R.

Chapter 7

Valuation Rings and Dedekind Domains

7.1 Valuation Rings and Discrete Valuation Rings

An abelian group Γ with a translation-invariant total order $\leq$ is said to be an *ordered abelian group*; to such a group we associate an ordered abelian monoid $\Gamma^+ := \Gamma \sqcup \{\infty\}$ by defining $\infty + \xi = \infty$ and $\xi \leq \infty$ for all $\xi \in \Gamma$.

Definition 7.1.1. Let R be a domain, and Γ be an ordered abelian group.

(a) A Γ-*valued valuation on* R, written $v : R \to \Gamma$, is a monoid homomorphism $v : (R, \cdot) \to \Gamma^+$ satisfying that for $x \in R$ we have $v(x) = \infty$ iff $x = 0$, and for all $x, y \in R$, we have

$$v(x + y) \geq \min\{v(x), v(y)\}.$$

In the above situation, v can be uniquely extended to a Γ-valued valuation on the fraction field $K := \operatorname{Frac} R$ by $v(x/y) = v(x) - v(y)$ whenever $x, y \in R$ with $y \neq 0$. Therefore, it suffices to talk about valuations on fields.

(b) Suppose K is a field and $v : K \to \Gamma$ is a valuation. Then we define the *value group* of v to be the subgroup $v(K^\times) \subset \Gamma$, the *valuation ring* of v to be

$$\mathcal{O}_v := \{x \in K : v(x) \geq 0\},$$

and the *maximal ideal* to be

$$\mathfrak{m}_v := \{x \in R : v(x) > 0\}.$$

(c) A valuation $v : K \to \Gamma$ is said to be a *discrete valuation* if the value group of v is isomorphic to $\mathbb{Z}$ as an ordered abelian group; in this case, identifying the value group with $\mathbb{Z}$, we say that an element $\pi \in K$ is a *uniformizing parameter*, or *uniformizer*, if $v(\pi) = 1$ (i.e., if $v(\pi) > 0$ is a generator of the value group). The valuation ring of a discrete valuation is called a *discrete valuation ring.*

Remark 7.1.2. If Γ is any ordered abelian group, then there is a field K and a Γ-valued valuation on K with value group Γ; in fact, K can be chosen to be of any characteristic, and indeed $K = \operatorname{Frac} k[\Gamma]$ suffices for any base field k. See [4, Exercise 5.33]. For a suitable choice of Γ, this can be used to construct a nonempty scheme with no closed points. See [14, Exercise 3.3.27].

Remark 7.1.3. It is easy to check (do!) that in (b) above, given $x \in K^\times$ we have $v(x^{-1}) = -v(x)$, we have $x \in \mathcal{O}_v^\times$ iff $v(x) = 0$, and that $\mathfrak{m}_v = \mathcal{O}_v \smallsetminus \mathcal{O}_v^\times$ is an ideal, so by 1.2.7, the nomenclature above is justified: $\mathcal{O}_v$ is a local domain with the unique maximal ideal $\mathfrak{m}_v$. In this case, note that $K = \operatorname{Frac} \mathcal{O}_v$; in fact, for any $x \in K^\times$ we have either $x \in \mathcal{O}_v$ or $x^{-1} \in \mathcal{O}_v$. And indeed, this property characterizes all rings that arise in this way; this is the content of 7.1.5 below.

Example 7.1.4.

(a) Let R be a UFD and $f \in R$ an irreducible element. Associated to f we get a discrete valuation $v_f : R \to \mathbb{Z}$ given by sending a nonzero $x \in R$ to the exact power of f dividing x. If $K = \operatorname{Frac} R$, then the corresponding (discrete) valuation ring is $R_{(f)} \subset K$ with uniformizer f. For instance, taking $R = \mathbb{Z}$ and $f = p$ recovers the p-adic valuation on $\mathbb{Q}$; taking $R = k[X]$ for a field k and f an irreducible polynomial produces an f-adic valuation on $k(X)$.

(b) For any field k, the maps $\deg : k(X) \to \mathbb{Z}$ and $\operatorname{ord} : k(\!(X)\!) \to \mathbb{Z}$ are both discrete valuations with uniformizer X.

(c) For any field k and $n \in \mathbb{Z}_{\geq 1}$, we have a valuation $\operatorname{mult}_0 : k[X_1, \dots, X_n] \to \mathbb{Z}$ given by taking the multiplicity at 0; this extends to a discrete valuation on $k(X_1, \dots, X_n)$ with each X_i a uniformizer. This is an example of a divisorial valuation: it corresponds to taking the order along the exceptional divisor in the blow-up of $\mathbb{A}^n_k$ at the origin.

Valuation rings form an important class of rings which admits several equivalent characterizations.

Theorem/Definition 7.1.5 (Valuation Rings)**.** Let $R \subset K$ be a ring extension with K a field. Then the following are equivalent:

(a) There is an ordered abelian group Γ and a Γ-valued valuation v on K such that $R = \mathcal{O}_v$.
(b) For all $x \in K^\times$, either $x \in R$ or $x^{-1} \in R$.
(c) The ideals of R are totally ordered by inclusion and $K = \operatorname{Frac} R$.
(d) The principal ideals of R are totally ordered by inclusion and $K = \operatorname{Frac} R$.
(e) The ring R is local, every finitely generated ideal of R is principal, and $K = \operatorname{Frac} R$.
(f) The ring R is local and is maximal with respect to dominance in K.[1]
(g) There is an algebraically closed field Ω and a ring homomorphism $R \to \Omega$ that cannot be extended to a ring homomorphism from a bigger subring of K.

A domain R satisfying these equivalent properties (for some field K, which must *a posteriori* be the fraction field of R) is said to be a *valuation ring.* Further, if R is a valuation ring with fraction field K, then:

(h) Any subring of K containing R is also a valuation ring.
(i) Every nonzero localization of R is a valuation ring.
(j) Every quotient of R by a prime ideal (i.e., every integral domain quotient of R) is a valuation ring.
(k) The domain R is normal, i.e., $\operatorname{Cl}_K(R) = R$.

Proof. The implication (a) ⇒ (b) was noted above (7.1.3), and (c) ⇒ (d) ⇒ (b) as well as (c) ⇒ (e) are clear. Finally, (g) ⇒ (b) follows immediately from 3.3.1(c).

(b) ⇒ (a) Let $\Gamma := K^\times / R^\times$, and given $\xi, \eta \in \Gamma$ represented by $x, y \in K^\times$ respectively, say $\xi \leq \eta$ iff $yx^{-1} \in R$. Then, by (b), Γ is an ordered abelian group, and the natural projection $v : K^\times \to \Gamma$ extended by $v(0) = \infty$ is the required valuation.

(b) ⇒ (c) Let $\mathfrak{a}, \mathfrak{b} \subset R$ be ideals, and suppose there is a $x \in \mathfrak{a} \setminus \mathfrak{b}$. Then for any nonzero $y \in \mathfrak{b}$, the fraction x/y cannot be in R, and hence $y/x \in R$, whence $y \in \mathfrak{a}$. This shows $\mathfrak{b} \subset \mathfrak{a}$.

(d) ⇒ (e) Locality follows from (d) ⇒ (c), and the second statement is clear.

(e) ⇒ (d) Let $\mathfrak{m} \subset R$ be the maximal ideal, and $k := R/\mathfrak{m}$. If $x, y \in R$ are any elements, then since (x, y) is principal, $k \otimes_R (x, y) = (x, y)/\mathfrak{m} \cdot (x, y)$ is one-dimensional over k. Therefore, there are $s, t \in R$, not both in $\mathfrak{m}$, such that $sx + ty \in \mathfrak{m} \cdot (x, y)$, so let $u, v \in \mathfrak{m}$ be such that $sx + ty = ux + vy$. Then $(s - u)x = (v - t)y$. If, say, $s \notin \mathfrak{m}$, then $s - u \notin \mathfrak{m}$ as well, and then $(x) \subset (y)$.

(b) ⇒ (f) Locality follows from the implication (a) ⇒ (b). If $S \subset K$ is a local ring such that $R \subset S$ and $\mathfrak{m}_R \subset \mathfrak{m}_S$ and $x \in S \setminus R$, then $x^{-1} \in \mathfrak{m}_R \subset \mathfrak{m}_S$, contradicting $x \in S$.

(f) ⇒ (g) Let $\mathfrak{m}$ be the maximal ideal, and $k = R/\mathfrak{m}$, and fix an algebraic closure $k \to \Omega$ of k. We claim that map $R \to \Omega$ has this property. Indeed, if it extends to a subring $S \subset K$, say via $\varphi : S \to \Omega$ with kernel $\mathfrak{p} := \ker \varphi$, then $S_\mathfrak{p}$ is a local subring of K dominating R, forcing $S_\mathfrak{p} = R \subset S \subset S_\mathfrak{p}$.

This finishes the proof of the equivalence of (a)-(g). Clearly, (b) ⇒ (h) ⇒ (i).

(j) Follows from (i) combined with the fact that if $\mathfrak{p} \subset R$ is a prime, then $R_\mathfrak{p} \to \operatorname{Frac}(R/\mathfrak{p})$ is

[1] This last property says that if $S \subset K$ is a local ring such that $R \subset S$ and $\mathfrak{m}_R \subset \mathfrak{m}_S$, then $R = S$.

surjective.

(k) If $x \in K^\times$ is such that for some integer $n \geq 1$ and elements $a_1, \dots, a_n \in R$ we have $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ and $x^{-1} \in R$, then multiplying throughout by x^{-n+1} yields also that $x \in R$.

■

Corollary 7.1.6. Let $R \subset K$ be any extension with K a field. Then the normalization of R in K is the intersection of all valuation rings of K containing R.

Proof. One inclusion follows from 7.1.5(k). Conversely, if $x \notin \mathrm{Cl}_K(R)$, then $x^{-1} \notin R[x^{-1}]^\times$, and hence there is a maximal ideal $\mathfrak{m}$ of $R[x^{-1}]$ containing x. Pick an algebraic closure Ω of $R[x^{-1}]/\mathfrak{m}$, and consider the corresponding $\varphi : R[x^{-1}] \to \Omega$. By Zorn's Lemma, this admits a maximal extension $\hat{\varphi} : S \to \Omega$ to a subring S of K, which by 7.1.5(g) is a valuation ring of K containing $R[x^{-1}]$. Since $x^{-1} \in S$ with $\hat{\varphi}(x^{-1}) = 0$, we conclude that S is a valuation ring of K containing R but not containing x. ■

Finally, we are able to characterize discrete valuation rings (i.e., valuation rings of discrete valuations), abbreviated DVRs, as rings with even more special properties.

Theorem 7.1.7 (DVRs)**.** The following conditions on a nonzero ring R are equivalent.

(a) R is a discrete valuation ring.
(b) R is a Noetherian valuation ring that is not a field.
(c) R is a Noetherian domain that is a maximal proper subring of its field of fractions.
(d) R is a local PID that is not a field.
(e) R is a UFD with a unique irreducible up to associates, i.e., multiplication by units.
(f) $(R, \mathfrak{m})$ is a local domain that is not a field and the following equivalent conditions hold.
  (f1) Containment is division for (integral) ideals: if $\mathfrak{a} \subset \mathfrak{b}$ are ideals in R, then there is an ideal $\mathfrak{c} \subset R$ such that $\mathfrak{a} = \mathfrak{b} \cdot \mathfrak{c}$.
  (f2) Containment is division for fractional ideals: if $\mathfrak{f} \subset \mathfrak{g}$ are fractional ideas in R, then there is a fractional ideal $\mathfrak{h}$ such that $\mathfrak{f} = \mathfrak{g} \cdot \mathfrak{h}$.
  (f3) Every nonzero fractional ideal is invertible.
  (f4) Every nonzero (integral) ideal is invertible.
  (f5) Every nonzero prime ideal is invertible.
  (f6) The only nonzero prime is $\mathfrak{m}$ and $\mathfrak{m}$ is invertible.
  (f7) Every nonzero ideal is a finite product of primes.
  (f8) Every nonzero ideal is a power of $\mathfrak{m}$.
  (f9) If $\mathfrak{a} \subset R$ is a nonzero ideal and $0 \neq a \in \mathfrak{a}$, then there is a $b \in \mathfrak{a}$ such that $\mathfrak{a} = (a, b)$.
(g) $(R, \mathfrak{m})$ is a Noetherian local ring such that the following equivalent conditions hold.
  (g1) $\operatorname{edim} R = 1$ (i.e., $\mathfrak{m}$ nonzero and principal) and R is a domain.
  (g2) $\dim R = 1$ and $\mathfrak{m}$ is principal (i.e., R is a regular local ring of dimension one).
  (g3) $\dim R = 1$ and R is a domain such that the only $\mathfrak{m}$-primary ideals are powers of $\mathfrak{m}$.
  (g4) $\dim R = 1$ and R is a UFD.
  (g5) $\dim R = 1$ and R is a normal domain.
  (g6) R is a normal domain that is not a field, and for any $x \in \mathfrak{m} \smallsetminus \{0\}$, we have $\mathfrak{m} \in \mathrm{Ass}(R/(x))$.
  (g7) R is a normal domain and for some $x \in \mathfrak{m} \smallsetminus \{0\}$ we have $\mathfrak{m} \in \mathrm{Ass}(R/(x))$.

In this case:

(h) The only prime ideals of R are (0) and $\mathfrak{m}$.
(i) The following conditions on an element $\pi \in R$ are equivalent.
  (j1) For *any* discrete valuation as in (a), π is a uniformizer.

(j2) For *some* discrete valuation as in (a), π is a uniformizer.

(j3) We have $\pi \in \mathfrak{m} \smallsetminus \mathfrak{m}^2$.

(j4) The element π generates the maximal ideal $\mathfrak{m}$.

In this case, $\operatorname{Frac} R = R[\pi^{-1}]$.

(j) The discrete valuation as in (a), when normalized to be $\mathbb{Z}$-valued, is determined uniquely (i.e., there is only one discrete valuation on a discrete valuation ring). It is given explicitly as follows: let π be any generator of $\mathfrak{m}$; every element of $K^\times$ be written uniquely as $u\pi^n$ for some $u \in R^\times$ and $n \in \mathbb{Z}$, and this has valuation n.

For the proof of a theorem such as this one, there are many different possible paths, some using more technology than others. We present one approach; the reader is encouraged to come up with their own proofs of the implications here.

Proof. First, we show the equivalence of (a)-(e).

(a) $\Rightarrow$ (c) Let v be a $\mathbb{Z}$-valued discrete valuation on $K = \operatorname{Frac} R$ with valuation ring $R = \mathcal{O}_v$; then $R \subsetneq K$ else $v(K^\times)$ would be trivial. If $\mathfrak{a} \subset R$ is a nonzero ideal and $x \in \mathfrak{a}$ chosen with smallest $v(x)$, then $\mathfrak{a} = (x)$, showing R is a PID and hence Noetherian. If S is a subring of K with $R \subset S \subset K$, then either $v(S) \subset \mathbb{Z}_{\geq 0}$ (in which case $S \subset R$) or $v(S) = \mathbb{Z}$, in which case, given any $x \in K^\times$, there is an $s \in S$ such that $xs^{-1} \in R$, which implies $x \in S$; therefore, $S = K$.

(c) $\Rightarrow$ (b) Given 7.1.5(f), we only need to check R is local. If there are maximal ideals $\mathfrak{m}, \mathfrak{n} \subset R$ and an $x \in \mathfrak{m} \smallsetminus \mathfrak{n}$, then $R \subsetneq R[x^{-1}] \subsetneq K = \operatorname{Frac} R$. Indeed, the first strict containment follows from $x \in \mathfrak{m}$, and the second from the fact that if $0 \neq y \in \mathfrak{n}$, then $y^{-1} \notin R[x^{-1}]$.

(c) $\Rightarrow$ (d) A Noetherian valuation ring is a PID by 7.1.5(e).

(d) $\Rightarrow$ (e) A PID is a UFD (1.4.4). If π is a generator of the maximal ideal, then π is an irreducible. Every nonunit is in (π), so π is the unique irreducible up to associates.

(e) $\Rightarrow$ (a) Let π be an irreducible element. For each nonzero $x \in R$, there is a unique integer $n = n(x) \geq 0$ and unit $u \in R^\times$ such that $x = u\pi^n$. The map $x \mapsto n(x)$ extends to a discrete valuation on $\operatorname{Frac} R$ with valuation ring R.

Next, we show the equivalence of (f1)-(f8). Clearly, (f1) $\Rightarrow$ (f2) $\Rightarrow$ (f3) $\Rightarrow$ (f4) $\Rightarrow$ (f5), and (f6) $\Rightarrow$ (f5), and (f8) $\Rightarrow$ (f1), (f7). We will finish by showing (f5) $\Rightarrow$ (f8) $\Rightarrow$ (f6) and (f7) $\Rightarrow$ (f5).

(f5) $\Rightarrow$ (f8) It follows from 1.7.3 and 1.3.6 that R is Noetherian. Therefore, if some ideal is not a power of $\mathfrak{m}$, there is a maximal such $\mathfrak{a}$. Then $0 \subsetneq \mathfrak{a} \subsetneq \mathfrak{m}$, so $\mathfrak{a} \subset \mathfrak{a} \cdot \mathfrak{m}^{-1} \subset R$. Note that $\mathfrak{a} \neq \mathfrak{a} \cdot \mathfrak{m}^{-1}$ thanks to the invertibility of $\mathfrak{m}$ and Nakayama (1.5.3). By the maximality of $\mathfrak{a}$, the ideal $\mathfrak{a} \cdot \mathfrak{m}^{-1}$ is a power of $\mathfrak{m}$, and then again by invertibility of $\mathfrak{m}$, so is $\mathfrak{a}$.

(f8) $\Rightarrow$ (f6) If $\mathfrak{p}$ is a nonzero prime, there is an $n \geq 1$ such that $\mathfrak{p} = \mathfrak{m}^n$, and then $\mathfrak{m} \subset \sqrt{\mathfrak{m}^n} \subset \sqrt{\mathfrak{p}} = \mathfrak{p}$. If $0 \neq x \in \mathfrak{m}$, then there is an $m \geq 1$ so that $(x) = \mathfrak{m}^m$, and then $\mathfrak{m}$ has inverse $x^{-1}\mathfrak{m}^{m-1}$.

(f7) $\Rightarrow$ (f5) We will show that the only invertible prime is $\mathfrak{m}$. This suffices: indeed, then every nonzero principal ideal is a power of $\mathfrak{m}$, and so every nonzero prime contains a power of $\mathfrak{m}$, and we finish as above. Let $\mathfrak{p}$ be an invertible prime, and pick an $x \in R \smallsetminus \mathfrak{p}$; it suffices to show that $\mathfrak{p} = \mathfrak{p}^2 + x\mathfrak{p}$. Write $\mathfrak{p} + (x) = \prod_i \mathfrak{p}_i$ and $\mathfrak{p} + (x^2) = \prod_j \mathfrak{q}_j$ as finite products of primes. In $R/\mathfrak{p}$, we have $(\overline{x}) = \prod_i \overline{\mathfrak{p}}_i$ and $(\overline{x}^2) = \prod_j \overline{\mathfrak{q}}_j$, so each $\overline{\mathfrak{p}}_i$ and $\overline{\mathfrak{q}}_j$ is invertible and so by 1.7.5, we have $(\mathfrak{p} + (x))^2 = \mathfrak{p} + (x^2)$. Then $\mathfrak{p} \subset \mathfrak{p} + (x^2) \subset (\mathfrak{p} + (x))^2 \subset \mathfrak{p}^2 + (x)$, which with $x \notin \mathfrak{p}$ forces $\mathfrak{p} \subset \mathfrak{p}^2 + x\mathfrak{p} \subset \mathfrak{p}$ as needed.

At this point, note that (d) $\Rightarrow$ (f5), (f9) is clear, and (f8) $\Rightarrow$ (d) follows from the fact that if $\mathfrak{m}$ is invertible, then it is principal (1.7.3). Conversely, we have

(f9) $\Rightarrow$ (d) Let $\mathfrak{a} \subset R$ be a nonzero ideal, and pick an $b \in \mathfrak{m} \cdot \mathfrak{a} \smallsetminus \{0\}$. Then there is a $a \in \mathfrak{a}$ such that $\mathfrak{a} = (a, b)$, and then $\mathfrak{a} = (a, b) \subset (a) + \mathfrak{m} \cdot \mathfrak{a} \subset \mathfrak{a}$, so Nakayama (1.5.3(c)) tells us that $\mathfrak{a} = (a)$ as needed.

Thus, we have shown the equivalence of (a)-(f). Next, (g1) and (g2) are equivalent by 2.5.5, and (d) $\Rightarrow$ (g1+2) $\Rightarrow$ (f6) is clear. Next, (d+f8) $\Rightarrow$ (g3) is clear, while (g3) $\Rightarrow$ (f8) follows from 2.2.7. Also, (d) $\Rightarrow$ (g4) $\Rightarrow$ (g5) is clear, as is (g6) $\Rightarrow$ (g7). The implication (g5) $\Rightarrow$ (g6) follows from 2.1.5(a) (along with 2.1.2(b)), since (g5) implies that $\operatorname{Spec} R/(x) = \{\overline{\mathfrak{m}}\}$. To finish the proof of the equivalence of (a)-(g), it then only remains to show

(g7) $\Rightarrow$ (g1) Pick a $y \in R$ such that $\mathfrak{m} = (x : y)$; then $y \notin (x)$. Let $\pi := x/y$; then $\pi^{-1} \in \operatorname{Frac} R \smallsetminus R$ and $\pi^{-1}\mathfrak{m} \subset R$. If $\pi^{-1}\mathfrak{m} \subset \mathfrak{m}$, then 1.5.2 tells us that $\pi^{-1} \in \operatorname{Cl}_K(R) = R$, which cannot be; therefore, $\pi^{-1}\mathfrak{m} = R$ and so $\mathfrak{m} = (\pi)$.

The statement (h) is clear at this point, as are the implications (i1) $\Rightarrow$ (i2) $\Rightarrow$ (i3) $\Leftrightarrow$ (i4), and that (i) $\Rightarrow$ (j); also, the last statement of (i) follows immediately from (c). It only remains to show

(i4) $\Rightarrow$ (i1) Let v be any discrete valuation on R, and pick a uniformizer ϖ for v. By (i2) $\Rightarrow$ (i4), we get that $(\varpi) = \mathfrak{m} = (\pi)$, so ϖ and π are associates, and hence have the same valuation, namely one.[2]

■

Example 7.1.8. Suppose that R is a Noetherian domain and $\mathfrak{p} \subset R$ a prime. Suppose that one of the following conditions hold.

(a) R is normal and $\operatorname{ht} \mathfrak{p} = 1$.
(b) The prime $\mathfrak{p}$ is invertible.

Then $R_\mathfrak{p}$ is a DVR. Indeed, in the first case, $R_\mathfrak{p}$ is normal (3.1.11(b)), so we are done by 7.1.7(g4). In the second case, $\mathfrak{p}$ is nonzero and by 1.7.3(d), the prime $\mathfrak{p}R_\mathfrak{p}$ is principal, so we are done by 7.1.7(g2).

We finish with two results that are extremely useful in algebraic geometry: the existence of valuation rings dominating local subrings of fields (for valuative criteria), and an algebraic analog of Hartogs's Lemma in complex geometry (for lots of reasons, such as extending sections of line bundles, or proving that the complement of nonempty open affine in a separated integral Noetherian normal scheme has pure codimension one, which in turn can be used to show that abelian varieties are projective, etc.).

Theorem 7.1.9. *Let R be a local domain, and suppose we have an inclusion $R \subset L$ for a field L.*

(a) *There is a valuation ring of L dominating R.*
(b) *If R is Noetherian and not a field, and L is finitely generated over $K := \operatorname{Frac} R$, there is a* discrete *valuation ring of L dominating R.*

Proof. Let $\mathfrak{m}$ be the maximal ideal of R and $k := R/\mathfrak{m}$ its residue field.

(a) Fix an algebraic closure $k \to \Omega$. By Zorn's Lemma, there is a maximal extension of $R \to \Omega$ to a subring of L, which is a valuation ring dominating R by 7.1.5(g).
(b) Factor L/K as the composite of a purely transcendental $K \to K(t) := K(t_1, \ldots, t_n)$ followed by an algebraic extension $K(t) \to L$, where $n = \operatorname{trdeg}_K L$; then replacing R by $R[t]_{(\mathfrak{m},t)}$ reduces us to the case of algebraic L/K. By (a), we may find a valuation ring S of L dominating R. For any set of (nonzero) generators $x_1, \ldots, x_n$ of $\mathfrak{m}$ for some $n \in \mathbb{Z}_{\geq 1}$, we may reorder so that x_1 has the least valuation (according to S) of the x_i. It follows that in the ring $S' := R[x_2/x_1, \ldots, x_n/x_1] \subset S$, the element x_1 is *not* a unit. Pick a prime $\mathfrak{p}$ of S' minimal over x_1; then by 2.4.4, $S'_\mathfrak{p}$ is a Noetherian local domain of dimension one

[2] See 7.1.3 if needed.

dominating R. Let S'' be the integral closure of $S'_{\mathfrak{p}}$ in L. By 3.4.1, S'' is a Noetherian normal domain of dimension one. Let $\mathfrak{m}$ be any prime ideal of S'' lying over $\mathfrak{p}S'_{\mathfrak{p}}$. Then $\operatorname{ht} m = 1$, and the localization $S''_{\mathfrak{m}}$ is the required DVR (7.1.8(a)).

■

Theorem 7.1.10 (Algebraic Hartogs's Lemma)**.** Let R be a Noetherian R_1 domain. Then R is normal iff $R = \bigcap_{\operatorname{ht}\mathfrak{p}=1} R_{\mathfrak{p}}$. In particular, if R is a Noetherian normal domain, then $R = \bigcap_{\operatorname{ht}\mathfrak{p}=1} R_{\mathfrak{p}}$.

Proof. A Noetherian normal domain is R_1 (7.1.8(a)), so the second statement follows immediately from the first. If R is Noetherian and R_1, then for every height one $\mathfrak{p} \subset R$, the localization $R_{\mathfrak{p}}$ is a DVR (7.1.7(g5)) and hence normal; so, if $R = \bigcap_{\operatorname{ht}\mathfrak{p}=1} R_{\mathfrak{p}}$, then R is normal.

For the converse, suppose that R is a Noetherian normal domain. We first note that for any $x \in R$, the R-module $R/(x)$ has no embedded primes, i.e., every associated prime to (x) has height one (we are using 2.4.4 of course). Indeed, if $\mathfrak{p} \in \operatorname{Ass}(R/(x))$, then by 2.1.3(c) we have $\mathfrak{p}R_{\mathfrak{p}} \in \operatorname{Ass}_{R_{\mathfrak{p}}}(R_{\mathfrak{p}}/(x))$. Then 3.1.11(b) and 7.1.7(g7) tell us that $\operatorname{ht}\mathfrak{p} = \dim R_{\mathfrak{p}} = 1$ as needed.

For the main proof, it suffices to show that if $x, y \in R$ with $0 \neq x$, and if $y \in xR_{\mathfrak{p}}$ for all $\mathfrak{p} \subset R$ with $\operatorname{ht}\mathfrak{p} = 1$, then in fact $y \in xR = (x)$. This is clear if $(x) = 1$. Else, consider a minimal primary decomposition (2.2.7) of (x) of the form $(x) = \bigcap_i \mathfrak{q}_i$ and let $\mathfrak{p}_i := \sqrt{\mathfrak{q}_i}$ for each i. By 2.2.9, $\operatorname{Ass}(R/(x)) = \{\mathfrak{p}_i\}$. By the above observation, for all i, we have $\operatorname{ht}\mathfrak{p}_i = 1$; in particular, these primes are all mutually incomparable for the inclusion partial order, and so it follows from 2.2.12 that for each i we have $xR_{\mathfrak{p}_i} = \mathfrak{q}_i R_{\mathfrak{p}_i}$ and $R \cap xR_{\mathfrak{p}_i} = \mathfrak{q}_i \ni y$. Therefore, $y \in \bigcap_i \mathfrak{q}_i = (x)$ as needed. ■

[TODO: Relate to R1S2.]

7.2 Dedekind Domains and their Extensions

Global versions of discrete valuation rings are called Dedekind domains. Some important examples of these are the rings of integers of number fields, and coordinate rings of smooth curves. In fact, the analogy between these two kinds of objects (and the behavior of their morphisms) was important impetus for the development of modern algebraic geometry.

Theorem/Definition 7.2.1 (Dedekind Domains)**.** Let R be a domain that is not a field. The following conditions on R are equivalent.

(a) *R is Noetherian and if $\mathfrak{p} \subset R$ is any nonzero prime, then $R_{\mathfrak{p}}$ is a DVR.*
(b) *R is Noetherian and if $\mathfrak{m} \subset R$ is any maximal ideal, then $R_{\mathfrak{m}}$ is a DVR.*
(c) Containment is division for integral ideals.
(d) Containment is division for fractional ideals.
(e) Every nonzero fractional ideal of R is invertible.
(f) Every nonzero (integral) ideal is invertible.
(g) Every nonzero prime ideal of R is invertible.
(h) Every nonzero ideal of R is a finite product of prime ideals.
(i) R is Noetherian, $\dim R = 1$, and R is normal.
(j) R is Noetherian, $\dim R = 1$, and every primary ideal of R is a prime power.
(k) If $\mathfrak{a} \subset R$ is any nonzero ideal, the quotient $R/\mathfrak{a}$ is a principal ideal ring.
(l) If $\mathfrak{a} \subset R$ is an ideal and $a \in \mathfrak{a}$ a nonzero element, then there is a $b \in \mathfrak{a}$ such that $\mathfrak{a} = (a, b)$.
(m) If $\mathfrak{a} \subset R$ is any ideal, there is a nonzero ideal $\mathfrak{b} \subset R$ such that $\mathfrak{a} + \mathfrak{b} = (1)$ and $\mathfrak{a} \cdot \mathfrak{b}$ is principal.
(n) If $\mathfrak{a} \subset R$ is any ideal, there is a nonzero ideal $\mathfrak{b} \subset R$ such that $\mathfrak{a} \cdot \mathfrak{b}$ is principal.

A domain R said to be a *Dedekind domain* if it is not a field and satisfies these equivalent conditions. In this case:

(o) The factorization of a nonzero ideal into primes is unique.
(p) The group $\mathrm{Ideal}(R)$ is the free abelian group on the set of nonzero prime ideals of R.
(q) If $\mathfrak{a}, \mathfrak{b} \subset R$ are nonzero ideals with prime factorization $\mathfrak{a} = \prod \mathfrak{p}^{e_{\mathfrak{p}}}$ and $\mathfrak{b} = \prod \mathfrak{p}^{f_{\mathfrak{p}}}$, then we have $\mathfrak{a} + \mathfrak{b} = \gcd(\mathfrak{a}, \mathfrak{b}) := \prod \mathfrak{p}^{\min\{e_{\mathfrak{p}}, f_{\mathfrak{p}}\}}$ and $\mathfrak{a} \cap \mathfrak{b} = \mathrm{lcm}(\mathfrak{a}, \mathfrak{b}) = \prod \mathfrak{p}^{\max\{e_{\mathfrak{p}}, f_{\mathfrak{p}}\}}$.
(r) (Weak Approximation) If $e_{\mathfrak{p}} \in \mathbb{N}$ are all but finitely many zero, then $R/\prod \mathfrak{p}^{e_{\mathfrak{p}}} \xrightarrow{\sim} \prod R/\mathfrak{p}^{e_{\mathfrak{p}}}$.
(s) Each nonzero prime $\mathfrak{p}$ of R gives a discrete valuation $v_{\mathfrak{p}}$ on R with corresponding DVR $R_{\mathfrak{p}}$, which is extended by a $\mathfrak{p}$-adic valuation on ideals. For a nonzero $x \in R$, the number $v_{\mathfrak{p}}(x)$ is the smallest $e \geq 0$ such that $x \in \mathfrak{p}^e$. For any $n \in \mathbb{Z}_{\geq 1}$, primes $\mathfrak{p}_1, \dots, \mathfrak{p}_n \subset R$ and $e_1, \dots, e_n \in \mathbb{N}$, there is an $x \in R$ with $v_{\mathfrak{p}_i}(x) = e_i$ for $i = 1, \dots, n$.
(t) Consider the following conditions on R.
 (t1) R is semilocal.
 (t2) R is a PID.
 (t3) R is a UFD.
 (t4) The class number $h(R) = 1$.
 Then (t1) ⇒ (t2) ⇔ (t3) ⇔ (t4).

A local Dedekind domain is the same thing as a DVR.

Proof. Clearly, (a) ⇒ (b) ⇒ (f) ⇒ (c) ⇒ (d) ⇒ (e) ⇒ (f) ⇒ (g), and (k) ⇔ (l), and (m) ⇒ (n) ⇒ (f). Also, (l) ⇒ (a) by 7.1.7(f9).

(g) ⇒ (h) It follows from 1.7.3 and 1.3.6 that R is Noetherian. Therefore, if some ideal is not a product of primes, there is a maximal such $\mathfrak{a}$. This $\mathfrak{a}$ is proper, and hence contained in some maximal ideal $\mathfrak{m}$. Then $\mathfrak{a} \subset \mathfrak{a} \cdot \mathfrak{m}^{-1} \subset R$. Note that $\mathfrak{a} \neq \mathfrak{a} \cdot \mathfrak{m}^{-1}$ thanks to 1.5.11, since $\mathfrak{a} \neq 0$. By the maximality of $\mathfrak{a}$, the ideal $\mathfrak{a} \cdot \mathfrak{m}^{-1}$ is a product of primes, and then again by invertibility of $\mathfrak{m}$, so is $\mathfrak{a}$.

(h) ⇒ (f) Proceeding as in the proof of (f7) ⇒ (f5) of 7.1.7 shows that an invertible prime of R is maximal. We now show that every nonzero prime is invertible: if $\mathfrak{p}$ is a nonzero prime and $0 \neq x \in \mathfrak{p}$, then write $(x) = \prod_i \mathfrak{p}_i$. Each $\mathfrak{p}_i$ is invertible and hence maximal; further, by 1.2.14(a), there is an i such that $\mathfrak{p}_i \subset \mathfrak{p}$ whence $\mathfrak{p}_i = \mathfrak{p}$ as needed.

(g) ⇒ (a) As noted above, R is Noetherian. If $\mathfrak{p} \subset R$ is a nonzero prime, then $R_\mathfrak{p}$ is a Noetherian local domain that is not a field; since $\mathfrak{p}$ is invertible (1.7.3), $\mathfrak{p}R_\mathfrak{p}$ is principal, so we are done by 7.1.7(g1).

For the equivalence with (i) and (j), we reduce to the local case (7.1.7). For (b) ⇒ (i), (j), note first that $\dim R = \sup_\mathfrak{m} \dim R_\mathfrak{m} = 1$. Then (b) ⇒ (i) by 3.1.11(b), and (b) ⇒ (j) by 2.2.2. The converses follow similarly: (i) ⇒ (a) is 7.1.8(a) and (j) ⇒ (a) is 2.2.2 combined with 7.1.7(g5). At this point, we have shown the equivalence of (a-j). Now 1.7.5 says that (g+h) ⇒ (o) ⇒ (p), and (o)+(c) ⇒ (q) ⇒ (r), (s). To complete the proof of the equivalence of (a)-(n), it remains to show that (a-j) ⇒ (k), (m).

(a-j) ⇒ (k) Since (a-j) implies (o-r), by (r) and the fact that principal ideal rings are closed under direct products, it suffices to show that if $\mathfrak{p} \subset R$ is a nonzero prime, then for any $e \in \mathbb{Z}_{\geq 1}$, the ring $R/\mathfrak{p}^e$ is a principal ideal ring, but indeed, since $\mathfrak{p}$ is maximal, $R/\mathfrak{p}^e \xrightarrow{\sim} R_\mathfrak{p}/(\mathfrak{p}R_\mathfrak{p})^e$, which is the quotient of the PID $R_\mathfrak{p}$.

(a-j) ⇒ (m) Clear if $\mathfrak{a} = 0$; else, use (s) to produce an $x \in R$ with $v_\mathfrak{p}(x) = v_\mathfrak{p}(\mathfrak{a})$ for all $\mathfrak{p}$ such that $v_\mathfrak{p}(\mathfrak{a}) \neq 0$; then by (c), there is an ideal $\mathfrak{b}$ such that $\mathfrak{a} \cdot \mathfrak{b} = (x)$, and this $\mathfrak{b}$ must satisfy $\mathfrak{a} + \mathfrak{b} = 1$ by (q).

The implication (t1) ⇒ (t2) follows immediately from (s), (t2) ⇒ (t3) is 1.4.4, and (t3) ⇒ (t4) is 1.7.7, and (t4) ⇒ (t2) is clear (check!). ■

Next, let us study extensions of domains. For this, we need the following important finiteness result.

Theorem 7.2.2. Let R be a domain with fraction field K. Let L/K be a finite extension. If either

(a) *R is Noetherian and normal and L/K is separable, or*
(b) *R is a finitely generated algebra over a field,*

then the integral closure $S := \mathrm{Cl}_L(R)$ of R in L is a finitely generated R-module.

Proof 1 of (a). For (a), by the algebraicity of L/K, every K-basis of L can be rescaled by elements of R to lie in S; let $v_1, \ldots, v_n \in S$ be one such basis. Since L/K is separable, the trace pairing $(x, y) \mapsto \mathrm{Tr}_K^L(xy)$ is nondegenerate (by 5.4.1(g)[TODO]). Using this pairing we find the dual basis $v_1^*, \ldots, v_n^* \in L$ with $\mathrm{Tr}_K^L(v_i^* v_j) = \delta_{ij}$. Write an $x \in S$ as $x = \sum_i x_i v_i^*$, then for each i, the inclusion $xv_i \in S$ implies that $x_i = \mathrm{Tr}_K^L(xv_i) \in R$ by 3.1.9(b) by taking $\mathfrak{a} = (1)$, combined with 10.4.5(b). Therefore, $S \subset \sum_j Rv_j^*$; we finish by the Noetherian hypothesis. ■

Proof 2 of (a). Replacing L by its Galois closure (and using that R is Noetherian), we may assume that L/K is finite Galois with Galois group $G := \mathrm{Gal}(L/K)$. As in the first proof, let $v_1, \ldots, v_n \in S$ be an a basis of L/K; and let D be the discriminant with respect to this basis (10.4.6), where $0 \neq D$ by separability as before. Again by 3.1.9 and 10.4.5(b), we have $D \in R$. If $x \in S$ is $x = \sum_j x_j v_j$ for some $x_j \in K$, then we'll show that $Dx_j \in R$ for each j. Indeed, by applying $\sigma_i \in G$ we get $\sigma_i x = \sum_j x_j \sigma_i v_j$. By Cramer's rule, we can write $x_j = y_j/\delta$ for some $y_j \in S$, where $\delta := \det(\sigma_i v_j)_{i,j}$ and $D = \delta^2$ (by 10.4.5(a) and 10.4.6); clearly also $\delta \in S$. Then $Dx_j = y_j\delta \in \mathrm{Cl}_K(R) = R$. In fact, this shows that we have $Dx_j^2 \in R$. ■

Proof of (b). By Noether normalization (6.1.1), R is integral over some polynomial $k[z_1, \dots, z_r]$, so by transitivity of integrality and algebraicity of K over $k(z_1, \dots, z_r)$ we may assume that $R = k[z_1, \dots, z_r]$ is polynomial and so $K = k(z_1, \dots, z_r)$. Since R is Noetherian, we can replace L by its normal closure over K (say the splitting field in some algebraic closure of L of the minimal polynomials over K of some generating set of L as a field extension of K) to assume that L/K is normal. Let $I := L^{\mathrm{Aut}(L/K)}$, so that L/I is Galois and I/K is purely inseparable (see [15, Theorem 4.23] if needed). If we show that $T := \mathrm{Cl}_I(R)$ is a finitely generated R-module, then we would have shown it is Noetherian and normal, and so by (a), $S = \mathrm{Cl}_L(T)$ would be a finitely generated T-module, and we would be done by transitivity of module-finiteness. Therefore, by replacing L by I, we can suppose that L/K is purely inseparable. If $L = K$ (e.g., if $\operatorname{char} K = 0$), this is trivial; else assume that $p := \operatorname{char} k > 0$. Then for some power q of p, the field L is generated by q^{th} roots of finitely many rational functions. Extending L further, we may assume that $L = k'(z_1^{1/q}, \dots, z_r^{1/q})$ for some extension k'/k (namely the one obtained from k by adjoining the q^{th} roots of the coefficients of those rational functions). Then $S = \mathrm{Cl}_L(R) = k'[z_1^{1/q}, \dots, z_r^{1/q}]$ since this is ring is integral over R and is normal in its quotient field L; visibly, S is module-finite over R. ■

Theorem 7.2.3 (Ramification Formula)**.** Let R be a Dedekind domain with fraction field K. Let L/K be a finite extension and $S := \mathrm{Cl}_L(R)$. Suppose that S is a finitely generated R-module (e.g., as in the hypotheses of 7.2.2).

(a) The ring S is also a Dedekind domain.

(b) If $n := [L : K]$ and $\mathfrak{p} \subset R$ is a prime and $\mathfrak{p}S = \prod_i \mathfrak{P}_i^{e_i}$, and $f_i := [\kappa(\mathfrak{P}_i) : \kappa(\mathfrak{p})]$, then $\sum_i e_i f_i = n$.

(c) If further L/K is normal, then all the e_i and f_i are equal, so if there are g distinct primes. In particular, if there are g such primes, then the formula in (b) reduces to $efg = n$.

Proof.

(a) The ring S is Noetherian since it is a finitely generated R-module with R Noetherian, it is normal because of 3.1.4(d), and $\dim S = \dim R = 1$ by 3.2.6(a), so S is Dedekind by 7.2.1(i).

(b) By Weak Approximation (7.2.1(r)), $S/\mathfrak{p}S \xrightarrow{\sim} \prod_i S/\mathfrak{P}_i^{e_i}$. On the one hand, since each $\mathfrak{P}_i S_{\mathfrak{P}_i}$ is principal, say (q_i), we have a $\kappa(\mathfrak{P}_i)$-linear isomorphism $q_i^j : S/\mathfrak{P}_i \xrightarrow{\sim} \mathfrak{P}_i^j/\mathfrak{P}_i^{j+1}$ for each $j \geq 0$; this shows that $\sum_{i=1}^n e_i f_i = \dim_{\kappa(\mathfrak{p})}(S/\mathfrak{p}S)$. On the other hand, let $x_1, \dots, x_r \in S$ reduce to a $\kappa(\mathfrak{p})$-basis of $S/\mathfrak{p}S$, so $r := \dim_{\kappa(\mathfrak{p})} S/\mathfrak{p}S$. Then the x_i also reduce to spanning set of $S_{\mathfrak{p}}/\mathfrak{p}S_{\mathfrak{p}}$ over $\kappa(\mathfrak{p})$, and so by 1.5.3 generate $S_{\mathfrak{p}}$ over $R_{\mathfrak{p}}$ and hence certainly span L over K. If they are linearly dependent, say $\sum_j a_j x_j = 0$ with $a_j \in K$ not all zero, then multiplying by a suitable power of the generator of $\mathfrak{p}R_{\mathfrak{p}}$ we can assume that the a_i are all in $R_{\mathfrak{p}}$ but not all in $\mathfrak{p}R_{\mathfrak{p}}$. Reducing mod $\mathfrak{p}R_{\mathfrak{p}}$, we get a nontrivial dependence relation over $\kappa(\mathfrak{p})$, which is not possible. This shows that $x_1, \dots, x_r$ form a basis of L/K and hence $n = r$ as needed.

(c) This follows immediately from (b) and the following lemma (7.2.4).

■

Lemma 7.2.4. Let R be a normal domain with fraction field K, and L/K a finite normal[3] field extension, and $S := \mathrm{Cl}_L(R)$. The automorphism group $\mathrm{Aut}(L/K)$ acts transitively on the fibers of $\operatorname{Spec} S \to \operatorname{Spec} R$.

Proof. Let $G := \mathrm{Aut}(L/K)$. Let $\mathfrak{P}, \mathfrak{Q}$ be two primes of S lying above the same $\mathfrak{p}$ of R. Suppose

[3] Apologies for the overloaded term "normal"; unfortunately, this is established nomenclature. I hope there is no confusion.

that $\mathfrak{P} \notin G\mathfrak{Q}$. Then by 3.2.1(b) and 1.2.14(b), we can produce a $x \in \mathfrak{P} \smallsetminus \bigcup G\mathfrak{Q}$. Then $Gx \cap \mathfrak{Q} = \emptyset$, and so by 10.4.5, $\mathrm{N}_K^L(x) \notin R \cap \mathfrak{Q} = \mathfrak{p}$, contradicting that $x \in \mathfrak{P} \Rightarrow \mathrm{N}_K^L(x) \in R \cap \mathfrak{P} = \mathfrak{p}$. ■

In fact, more generally we have

Theorem 7.2.5. Let R be a Noetherian one-dimensional domain with fraction field K. Let L/K be a finite extension and let $S := \mathrm{Cl}_L(R)$. Then S is a Dedekind domain.

Proof. Simply replace the use of 7.2.2 in the proof of 7.2.3(a) with that of 3.4.1. ■

However, at this level of generality, S need not be a finitely generated R-module, and we only have the inequality $[L : K] > \sum_{\mathfrak{P}|\mathfrak{p}} e_{\mathfrak{P}} f_{\mathfrak{P}}$. See [TOCITE] for more discussion about this situation.

7.3 Modules over Dedekind Domains

Steinitz Theory.

7.4 Exercises

Exercise 7.1. Let R be a Dedekind domain. If we have an inclusion of ideals $0 \subsetneq \mathfrak{a} \subset \mathfrak{b} \subsetneq R$, there is a $\gamma \in \operatorname{Frac} R$ such that $\gamma\mathfrak{a} \subset R$ but $\gamma\mathfrak{a} \not\subset \mathfrak{b}$.

Exercise 7.2. Show that a Dedekind domain is a Jacobson ring iff it has infinitely many prime ideals.

Chapter 8

A Little Homological Algebra and Some Applications

8.1 Projective, Injective, and Flat Modules

For this chapter only, we do not require that rings be commutative, and work carefully with left- and right- modules over possibly noncommutative rings, although (a) the whole setup can more-or-less be carried out in any suitable abelian category, and (b) the reader will not lose much by focusing on the commutative case on the first pass. For a (possibly noncommutative) ring R, we let R-Mod denote the category of left R-modules (i.e. $(R,\mathbb{Z})$-bimodules), and let Mod-R denote the category of right R-modules (i.e. $(\mathbb{Z},R)$-bimodules). Let $\mathsf{Ab} = \mathbb{Z}$-Mod be the category of abelian groups.

Remark 8.1.1. For any ring R, there is an *isomorphism* of categories R-$\mathsf{Mod} \cong \mathsf{Mod}$-$R^{\mathrm{op}}$, where R^{op} is the *opposite* ring to R. Therefore, any statement about left modules for R has a corresponding version for right modules for R^{op}, and vice-versa. In particular, when R is a commutative ring, there is a natural isomorphism R-$\mathsf{Mod} \cong \mathsf{Mod}$-$R$, which we will use implicitly in what follows.

The first key observation here is

Lemma 8.1.2 (The Definitive Tensor-Hom Adjunction)**.** Let A, B, C be rings. Let X be an (A,B)-bimodule, Y be a (B,C)-bimodule, and Z be an (A,C)-bimodule. There are isomorphisms of abelian groups

$$\mathrm{Hom}_{(A,B)}(X, \mathrm{Hom}_{(\mathbb{Z},C)}(Y,Z)) \cong \mathrm{Hom}_{(A,C)}(X \otimes_B Y, Z) \cong \mathrm{Hom}_{(B,C)}(Y, \mathrm{Hom}_{(A,\mathbb{Z})}(X,Z)).$$

These isomorphisms are natural in $A, B, C, X, Y,$ and Z. Further, when we have more structure, then the isomorphisms above respect that structure. For instance, when $A = B = C$ is a commutative ring, then the three modules above have a natural module structure over this ring, and the above are isomorphisms of modules.

Proof. Let $\varphi : X \to \mathrm{Hom}_{(\mathbb{Z},C)}(Y,Z)$ be an (A,B)-bimodule homomorphism. Consider the map $X \times Y \to Z$ given by $(x,y) \mapsto \varphi(x)(y)$. This is B-balanced, and so descends to a map $\tilde{\varphi} : X \otimes_B Y \to Z$ which is easily seen to be an (A,C)-bimodule homomorphism. The resulting map $\mathrm{Hom}_{(A,B)}(X, \mathrm{Hom}_{(\mathbb{Z},C)}(Y,Z)) \to \mathrm{Hom}_{(A,C)}(X \otimes_B Y, Z)$ given by $\varphi \mapsto \tilde{\varphi}$ is the required isomorphism. The second part is similar, and the naturality statement as well as the last one is clear from the proof; the details are left to the reader. ■

A ring homomorphism $f : R \to S$ makes S an (R,R)-bimodule and gives rise to three functors:

(a) the extension-of-scalars functor $f^* : R\text{-}\mathsf{Mod} \to S\text{-}\mathsf{Mod}$ given by $M \mapsto S \otimes_R M$,

(b) the restriction-of-scalars functor $f_* : S\text{-}\mathsf{Mod} \to R\text{-}\mathsf{Mod}$,

(c) the dualizing-of-scalars functor $f^! : R\text{-}\mathsf{Mod} \to S\text{-}\mathsf{Mod}$ given by $M \mapsto \mathrm{Hom}_R(S,M) := \mathrm{Hom}_{(R,\mathbb{Z})}(S,M)$, with S-module structure given by $(s \cdot \varphi)(t) := \varphi(ts)$ for $s,t \in S$ and $\varphi \in f^!M$.

Corollary 8.1.3. If $f : R \to S$ is a ring homomorphism, then $f^* \dashv f_* \dashv f^!$. In particular, f^* is right-exact, f_* is exact, and $f^!$ is left-exact.

Proof. If M is a left R-module and N a left S-module, then there are natural abelian group isomorphisms

$$\mathrm{Hom}_S(f^*M, N) = \mathrm{Hom}_S(S \otimes_R M, N) \cong \mathrm{Hom}_R(M, \mathrm{Hom}_S(S,N)) \cong \mathrm{Hom}_R(M, f_*N),$$

where in the second step we have applied the second of the two isomorphisms in 8.1.2 applied to $(A,B,C,X,Y,Z) = (S,R,\mathbb{Z},S,M,N)$ and in the third step we have used that $\mathrm{Hom}_S(S,N) \cong N$

as S-modules, whence $\mathrm{Hom}_S(S,N) \cong f_*N$ as R-modules. Similarly, there are natural abelian group isomorphisms

$$\mathrm{Hom}_R(f_*N, M) \cong \mathrm{Hom}_R(S \otimes_S N, M) \cong \mathrm{Hom}_S(N, \mathrm{Hom}_R(S,M)) = \mathrm{Hom}_S(N, f^!M),$$

where in the first step we have used $N \cong S \otimes_S N$ as S-modules, and in the second step the second isomorphism from 8.1.2 applied to $(A,B,C,X,Y,Z) = (R,S,\mathbb{Z},S,N,M)$. ■

Remark 8.1.4. Similarly, we have functors on the "other side": $f^* : \mathsf{Mod}\text{-}R \to \mathsf{Mod}\text{-}S$ given by $M \mapsto M \otimes_R S$, the functor $f_* : \mathsf{Mod}\text{-}S \to \mathsf{Mod}\text{-}R$ as before, and $f^! : \mathsf{Mod}\text{-}R \to \mathsf{Mod}\text{-}S$ given by $M \mapsto \mathrm{Hom}_{(\mathbb{Z},R)}(S,M)$ with right S-module structure given by $(\varphi \cdot s)(t) := \varphi(st)$ for $s,t \in S$ and $\varphi \in f^!M$. Then 8.1.1 combined with 8.1.3 similarly gives the adjunctions $f^* \dashv f_* \dashv f^!$.

Corollary 8.1.5. Let R be a ring, and T be a left R-module.

(a) The functor $\mathrm{Hom}_R(T,-) : R\text{-}\mathsf{Mod} \to \mathsf{Ab}$ is right adjoint, and hence left-exact.
(b) The functor $\mathrm{Hom}_R(-,T) : R\text{-}\mathsf{Mod}^{\mathrm{op}} \to \mathsf{Ab}$ is right adjoint, and hence left-exact.
(c) The functor $- \otimes_R T : \mathsf{Mod}\text{-}R \to \mathsf{Ab}$ is left adjoint, and hence right-exact.

Similarly, if T is a right R-module, then:

(d) The functor $T \otimes_R - : R\text{-}\mathsf{Mod} \to \mathsf{Ab}$ is left-adjoint, and hence right-exact.

Finally, if R is a commutative ring, then all of these can be upgraded to functors mapping to $R\text{-}\mathsf{Mod}$ with the same properties.

Proof.

(a) Let M be a (left) $\mathbb{Z}$-module and N a left R-module; then 8.1.2 applied to $(A,B,C,X,Y,Z) = (R,\mathbb{Z},\mathbb{Z},T,M,N)$ gives us the required natural isomorphism

$$\mathrm{Hom}_R(T \otimes_{\mathbb{Z}} M, N) \cong \mathrm{Hom}_{\mathbb{Z}}(M, \mathrm{Hom}_R(T,N)).$$

(b) Let M,N be as in (a); then 8.1.2 applied to $(A,B,C,X,Y,Z) = (R,\mathbb{Z}.\mathbb{Z},N,M,T)$ gives us the required natural isomorphisms

$$\mathrm{Hom}_{\mathbb{Z}}(M, \mathrm{Hom}_R(N,T)) \cong \mathrm{Hom}_R(N, \mathrm{Hom}_{\mathbb{Z}}(M,T)) \cong \mathrm{Hom}_{R\text{-}\mathsf{Mod}^{\mathrm{op}}}(\mathrm{Hom}_{\mathbb{Z}}(M,T), N).$$

(c) Let M be a right R-module and N a left $\mathbb{Z}$-module; then 8.1.2 applied to $(A,B,C,X,Y,Z) = (\mathbb{Z},R,\mathbb{Z},M,T,N)$ gives us the required natural isomorphisms

$$\mathrm{Hom}_{\mathbb{Z}}(M \otimes_R T, N) \cong \mathrm{Hom}_{(\mathbb{Z},R)}(M, \mathrm{Hom}_{\mathbb{Z}}(T,N)).$$

(d) Similar and left to the reader.

The last statement follows from that of 8.1.2. ■

This leads us directly to

Proposition/Definition 8.1.6 (Projective Modules)**.** Let R be a ring, and P be a left R-module. The following conditions are equivalent:

(a) The functor $\mathrm{Hom}_R(P,-) : R\text{-}\mathsf{Mod} \to \mathsf{Ab}$ is exact.
(b) If $M \to N \to 0$ is exact in $R\text{-}\mathsf{Mod}$, then so is $\mathrm{Hom}_R(P,M) \to \mathrm{Hom}_R(P,N) \to 0$ in Ab.
(c) If $M \to N \to 0$ is exact in $R\text{-}\mathsf{Mod}$ and $P \xrightarrow{f} N$ a morphism, then there exists a lift $\tilde{f} : P \to M$ of f, i.e., there is a dashed arrow making the following diagram commutative:

$$\begin{tikzcd}
& P \arrow[dl, dashed, "\tilde{f}"'] \arrow[d, "f"] & \\
M \arrow[r] & N \arrow[r] & 0.
\end{tikzcd}$$

(d) Every short exact sequence $0 \to L \to M \to P \to 0$ in R-Mod splits.[1]
(e) P is a (left) direct summand of a free (left) module.

The module P is said to be *projective* if it satisfies these equivalent conditions.

Proof. In light of 8.1.5(a) and the fact that every module is the quotient of a free module, the implications (a) $\Leftrightarrow$ (b) $\Leftrightarrow$ (c) $\Rightarrow$ (d) $\Rightarrow$ (e) are clear. Therefore, it suffices to show that (e) $\Rightarrow$ (c), which follows from observations that a free module is projective, and given a family P_i of modules, the direct sum $\bigoplus_i P_i$ is projective iff each P_i is. ■

Similarly, we can define projective *right* R-modules. The following consequences of the definition are clear.

Corollary 8.1.7.

(a) If R is a (commutative) PID, then every projective module over R is free.[2]
(b) A finitely generated module is projective iff it is a direct summand of a finitely generated free module.
(c) Every module is a quotient of a projective module, i.e., for any ring R, the category R-Mod (resp. Mod-R) has enough projectives. In particular, every module admits a projective (in fact a free) resolution.
(d) Suppose that R is commutative, and that $\{P_j\}_j$ is a finite family of projective modules. Then the tensor product $\bigotimes_j P_j$ is also projective.

Example 8.1.8. Not all projective modules are free, as a non-principal ideal in a Dedekind domain shows. To say more, suppose R is a Dedekind domain and $\mathfrak{a} \subset R$ a non-principal ideal. Then $\mathfrak{a}$ is projective because it is invertible (7.2.1 and 1.7.3). If it were free, then tensoring with the fraction field of R would show that $\mathfrak{a}$ is free of rank 1, which would mean that it is in fact principal, contrary to hypothesis. For a concrete example, take $R := \mathbb{Z}[\sqrt{-21}]$ and $\mathfrak{a} = (5, 2 + \sqrt{-21})$. Then R is a Dedekind domain thanks to 7.2.3(a) and 3.1, and the ideal $\mathfrak{a}$ is not principal for norm reasons: we have $\#R/\mathfrak{a} = 5$, so if $\mathfrak{a}$ were principal, we would get an integer solution (x, y) to $x^2 + 21y^2 = 5$, which does not exist. However, it can be shown that over a local ring, every projective module is free; see [7, Theorem 2.5]. The relationship between projective and free modules (at least in the case of finitely presented modules) will be explained in 8.3.2.

The dual definition is

Proposition/Definition 8.1.9 (Injective Modules)**.** Let R be a ring and Q a left R-module. The following conditions are equivalent:

(a) The functor $\operatorname{Hom}_R(-, Q) : R\text{-}\mathsf{Mod} \to \mathsf{Ab}$ is exact.
(b) If $0 \to L \to M$ is exact in R-Mod, then so is $\operatorname{Hom}_R(M, Q) \to \operatorname{Hom}_R(L, Q) \to 0$ in Ab.
(c) If $0 \to L \to M$ is exact in R-Mod and $L \xrightarrow{f} Q$ a morphism, then there exists an extension $\tilde{f} : M \to Q$ of f, i.e. there is a dashed arrow making the following diagram commutative:

[1] See 8.1 if needed.

[2] Recall, if needed, that any submodule M of a free module F over a PID is free of rank at most that of F. This is well-known in the finitely generated case, but we do not need the hypothesis of finite generation. Indeed, let R be a PID and F be a free module with free basis $\{e_i\}_{i \in I}$. Let $p_i : F \to R$ denote the projection onto the i^{th} coordinate. Well-order I, and for each i, let $F_i \subset F$ be the free module generated by the e_j with $j \leq i$, so that for each i we have $F_i = \bigcap_{j>i} \ker p_j$ and $\ker p_i = \bigcup_{j<i} F_j$. Now suppose that $M \subset F$ is a submodule, and for each i, let $M_i := M \cap F_i$. Then $p_i(M_i) \subset R$ has the form Ra_i for some $a_i \in R$; pick, for each i, an element $m_i \in M_i$ such that $p_i(m_i) = a_i$, ensuring that $m_i = 0$ if $a_i = 0$. It is then easy to see via transfinite induction on I that the nonzero m_i constitute a free basis for M.

$$\begin{tikzcd}
0 \arrow[r] & L \arrow[r] \arrow[d, "f"] & M \arrow[dl, dashed, "\tilde{f}"] \\
& Q. &
\end{tikzcd}$$

(d) Every short exact sequence $0 \to Q \to M \to N \to 0$ in R-Mod splits.

(e) (Baer) The condition in (c) for the special case where $M = R$, so $L = \mathfrak{a} \subset R$ is a (left) ideal.

Proof. Thanks to 8.1.5(b), the implications (a) $\Leftrightarrow$ (b) $\Leftrightarrow$ (c) $\Rightarrow$ (d), (e) are clear.

(d) $\Rightarrow$ (c) Given a solid diagram as in (c), complete it to a pushout diagram

$$\begin{tikzcd}
0 \arrow[r] & L \arrow[r] \arrow[d, "f"] & M \arrow[d] \\
0 \arrow[r] & Q \arrow[r] & P.
\end{tikzcd}$$

Since the map $L \to M$ is injective, so is the map $Q \to P$ (8.2). Since by assumption the sequence $0 \to Q \to P \to P/Q \to 0$ splits, we have a splitting map $p : P \to Q$; then the composition $M \to P \xrightarrow{p} Q$ gives the extension $\tilde{f}$.[3]

(e) $\Rightarrow$ (c) Given a solid diagram as in (c), consider the partially ordered set

$$\mathcal{C} = \{(L', f') : L \subset L' \subset M, f' : L' \to Q \text{ such that } f'|_L = f\}.$$

By Zorn's Lemma, this has a maximal element, say (L_0, f_0). If $L_0 \subsetneq M$, pick an $m \in M \smallsetminus L_0$. Let $\mathfrak{a} := (L_0 :_R m) = \{r \in R : rm \in L_0\}$, and define a map $\varphi : \mathfrak{a} \to Q$ by $\varphi(r) = f_0(rm)$. By assumption, there is a lift $\tilde{\varphi} : R \to Q$ of φ to R. Define the map $f_1 : L_0 + Rm \to Q$ by $f_1(\ell + rm) = f_0(\ell) + \tilde{\varphi}(r)$; this is well-defined because if $\ell + rm = \ell' + r'm$, then $\ell - \ell' = (r - r')m \in L_0$, whence $r - r' \in \mathfrak{a}$ and so

$$\tilde{\varphi}(r - r') = \varphi(r - r') = f_0((r - r')m) = f_0(\ell - \ell').$$

From this, we see that $(L_0, f_0) < (L_0 + Rm, f_1)$ in $\mathcal{C}$, contradicting the maximality of (L_0, f_0).

■

As above, we can then define injective *right* modules. Let us now give some examples. For this, we need the following comparison lemma.

Lemma 8.1.10. Let $f : R \to S$ be a ring homomorphism.

(a) If P is a projective left (resp. right) R-module, then f^*P is a projective left (resp. right)S-module.

(b) If Q is an injective left (resp. right) R-module, then $f^!Q$ is an injective left (resp. right) S-module.

Proof.

(a) The functor $\mathrm{Hom}_S(f^*P, -) \cong \mathrm{Hom}_R(P, f_*-)$ is a composition of two exact functors. Here, the functor $\mathrm{Hom}_R(P, -)$ is exact because P is projective, and that f_* is exact was observed in 8.1.3.

[3] Alternatively, use 8.1.12(b) below to find an injective M such that $Q \hookrightarrow M$; then since $0 \to Q \to M \to M/Q \to 0$ splits, we see that $M \cong Q \oplus M/Q \cong Q \times M/Q$, so we are done by the observation that given a family Q_i of modules, the direct product $\prod_i Q_i$ is injective iff each Q_i is.

(b) Identical to (a), using $\mathrm{Hom}_S(-, f^!Q) \cong \mathrm{Hom}_R(f_*-, Q)$ instead.

■

In all, it suffices to exhibit injective modules over *one* ring, say $R = \mathbb{Z}$. We do a little better.

Definition 8.1.11. Given a ring R and an R-module Q, we say that Q is *divisible* if for every nonzerodivisor[4] $r \in R$, we have $rQ = Q$, i.e. given any $q \in Q$, there is a $q' \in Q$ such that $q = rq'$.

Proposition 8.1.12 (Enough Injectives)**.** Let R be a ring.

(a) A quotient of a divisible R-module is divisible.

(b) Every injective R-module is divisible, and the converse holds if the R is a (commutative) PID.

(c) Every module is a submodule of an injective module, i.e., the category R-Mod (resp. Mod-R) has enough injectives. In particular, every module admits an injective resolution.

Proof.

(a) Clear.

(b) Let Q be an injective R-module, $q \in Q$ and $r \in R$ a nonzerodivisor. Define the R-module homomorphism $f : (r) \to Q$ by $f(ar) = aq$ for $a \in R$; this is well-defined because if $ar = a'r$, then $(a - a')r = 0$ and hence $a = a'$ because r is a nonzerodivisor. Since Q is injective, there is an extension $\tilde{f} : R \to Q$ of f. Setting $q' := \tilde{f}(1)$, we conclude that

$$q = f(r) = \tilde{f}(r) = r\tilde{f}(1) = rq'$$

as needed. Now suppose that R is a (commutative) PID, and Q a divisible R-module; to show that Q is injective, we use Baer's criterion (8.1.9(e)). Assume that there is a morphism $f : \mathfrak{a} \to Q$. Since R is a PID, $\mathfrak{a} = (r)$ for some $r \in R$. If $r = 0$, then $\tilde{f} = 0$ works; else r is a nonzerodivisor, so by divisibility there is a $q' \in Q$ such that $f(r) = rq'$. Then the map $\tilde{f} : R \to Q$ by $\tilde{f}(s) = sq'$ is an extension of f.

(c) It suffices to do the case of left-modules; that of right modules follows by symmetry (8.1.1). First we show the result for $R = \mathbb{Z}$, so R-$\mathsf{Mod} = \mathsf{Ab}$. Let G be any abelian group. Pick a short exact sequence $0 \to K \to F \to G \to 0$ with F free so that $F/K \cong G$. The composite $F \hookrightarrow \mathbb{Q} \otimes_{\mathbb{Z}} F \twoheadrightarrow (\mathbb{Q} \otimes_{\mathbb{Z}} F)/K$ has kernel K, and hence gives us an embedding $G \cong F/K \hookrightarrow (\mathbb{Q} \otimes_{\mathbb{Z}} F)/K$, where the last group is divisible and hence injective thanks to (a). Now suppose that R is any ring, and let $f : \mathbb{Z} \to R$ be the natural homomorphism. Suppose that M is any R-module. By the previous case, we can find an injective $\mathbb{Z}$-module Q such that $f_*M \hookrightarrow Q$. Since the left adjoint f_* is faithful, it follows that the unit map $M \to f^!f_*M$ of the adjunction $f_* \dashv f^!$ is a monomorphism (check!); then we have the composition of monomorphisms

$$M \hookrightarrow f^!f_*M \hookrightarrow f^!Q,$$

where the second step uses that $f^!$ is left-exact (8.1.3). Since $f^!Q$ is an injective R-module thanks to 8.1.10(b), we are done.

■

Remark 8.1.13. Not all divisible modules are injective; see 10.6.8. In fact, it can be shown that for a domain R, all divisible R-modules are injective iff R is a Dedekind domain; see [16, 3.24].

[4] By this, we mean that if $ar = 0$ for $a \in R$, then $a = 0$. An r not satisfying this condition is called a right zerodivisor. Of course, over commutative rings, it is clear what a nonzerodivisor is.

The final notion that we will need is that of a *flat* R-module. We'll pick one side to work on; the other side is completely symmetric.

Proposition/Definition 8.1.14 (Flat Modules)**.** Let R be a ring and F a right R-module. The following conditions are equivalent:

(a) The functor $F \otimes_R - : R\text{-}\mathsf{Mod} \to \mathsf{Ab}$ is exact.
(b) If $0 \to M \to N$ is exact in R-Mod, then so is $0 \to F \otimes_R M \to F \otimes_R N$.
(c) If $0 \to M \to N$ is exact in R-Mod with N finitely generated, then so is $0 \to F \otimes_R M \to F \otimes_R N$.
(d) If $0 \to M \to N$ is exact in R-Mod with N finite free, then so is $0 \to F \otimes_R M \to F \otimes_R N$.
(e) If $\mathfrak{a} \subset R$ is any left ideal, the natural map $F \otimes_R \mathfrak{a} \to F$ is injective.
(f) If $\mathfrak{a} \subset R$ is any finitely generated left ideal, the natural map $F \otimes_R \mathfrak{a} \to F$ is injective.
(g) (Equational Criterion) Every relation in F is trivial. In other words, suppose we are given a finitely generated free R-module G and a morphism $f : G \to F$. Then for any morphism $a : R \to G$ such that $fa = 0$ ("a relation in F"), there is a finitely generated free module H and morphisms $b : G \to H$ and $g : H \to F$ such that $ba = 0$ and $f = gb$ ("the relation is trivial").

$$\begin{tikzcd}
 & H \arrow[dr, dashed, "\exists g"] & \\
R \arrow[r, "a"] & G \arrow[u, dashed, "\exists b"] \arrow[r, "f"] & F.
\end{tikzcd}$$

Proof. In light of 8.1.5(d) and the fact that $F \otimes_R -$ commutes with colimits, the equivalence (a) ⇔ (b) ⇔ (c) ⇒ (d) ⇒ (e) ⇔ (f) and (g) ⇒ (f) is clear.

(d) ⇒ (c) Pick a surjection $G \twoheadrightarrow N$ from a finite free R-module G, let K be its kernel, and let $H \hookrightarrow G$ be the pull-back of $M \hookrightarrow N$ along $G \to N$ to produce a commutative diagram with exact rows of the form

$$\begin{tikzcd}
0 \arrow[r] & K \arrow[r] \arrow[d, "="] & H \arrow[r] \arrow[d] & M \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & K \arrow[r] & G \arrow[r] & N \arrow[r] & 0.
\end{tikzcd}$$

We finish by the Snake Lemma and the fact that $F \otimes_R H \to F \otimes_R G$ is injective.

(e) ⇒ (d) We induct on the rank $r \in \mathbb{Z}_{\geq 0}$ of N, with $r = 0$ obvious and $r = 1$ by hypothesis. Suppose $r \geq 2$, and fix an inclusion $R \to N$ of a basis vector. Let $\mathfrak{a} \to R$ be the pull-back of $M \to N$ under this map, so we have a commutative diagram with exact rows of the form

$$\begin{tikzcd}
0 \arrow[r] & \mathfrak{a} \arrow[r] \arrow[d] & M \arrow[r] \arrow[d] & M/\mathfrak{a} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & R \arrow[r] & N \arrow[r] & N/R \arrow[r] & 0,
\end{tikzcd}$$

where all the vertical arrows are injections. Tensoring with F gives the commutative diagram

$$\begin{tikzcd}
 & F \otimes_R \mathfrak{a} \arrow[r] \arrow[d] & F \otimes_R M \arrow[r] \arrow[d] & F \otimes_R M/\mathfrak{a} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & F \arrow[r] & F \otimes_R N \arrow[r] & F \otimes_R (N/R) \arrow[r] & 0.
\end{tikzcd}$$

The left vertical map is injective by hypothesis, and the right vertical map is injective by induction; the Snake Lemma then tells us that the middle vertical map is an injection too.

(f) ⇒ (g) Let $r := \operatorname{rank} G \in \mathbb{Z}_{\geq 0}$, and fix an isomorphism $G \cong R^{\oplus r}$. Under this identification, a corresponds to an $r \times 1$ vector say with coordinates $a_1, \ldots, a_r \in R$; similarly, f corresponds to a $1 \times r$ vector with entries say $f_1, \ldots, f_r \in F$. The statement $fa = 0$ means precisely $\sum_{i=1}^r f_i a_i = 0$, so by hypothesis that $\sum_{i=1}^r f_i \otimes a_i = 0 \in F \otimes_R \mathfrak{a}$, where $\mathfrak{a} := (a_1, \ldots, a_r) \subset R$. The result then follows immediately from 8.1.15 below.

■

Lemma 8.1.15 (Equational Criterion)**.** Let R be a ring, $M \in \mathsf{Mod}\text{-}R$, and $N \in R\text{-}\mathsf{Mod}$. Suppose that N is generated by a family of elements n_i. Every element of $M \otimes_R N$ can be written as $\sum_i m_i \otimes n_i$ for some $m_i \in M$. Such an expression is zero iff there are elements m'_j of M and b_{ij} of R such that for all i we have $\sum_j m'_j b_{ij} = m_i$ and for all j we have $\sum_i b_{ij} n_i = 0$.

Proof. ([8, Lemma 6.4]) One direction is clear. For the other, pick a presentation $0 \to K \to G \xrightarrow{n} N \to 0$ with G free, chosen so the generators g_i of G map to the n_i. Since $M \otimes_R -$ is right exact (8.1.5), we have the exact sequence

$$M \otimes_R K \to M \otimes_R G \to M \otimes_R N \to 0.$$

By hypothesis, $\sum_i m_i \otimes g_i$ maps to zero in $M \otimes_R N$, so it is in $M \otimes_R F$. Writing it as $\sum_j m'_j \otimes b_j$ with each $b_j \in K$, say $b_j = \sum_i b_{ij} g_i$ gives the required expression. ■

Let's now give some examples. We will have much more to say about flatness in 9.2.

Lemma 8.1.16.

(a) Projective modules are flat.
(b) Flat modules are torsion-free. If R is a (commutative) PID, then a torsion-free R-module is flat.[5]
(c) If $f : R \to S$ is a ring homomorphism and F a flat left R-module, then $f^*P = S \otimes_R F$ is a flat left S-module.

Proof.

(a) Given a ring R, the ring R itself is a flat R-module, and since $\otimes$ commutes with $\oplus$, given a family F_i of modules, the sum $\bigoplus F_i$ is flat iff each F_i is. In particular, free modules are flat, and so are their direct summands, i.e., projective modules.
(b) If F is a flat right module and $a \in R$ is a nonzerodivisor, then the map $R \xrightarrow{a} R$ is injective, and hence so is the map $F \xrightarrow{a} F$ given by tensoring by F. When R is a commutative PID, the converse follows from 8.1.14(e).
(c) The functor $- \otimes_S f^*F : \mathsf{Mod}\text{-}S \to \mathsf{Ab}$ can be factored as $\mathsf{Mod}\text{-}S \xrightarrow{f_*} \mathsf{Mod}\text{-}R \xrightarrow{-\otimes_R F} \mathsf{Ab}$; now use 8.1.3.

■

Example 8.1.17.

(a) We say that a ring homomorphism $f : R \to S$ (of commutative rings, for simplicity) is *flat* if S is flat as a module over R; for instance, if R is a (commutative) ring and $S \subset R$ a multiplicative subset, then the localization $R \to S^{-1}R$ is flat by 1.1.9. In particular, for any (commutative) domain R, the field of fractions $R \to \operatorname{Frac} R$ is flat.
(b) The $\mathbb{Z}$-module $\mathbb{Q}$ is flat but not projective, since it is not free (8.1.7(a)). The $\mathbb{Z}$-module $\mathbb{Q}/\mathbb{Z}$ is injective but not flat.

[5] A right module F over a ring R is said to be *torsion-free* iff for all $f \in F$ and $a \in R$ such that $fa = 0$, then either $f = 0$ or a is a zerodivisor for R.

(c) Let k be a field, and $R := k[X, Y]$. The torsion-free R-module $(X, Y) \subset R$ is *not* flat; indeed, the relation $(-Y) \cdot X + X \cdot Y = 0$ in (X, Y) is not trivial (8.4).

Remark 8.1.18. For a different proof of 8.1.16(a) when R is commutative (for simplicity), we can argue as follows. From 8.1.12(c), a morphism $\phi : M \to N$ of modules is injective iff for all injective modules Q, the morphism $\phi^* : \mathrm{Hom}_R(N, Q) \to \mathrm{Hom}_R(M, Q)$ of R-modules is surjective. Given modules P, Q, and a module homomorphism $\phi : M \to N$ we have a commutative diagram

$$\begin{tikzcd}
\mathrm{Hom}_R(P \otimes_R N, Q) \arrow[r] \arrow[d, "\sim"] & \mathrm{Hom}_R(P \otimes_R N, Q) \arrow[d, "\sim"] \\
\mathrm{Hom}_R(P, \mathrm{Hom}_R(N, Q)) \arrow[r] & \mathrm{Hom}_R(P, \mathrm{Hom}_R(M, Q)).
\end{tikzcd}$$

If ϕ is injective and Q is injective, then ϕ^* is surjective; if, in addition, P is projective, then the bottom row is surjective, and hence commutativity tells us that the top row is surjective. If this is true for all Q, then we conclude that $P \otimes_R M \hookrightarrow P \otimes_R N$, which is saying that P is flat as needed. [TODO Lambek]

Remark 8.1.19. Once we know that flatness is local [TODO], we will see that 8.1.16(b) says more generally that a torsion-free module over a Dedekind domain is flat.

8.2 Derived Functors: Tor and Ext

Let R be a ring. Let $M \in \mathsf{Mod}\text{-}R$. The additive functor $M \otimes_R - : R\text{-}\mathsf{Mod} \to \mathsf{Ab}$ is right-exact (8.1.5(d)), and the category R-Mod has enough projectives (8.1.7(c)), so by 10.5.8, we are allowed to make

Definition 8.2.1. In the above setting, we define

$$\mathrm{Tor}^R_\bullet(M, -) := \mathsf{L}_\bullet(M \otimes_R -) : R\text{-}\mathsf{Mod} \to \mathsf{Ab}.$$

Observation 8.2.2. The following are clear from the definition.

(a) For a fixed N, the map $M \mapsto \mathrm{Tor}^R_\bullet(M, N)$ is a covariant functor in M. There is a natural isomorphism of additive functors $\mathrm{Tor}^R_0(M, -) \cong M \otimes_R -$, natural in M.

(b) Tor can be computed as follows: given an $N \in R\text{-}\mathsf{Mod}$, pick a projective resolution $Q_\bullet \to N[0]$ of N, tensor with M to get the sequence of abelian groups $M \otimes_R Q_\bullet$, and then $\mathrm{Tor}^R_\bullet(M, N) \cong \mathrm{H}_\bullet(M \otimes_R Q)$. The magic of derived functors (10.5) tells us that this is independent of the choice of Q; further, given a short exact sequence $0 \to N' \to N \to N'' \to 0$ it produces the usual long exact sequence of Tors, which is further natural in the short exact sequence.

(c) The module M is flat iff $\mathrm{Tor}^R_{>0}(M, -) = 0$ iff $\mathrm{Tor}^R_1(M, -) = 0$ (10.5.2); by 8.1.14 and 8.2.6, this is further equivalent to the statement that $\mathrm{Tor}^R_1(M, R/\mathfrak{a}) = 0$ for a finitely generated left ideal $\mathfrak{a} \subset R$.

(d) If M is flat or N is projective, then $\mathrm{Tor}^R_{>0}(M, N) = 0$. More generally, if N has a projective resolution of length $n \in \mathbb{Z}_{\geq 0}$, then for any M we have $\mathrm{Tor}^R_{>n}(M, N) = 0$.

(e) If $\{M_\lambda\}$ is a direct system of right R-modules, then for any N we have

$$\varinjlim_\lambda \mathrm{Tor}^R_\bullet(M_\lambda, N) \xrightarrow{\sim} \mathrm{Tor}^R_\bullet(\varinjlim_\lambda M_\lambda, N).$$

This is because of (b) and the fact that $- \otimes_R P_i$, as well as taking homology, preserves limits.

Similarly, given an $N \in R\text{-}\mathsf{Mod}$, the additive functor $- \otimes_R : \mathsf{Mod}\text{-}R \to \mathsf{Ab}$ is also right-exact (8.1.5(c)), and the category Mod-R has enough projectives (8.1.7(c)), so by 10.5.8 we can also define $\mathrm{Tor}^R_\bullet(-, N) := \mathsf{L}_\bullet(- \otimes_R N) : R\text{-}\mathsf{Mod} \to \mathsf{Ab}$. This does not yield a different definition of Tor than 8.2.1 thanks to

Lemma 8.2.3. Given $M \in \mathsf{Mod}\text{-}R$ and $N \in R\text{-}\mathsf{Mod}$, the two definitions of $\mathrm{Tor}^R_\bullet(M, N)$ above agree.

Proof 1. Fix a left R-module N and a projective resolution $Q_\bullet \to N[0]$. It suffices to show that the functor $\mathsf{Mod}\text{-}R \to \mathsf{Ab}$ given by $M \mapsto \mathrm{H}_\bullet(M \otimes_R Q)$ is a (homological) universal δ-functor extending $- \otimes_R N$. Here the identification $M \otimes_R N \xrightarrow{\sim} \mathrm{H}_0(M \otimes_R Q)$ comes from the right-exactness of $- \otimes_R N$ (8.1.5(c)), and the long exact sequences and connecting homomorphisms δ associated to a short exact sequence $0 \to M' \to M \to M'' \to 0$ come from taking the long exact homology sequence associated to the short exact sequence of complexes $0 \to M' \otimes_R Q_\bullet \to M \otimes_R Q_\bullet \to M'' \otimes_R Q_\bullet \to 0$, where this sequence of complexes is exact because projective modules are flat (8.1.16(a)). By 10.5.5, it remains only to show that for $q \geq 1$, the functor $M \mapsto \mathrm{H}_q(M \otimes_R Q)$ is coeffaceable. This in turn follows from the fact that P is a resolution and Mod-R has enough projectives; therefore, if we take a projective (for simplicity of argument, say free) module P and surjection $P \twoheadrightarrow M$, then necessarily $\mathrm{H}_q(P \otimes_R Q) = 0$ for $q \geq 1$. ■

Proof 2. Take projective resolutions $P_\bullet \to M[0]$ and $Q_\bullet \to N[0]$ of M and N respectively, and consider the first-quadrant double complex given by their tensor product $P \otimes_R Q$. The corresponding counterclockwise spectral sequence has E^1 page $E^1_{p,q} = \mathrm{Tor}^R_p(M, Q_q)$, which is supported on $p = 0$ because each Q_q is projective and hence flat (8.1.16(a)). The vertical differentials on the E^1 page can be identified with $1_M \otimes \partial_Q$, and hence the E^2 page is supported on $p = 0$ with $E^2_{0,q} = \mathrm{Tor}^R_q(M, N)$. At this point, all further differentials are zero, the spectral sequence abuts, and the total homology of the double complex is exactly $\mathrm{H}_\bullet(P \otimes_R Q) \cong \mathrm{Tor}^R_\bullet(M, N)$ using the first definition.[6] The symmetric argument in the other direction then tells us that $\mathrm{H}_\bullet(P \otimes_R Q)$ can be identified with $\mathrm{Tor}^R_\bullet(M, N)$ using the second definition. In particular, the two definitions agree with each other and with the homology of the double complex. ■

In particular, $\mathrm{Tor}^R_\bullet(M, N)$ can be computed by taking a projective resolution $P_\bullet \to M[0]$ of M, taking $- \otimes_R N$, and then taking homology; a short exact sequence $0 \to M' \to M \to M'' \to 0$ also produces a long exact sequence of Tors; the limiting behavior of 8.2.2(c) is true in the second variable as well; and if either M or N is flat, then $\mathrm{Tor}^R_{>0}(M, N) = 0$.[7] Finally, if R is a commutative ring, then in the above, all functors can be upgraded to have target $R\text{-}\mathsf{Mod}$ instead of Ab; i.e., for any R-modules M, N and $n \in \mathbb{Z}_{\geq 0}$, the abelian group $\mathrm{Tor}^R_n(M, N)$ has the natural structure of an R-module. The naturality means also that for any M, N and $a \in R$, the endomorphism of $\mathrm{Tor}^R_\bullet(M, N)$ induced by multiplication by a on either M or N is precisely again multiplication by a; this again follows from the δ-functor framework.

Finally, when R is a commutative ring, the symmetry of $\otimes_R$ manifests itself also in a derived form:

Lemma 8.2.4. When R is a commutative ring, then for R-modules M, N we have natural isomorphisms

$$\mathrm{Tor}^R_\bullet(M, N) \cong \mathrm{Tor}^R_\bullet(N, M).$$

Proof. Follows from the natural isomorphism $M \otimes_R N \cong_{R\text{-}\mathsf{Mod}} N \otimes_R M$ combined with 8.2.3 (check!). ■

Example 8.2.5. When R is a (commutative) PID, then every R-module has a projective resolution of length 1: pick a surjection from a free module, and then conclude using that every submodule of a free module is free (c.f. footnote 2). In particular, we have $\mathrm{Tor}^R_{>1} = 0$, so that Tor^R_1 can reasonably just be called Tor or Tor^R. For instance, when $R = \mathbb{Z}$, then $\mathrm{Tor} = \mathrm{Tor}^{\mathbb{Z}}_1$ is also called the *torsion product*, and sometimes denoted by $*$. Further, the short exact sequence $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$ combined with the fact that $\mathbb{Z}$ and $\mathbb{Q}$ are flat (8.1.16(b)) tells us that for any abelian group M, we have that $M * (\mathbb{Q}/\mathbb{Z}) := \mathrm{Tor}(M, \mathbb{Q}/\mathbb{Z}) \cong \ker(M \to \mathbb{Q} \otimes_{\mathbb{Z}} M) = \mathrm{Tors}(M)$ is the torsion-submodule of M. This is essentially where the name comes from. See also 8.2.6 and 8.2.7.

Example 8.2.6. Let R be a ring and $\mathfrak{a} \subset R$ a left ideal. For an $M \in R\text{-}\mathsf{Mod}$, we have

$$\mathrm{Tor}^R_n(R/\mathfrak{a}, M) \cong \begin{cases} M/\mathfrak{a}M, & n = 0, \\ \ker(\mathfrak{a} \otimes_R M \to M), & n = 1, \text{ and} \\ \mathrm{Tor}^R_{n+1}(\mathfrak{a}, M), & n \geq 2. \end{cases}$$

In particular, when $\mathfrak{a} = (a)$ for a nonzerodivisor a, so that the map $R \to (a)$ given by $1 \mapsto a$ is

[6] More precisely, the horizontal morphism induces a quasi-isomorphism of the total complex with $M \otimes_R Q_\bullet$. This is useful when you are using this argument to prove that the isomorphism between the two definitions of Tor is natural, but we won't pursue this too much here.

[7] The above suggests a theory of derived bifunctors so that Tor is the derived functor of $- \otimes_R -$. Such a theory does indeed exist, but is best done in the context of derived categories. [TOCITE]

an isomorphism, we have that

$$\operatorname{Tor}_n^R(R/(a), M) \cong \begin{cases} M/aM, & n = 0, \\ M[a], & n = 1, \text{ and } \\ 0, & n \geq 2. \end{cases}.$$

Example 8.2.7. We compute $\operatorname{Tor}(M, N) = \operatorname{Tor}_1^R(M, N)$ for any finitely generated modules M and N over a PID R. Since $\operatorname{Tor}(R, N) = 0$ for any N, we have for any M, N that

$$\operatorname{Tor}(\operatorname{Tors}(M), \operatorname{Tors}(N)) \xrightarrow{\sim} \operatorname{Tor}(M, N).$$

When M is finitely generated, $\operatorname{Tors}(M)$ is a direct sum of cyclic modules of the form R/p^a for prime p and $a \in \mathbb{Z}_{\geq 1}$; therefore, by additivity, it suffices to compute using 8.2.6 that for primes p, q and $a, b \in \mathbb{Z}_{\geq 1}$,

$$(R/p^a) * (R/q^b) \cong \begin{cases} 0, & (p) \neq (q), \\ R/p^{\min\{a,b\}}, & (p) = (q). \end{cases}$$

This tells us in particular, that for any $m, n \in R \smallsetminus \{0\}$, we have the (non-canonical) isomorphism of abelian groups

$$(R/m) * (R/n) \cong R/\gcd(m, n) \cong (R/m) \otimes_R (R/n).$$

Similar work with the Hom functor instead of $\otimes$ leads us to the Ext functors, already introduced in 10.5.9, but which we redo here in the category of modules. Specifically, let R be a ring as before, and let $M \in R\text{-}\mathsf{Mod}$. The additive functor $\operatorname{Hom}_R(M, -) = \operatorname{Hom}_{(R,\mathbb{Z})}(M, -) : R\text{-}\mathsf{Mod} \to \mathsf{Ab}$ is left-exact (8.1.5(a)), and the category $R\text{-}\mathsf{Mod}$ has enough injectives (8.1.12(c)), so by 10.5.8 we are allowed to make

Definition 8.2.8. In the above setting, we define

$$\operatorname{Ext}_R^\bullet(M, -) := \mathsf{R}^\bullet \operatorname{Hom}_R(M, -) : R\text{-}\mathsf{Mod} \to \mathsf{Ab}.$$

Clearly, remarks analogous to 8.2.2 hold for Ext as well as for Tor. The same proofs with minor modifications as in 8.2.3 then show that $\operatorname{Ext}_R^\bullet(-, N)$ can also be defined as $\mathsf{R}^\bullet \operatorname{Hom}_R(-, N)$; this uses that $R\text{-}\mathsf{Mod}$ has both enough projectives and enough injectives. Indeed, fixing an $M \in R\text{-}\mathsf{Mod}$ and a projective resolution $P_\bullet \to M[0]$, it suffices to show that $N \mapsto \mathrm{H}^\bullet \operatorname{Hom}_R(P, N)$ is a (homological) universal δ-functor extending $\operatorname{Hom}_R(M, -)$. The proof proceeds as before, and the coeffaceability of $N \mapsto \mathrm{H}^q \operatorname{Hom}_R(P, N)$ for $q \geq 1$ follows because this functor is evidently zero when N is injective, and $R\text{-}\mathsf{Mod}$ has enough injectives (8.1.12). The spectral sequence argument is similar as well.

In all, we have produced a sequence of bifunctors $R\text{-}\mathsf{Mod}^{\mathrm{op}} \times R\text{-}\mathsf{Mod} \to \mathsf{Ab}$ given by $(M, N) \mapsto \operatorname{Ext}_R^\bullet(M, N)$ which are contravariant in M and covariant in N. As before, if R is a commutative ring, then these can be upgraded to lie in $R\text{-}\mathsf{Mod}$. The advantage of this bifunctor perspective is that the follow statement is then clear from 10.5.2: if $M, N \in R\text{-}\mathsf{Mod}$, then M is projective iff $\operatorname{Ext}_R^{>0}(M, -) = 0$ iff $\operatorname{Ext}_R^1(M, -) = 0$; similarly, N is injective iff $\operatorname{Ext}_R^{>0}(-, N) = 0$ iff $\operatorname{Ext}_R^1(-, N) = 0$. More generally, if M has a projective resolution of length $n \in \mathbb{Z}_{\geq 0}$, or if N has an injective resolution of length n, then $\operatorname{Ext}_R^{>n}(M, N) = 0$.

We leave the computation of Exts along hypersurfaces and for PIDs as in 8.2.6 and 8.2.7 respectively to the reader.

Remark 8.2.9. As noted in 10.5.9, the group $\operatorname{Ext}_R^1(M, N)$ classifies the R-module extensions of M by N. The higher Ext groups also admit a similar, albeit more complication description, in terms of Yoneda extensions.

The functors Tor and Ext are ubiquitous in mathematics. Outside of their uses in commutative algebra and algebraic geometry, they are used in Lie theory, non-commutative algebra, and much more. Here are a couple of examples.

Example 8.2.10 (Lie Algebra (Co)homology)**.** Let R be a commutative unitary ring and $\mathfrak{g}$ be a Lie algebra over R. The universal enveloping algebra $U\mathfrak{g}$ of $\mathfrak{g}$ is an associative R-algebra such that representations of $\mathfrak{g}$ as a Lie algebra coincide with those of $U\mathfrak{g}$ as an associative algebra, i.e., the left module over $U\mathfrak{g}$. In particular, we have the trivial representation R which can be thought of both as a left $U\mathfrak{g}$-module and a right $U\mathfrak{g}$-module. In this context, for any $M \in U\mathfrak{g}\text{-}\mathsf{Mod}$, we define the Lie algebra (co)homology of M to be

$$\mathrm{H}_\bullet(\mathfrak{g}; M) := \mathrm{Tor}_\bullet^{U\mathfrak{g}}(R, M) \text{ and } \mathrm{H}^\bullet(\mathfrak{g}; M) := \mathrm{Ext}^\bullet_{U\mathfrak{g}}(R, M).$$

Several classical results in the theory of Lie algebras, such as Whitehead's theorems, Weyl's complete reducibility, and the Levi decomposition theorem can then be interpreted as statements about Lie algebra cohomology.

Example 8.2.11 (Hochschild (Co)homology)**.** Let k be a ring and A an associative k-algebra. We define the associated *enveloping algebra* to be $A^{\mathrm{e}} := A \otimes_k A^{\mathrm{op}}$, so that (A, A)-bimodules are the same thing as left A^{e}-modules and right A^{e}-modules. The k-bilinear multiplication map $A \otimes_k A \to A$ makes A into one such A^{e}-module. For any A^{e}-module M, we define the Hochschild (co)homology of A with coefficients in M to be

$$\mathrm{HH}_\bullet(A, M) := \mathrm{Tor}_\bullet^{A^{\mathrm{e}}}(A, M) \text{ and } \mathrm{HH}^\bullet(A, M) = \mathrm{Ext}^\bullet_{A^{\mathrm{e}}}(A, M).$$

These (co)homology groups are important tools in studying the deformation theory of associative algebras.

We end by defining various homological notions of dimension associated to rings and modules.

Definition 8.2.12. Let R be a ring and M be an R-module.

- Given an $n \in \mathbb{Z}_{\geq 0}$, by a *projective (resp. injective) resolution of length n* we mean a resolution $P_\bullet \to M[0]$ (resp. $M[0] \to I_\bullet$) such that P (resp. I) is supported only in degrees $0, 1, \ldots, n$.
- We define the *projective (resp. injective) dimension*, denoted $\mathrm{pd}(M)$ (resp. $\mathrm{id}(M)$) of M to be the infimum of the set of $n \in \mathbb{Z}_{\geq 0}$ for which M has a projective (resp. injective) resolution of length n (if M does in fact admit a finite projective (resp. injective) resolution, and ∞ otherwise).

Example 8.2.13.

(a) We have $\mathrm{pd}(M) = 0$ (resp. $\mathrm{id}(M) = 0$) iff M is projective (resp. injective).

(b) If R is a (commutative) PID, then for any R-module M, we have that $\mathrm{pd}(M) \leq 1$, with equality iff M is not free.

Theorem/Definition 8.2.14 (Global Dimension)**.** Let R be a ring, $M, N \in R\text{-}\mathsf{Mod}$, and $n \in \mathbb{Z}_{\geq 0}$. The following conditions are equivalent:

(a) We have $\mathrm{pd}(M) \leq n$.

(b) We have $\mathrm{Ext}_R^{>n}(M, -) = 0$.

(c) We have $\mathrm{Ext}_R^{n+1}(M, -) = 0$.

(d) If $0 \to P_n \to P_{n-1} \to \cdots \to P_0 \to M \to 0$ is an exact sequence with $P_0, \ldots, P_{n-1}$ projective, then also P_n is projective.

Dually, the following conditions are equivalent:

(a) We have $\mathrm{id}(N) \leq n$.
(b) We have $\mathrm{Ext}_R^{\geq n}(-, N) = 0$.
(c) We have $\mathrm{Ext}_R^{n+1}(-, N) = 0$.
(d) If $0 \to N \to I_0 \to I_1 \to \cdots \to I_{n-1} \to I_n \to 0$ is an exact sequence with $I_0, \ldots, I_{n-1}$ injective, then also I_n is injective.

In particular, we define the *global dimension* of the ring R to be

$$\mathrm{gd}(R) := \sup\{\mathrm{pd}(M) : M \in R\text{-}\mathsf{Mod}\} = \sup\{\mathrm{id}(M) : M \in R\text{-}\mathsf{Mod}\} = \inf\{n \in \mathbb{Z}_{\geq 0} : \mathrm{Ext}_R^{n+1} \equiv 0\}.$$

Proof. In both cases, (a) ⇒ (b) ⇒ (c) and (d) ⇒ (a) is clear, while (c) ⇒ (d) is proven by *degree-shifting*: in both cases, $\mathrm{Ext}_R^{n+1}(M, N)$ is isomorphic to $\mathrm{Ext}_R^1(P_n, N)$ and $\mathrm{Ext}_R^1(M, I_n)$ respectively. The proofs are similar, so we just do the first one. Given a sequence $0 \to P_n \to \cdots \to P_0 \to M \to 0$ as above, break it up into short exact sequences of the form

$$0 \to K_0 \to P_0 \to M \to 0 \text{ and } 0 \to K_j \to P_j \to K_{j-1} \to 0 \text{ for } j = 1, \ldots, n$$

with $P_n \xrightarrow{\sim} K_n$. Now finish the proof by noting that if $0 \to P' \to P \to P'' \to 0$ is a short exact sequence with P projective, then for all $N \in R\text{-}\mathsf{Mod}$ and $i > 0$ we have that $\mathrm{Ext}_R^i(P'', N) \xrightarrow{\sim} \mathrm{Ext}_R^{i+1}(P', N)$. ■

Example 8.2.15.

(a) For a commutative ring R, we have $\mathrm{gd}(R) = 0$ iff R is a reduced Artinian ring (8.3). In particular, if R is also a domain or a local ring, then R is a field.
(b) If R is a commutative domain, then $\mathrm{gd}\, R \leq 1$ iff R is a PID. One direction is clear now, and the other will be shown in [TODO].

These examples suggest that rings of finite global dimension are rather special. This is indeed true: [TOCITE].

8.3 First Applications of Homological Methods

In this section, we see how to apply homological methods to solve problems in commutative algebra. We first start by showing that finitely generated flat modules over a local ring are free, and using this to show that for finitely presented modules, being projective is the same thing as being flat, which is in turn the same as being locally free. Next, we give a characterization in terms of Tor for a Noetherian local ring to have bounded global dimension. Finally, we give a homological characterization of depth to show that maximal regular sequences under suitable hypotheses always have the same length.

In this section and in what follows, we again assume that our rings are commutative.

Theorem 8.3.1. Let $(R, \mathfrak{m}, k)$ be a local ring and M a finitely generated R-module. The following conditions on M are equivalent.

(a) M is free.
(b) M is projective.
(c) M is flat.

When M is finitely presented, these are further equivalent to:

(d) $\operatorname{Tor}_1^R(k, M) = 0$.

Recall as mentioned in 8.1.8 that the implication (b) ⇒ (a) does not need finite generation. In the present case, the implications (a) ⇒ (b) ⇒ (c) ⇒ (d) are clear.

Proof 1, when M is finitely presented. We show (d) ⇒ (a). Let $n := \dim_k k \otimes_R M$, and using 1.5.4, pick a surjection $F \to M$ with F free of rank n. Let K be the kernel, so there is a short exact sequence $0 \to K \to F \to M \to 0$. By the persistence property of finite presentation[8], the R-module K is finitely generated. Tensoring with k and passing to the associated long exact sequence gives us

$$0 = \operatorname{Tor}_1^R(k, M) \to k \otimes_R K \to k \otimes_R F \to k \otimes_R M \to 0.$$

Since $k \otimes_R F \xrightarrow{\sim} k \otimes_R M$ (for dimension reasons), we conclude that $k \otimes_R K = K/\mathfrak{m}K = 0$, and hence using 1.5.3 that $K = 0$. ■

Proof 2, in general. ([7, Thm. 7.10]) We use the equational criterion (8.1.14(g)) to show that if $n \in \mathbb{Z}_{\geq 1}$ and $m_1, \ldots, m_n \in M$ are elements such that $\{\overline{m}_1, \ldots, \overline{m}_n\}$ is k-linearly independent in $k \otimes_R M$, then the m_i are free: if there is a linear relation $\sum_{j=1}^n a_j m_j = 0$ with $a_j \in R$, then each $a_j = 0$. This suffices by 1.5.4.

We proceed by induction on n. When $n = 1$ and $m := m_1$ and $a := a_1$, then by 8.1.14(g), there are $b_i \in R$ and $m_i \in M$ such that $m = \sum_i b_i m_i$ and for all i we have $ab_i = 0$. Since $m \notin \mathfrak{m}M$, there is a i such that $b_i \notin \mathfrak{m}$, and then $ab_i = 0$ implies that $a = 0$.

Suppose now that $n \geq 2$. As above, there are $b_{ij} \in R$ and $m_i' \in M$ such that for all j we have $m_j = \sum_i b_{ij} m_i'$ and for all i we have $\sum_j a_j b_{ij} = 0$. Since $m_n \notin \mathfrak{m}M$, there is an i such that b_{in} is a unit, so a_n is a linear combination of $a_1, \ldots, a_{n-1}$. Write $a_n = \sum_{j=1}^{n-1} c_j a_j$ for $c_j \in R$, so that $\sum_{j=1}^{n-1} a_j(m_j + c_j m_n) = 0$. Since the elements $\overline{m_j + c_j m_n}$ of $k \otimes_R M$ are linearly independent, we conclude by induction that $a_j = 0$ for $j = 1, \ldots, n-1$ and hence $a_n = 0$ as well. ■

Corollary 8.3.2. Let R be a ring and M be a finitely presented R-module (e.g., when R is Noetherian and M finitely generated). The following conditions on M are equivalent.

[8] This is even easier when R is Noetherian.

(a) M is Zariski-locally free, i.e., for all primes $\mathfrak{p} \subset R$, there is an $f \in R$ with $f \notin \mathfrak{p}$ and $R[f^{-1}] \otimes_R M$ is a free $R[f^{-1}]$-module.
(b) For all primes $\mathfrak{p} \subset R$, the localization $M_\mathfrak{p}$ is a free $R_\mathfrak{p}$-module.
(c) For all maximal ideals $\mathfrak{m} \subset R$, the localization $M_\mathfrak{m}$ is a free $R_\mathfrak{m}$-module.
(d) M is projective.
(e) M is flat.
(f) For all maximal ideals $\mathfrak{m} \subset R$, we have $\operatorname{Tor}_1^R(R/\mathfrak{m}, M) = 0$.

Thus, for finitely presented modules, being flat is the same as being projective, which in turn is the same as being locally free.

Proof. The implications (a) ⇒ (b) ⇒ (c) and (e) ⇒ (f) are clear, and (d) ⇒ (e) is 8.1.16(a). ■

Corollary 8.3.3. Let $(R, \mathfrak{m}, k)$ be a Noetherian local ring, M a finitely generated R-module, and $n \in \mathbb{Z}_{\geq 0}$. The following are equivalent.

(a) $\operatorname{pd}(M) \leq n$.
(b) $\operatorname{Tor}_{>n}^R(-, M) = 0$.
(c) $\operatorname{Tor}_{n+1}^R(-, M) = 0$.
(d) $\operatorname{Tor}_{n+1}^R(k, M) = 0$.

Corollary 8.3.4. Let $(R, \mathfrak{m}, k)$ be a Noetherian local ring and $n \in \mathbb{Z}_{\geq 0}$. The following are equivalent.

(a) $\operatorname{gd}(R) \leq n$.
(b) $\operatorname{Tor}_{>n}^R = 0$.
(c) $\operatorname{Tor}_{n+1}^R = 0$.
(d) $\operatorname{Tor}_{n+1}^R(k, -) = 0$.
(e) $\operatorname{Tor}_{n+1}^R(k, k) = 0$.

8.4 Exercises

Exercise 8.1. Let $\mathscr{A}$ be any abelian category; think $\mathscr{A} = R\text{-}\mathsf{Mod}$ for some ring R if needed. Let $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ be a short exact sequence in $\mathscr{A}$. Show that the following conditions are equivalent:

(a) The monomorphism f splits, i.e. there is a morphism $p : M \to M'$ such that $pf = 1_{M'}$.
(b) The epimorphism g splits, i.e. there is a morphism $i : M'' \to M$ such that $gi = 1_{M''}$.
(c) There is an isomorphism of short exact sequences

$$\begin{tikzcd}
 & & M \arrow[dr, "g"] \arrow[dd, "\sim"] & & \\
0 \arrow[r] & M' \arrow[ur, "f"] \arrow[dr, "\iota"'] & & M'' \arrow[r] & 0. \\
 & & M' \oplus M'' \arrow[ur, "\pi"'] & &
\end{tikzcd}$$

(d) There is a morphism of short exact sequences as in (c), i.e. the condition in (c), except we do not necessarily require the map $M \to M' \oplus M''$ to be an isomorphism a priori.

When these equivalent conditions are satisfied, the sequence $0 \to M' \to M \to M'' \to 0$ is called *split*.

Exercise 8.2. Given a ring R and a diagram

$$\begin{tikzcd}
L \arrow[r, "g"] \arrow[d, "f"'] & M \\
Q &
\end{tikzcd}$$

in $R\text{-}\mathsf{Mod}$, explicitly identify the colimit P of this diagram (called the *pushout*) as a quotient of $M \oplus Q$. Let $f' : M \to P$ and $g' : Q \to P$ denote the maps that complete the pushout square, i.e.

$$\begin{tikzcd}
L \arrow[r, "g"] \arrow[d, "f"'] & M \arrow[d, "f'"] \\
Q \arrow[r, "g'"] & P.
\end{tikzcd}$$

Show that if f (resp. g) is a monomorphism, then so is f' (resp. g'), and the same holds with the word "monomorphism" replaced by "epimorphism".

Exercise 8.3. Show that the following conditions on a commutative ring R are equivalent:

(a) R is a reduced Artinian ring.
(b) R is a finite direct product of fields.
(c) Every R-module is projective.
(d) Every R-module is injective.
(e) Every short exact sequence of modules over R splits.
(f) Every R-module is semisimple.
(g) The global dimension $\operatorname{gd} R$ of R is zero.
(h) R is semisimple as a module over itself.

Exercise 8.4. Let k be a field, $R = k[X, Y]$, and $\mathfrak{a} := (X, Y) \subset R$. Show that the R-module $\mathfrak{a}$ is not flat, by showing that the relation $(-Y) \cdot X + X \cdot Y = 0$ is not trivial, i.e., given the short exact sequence

$$0 \to R \xrightarrow{a = \begin{bmatrix} -Y \\ X \end{bmatrix}} R^{\oplus 2} \xrightarrow{f = \begin{bmatrix} X & Y \end{bmatrix}} \mathfrak{a} \to 0,$$

there does not exist a finite free R-module H and morphisms $b : R^{\oplus 2} \to H$ and $g : H \to \mathfrak{a}$ such that $ba = 0$ and $f = gb$.

Chapter 9

Selected Advanced Topics

9.1 Unique Factorization II

Theorem 9.1.1 (Auslander-Buchsbaum)**.** A regular local ring is a UFD.

Theorem 9.1.2. If R is a regular UFD, then so are $R[X]$ and $R[\![X]\!]$.

Corollary 9.1.3. If K is a field, then for any $n \geq 1$ the ring $K[\![X_1, \dots, X_n]\!]$ is a UFD.

Proof. Clear from Theorem 9.1.2 by induction, since K is trivially a regular UFD. ■

Theorem 9.1.4. Let R be a Noetherian ring. Then $\dim R[X] = \dim R[\![X]\!] = \dim R + 1$.

Corollary 9.1.5. Let R be a Noetherian ring, and $\mathfrak{m}$ a maximal ideal. If the completion $\hat{R}_{\mathfrak{m}}$ is a UFD, then so is R.

9.2 More on Flatness

[Faithfully exact functors by Ishikawa] Flatness is local, filtered colimits, Dedekind domains, flat going down. Lambek's test. Connection to torsion-free. For finitely presented, flat is projective. For Noetherian ring R, have $\dim R[X] = \dim R[\![X]\!]$.

Chapter 10

Appendices

10.1 Length and the Jordan-Hölder Theorem

In this section, the base ring R is not necessarily commutative, and the word "R-module" refers to a left R-module. Much of what follows can be generalized to arbitrary abelian categories without much more effort.

Definition 10.1.1. Let R be a ring and M be an R-module.

(a) We say that M is *simple* if it is nonzero and has no nontrivial proper submodules.
(b) A finite chain of submodules $M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_n = 0$ is called a *composition series* of length $n \geq 1$ if each successive quotient M_i/M_{i+1} for $i = 0, \dots, n-1$ is simple. The successive quotients M_i/M_{i+1} are called the *composition factors* of the series.
(c) The *length* $\ell_R(M) \in \mathbb{N} \cup \{\infty\}$ is the infimum of the lengths of all composition series of M.

When R is commutative, every simple module is isomorphic to a field quotient of R. In general, a module has length 0 iff it is trivial, length 1 iff it is simple, and finite length iff it admits a finite composition series, so, for instance, $\ell_{\mathbb{Z}}(\mathbb{Z}) = \infty$. The notion of length generalizes that of dimension[1]: if $R = k$ is a field, then $\ell_k(M) = \dim_k M$.

Lemma 10.1.2. Let R be a ring and M be a nonzero R-module. If M is finitely generated, then M has a maximal proper submodule, and hence a simple quotient.

Proof. The collection $\mathscr{A}$ of all proper submodules of M is nonempty since $0 \in \mathscr{A}$. To invoke Zorn's Lemma, it remains to show that if (N_α) is a chain in $\mathscr{A}$, then $\bigcup_\alpha N_\alpha$ is proper. This follows from the fact that M is finitely generated: if $\bigcup_\alpha N_\alpha = M$, then finitely many generators of M lie in some N_α thanks to the total ordering. ■

Counterexample 10.1.3. Lemma 10.1.2 is false if we do not assume M to be finitely generated: take $R = \mathbb{Z}$ and $M = \mathbb{Q}$. The only simple $\mathbb{Z}$-modules are finite fields of prime order, but every $\mathbb{Z}$-module homomorphism from $\mathbb{Q}$ to a finite field is zero (Exercise 10.1). This gives us another proof of the well-known fact that $\mathbb{Q}$ is not a finitely generated abelian group.

Lemma 10.1.4. Let $M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_n = 0$ be a composition series of an R-module M, and let $N \subset M$ be a submodule. Then:

(a) Intersection with N gives a sequence of submodules of N as

$$N = M_0 \cap N \supset M_1 \cap N \supset \cdots \supset M_n \cap N = 0.$$

This sequence becomes a composition series for N after eliminating repetitions.

(b) Taking quotients by N gives a sequence of submodules of M/N as

$$M/N = M_0/N \supset (M_1 + N)/N \supset \cdots \supset (M_n + N)/N = 0.$$

This sequence becomes a composition series for M/N after eliminating repetitions.

In particular, for any submodule $N \subset M$ we have $\max\{\ell_R(N), \ell_R(M/N)\} \leq \ell_R(M)$.

Proof.

(a) For each i, the map $M_i \cap N \hookrightarrow M_i \twoheadrightarrow M_i/M_{i+1}$ has kernel $M_{i+1} \cap N$ giving us an injection

$$(M_i \cap N)/(M_{i+1} \cap N) \hookrightarrow M_i/M_{i+1}.$$

[1] At least in a naive way that conflates all infinite cardinalities.

(b) Similarly, for each i, the composite map

$$M_i \hookrightarrow M_i + N \twoheadrightarrow \frac{M_i + N}{M_{i+1} + N} \cong \frac{(M_i + N)/N}{(M_{i+1} + N)/N}$$

is surjective and its kernel contains M_{i+1}, giving us a surjection from M_i/M_{i+1} to this last module.

■

The key result is

Theorem/Definition 10.1.5 (Jordan-Hölder)**.** Let R be a ring and M an R-module. If $\ell_R(M) < \infty$, then the lengths and the multisets of factors of any two composition series of M are the same, so that $\ell_R(M)$ is the length of *any* composition series of M. The multiset of composition factors that appear in any composition series of M is called the multiset of *simple factors* of M.

Proof. We induct on $n := \ell_R(M)$. If $n = 0$, then $M = 0$ and the result is trivial; hence assume $n \geq 1$. Let $M = M_0 \supsetneq \cdots \supsetneq M_n = 0$ be a composition series of length n, and let $M = M'_0 \supsetneq \cdots \supsetneq M'_m = 0$ be another, for some $m \geq 0$. We have to show that $m = n$ and that the composition factors in both are the same. If $m = 0$, then $M = 0$ and $n = 0$, a contradiction; therefore, $m \geq 1$. If $M_1 = M'_1$, then we are done by induction, since $\ell_R(M_1) \leq n - 1$; therefore, assume that $M_1 \neq M'_1$. Since both M/M_1 and M/M'_1 are simple, we must have $M_1 + M'_1 = M$ and that $N := M_1 \cap M'_1 \subsetneq M_1, M'_1$. By Lemma 10.1.4, N has finite length; pick any finite composition series $N = N_0 \supsetneq N_1 \supsetneq \cdots \supsetneq N_r = 0$ for it. Then

$$\frac{M_1}{N} = \frac{M_1}{M_1 \cap M'_1} \cong \frac{M_1 + M'_1}{M'_1} = \frac{M}{M'_1} \text{ and similarly } \frac{M'_1}{N} \cong \frac{M}{M_1}.$$

Therefore, we get two new composition series for M that look like

$$M \supsetneq M_1 \supsetneq N \supsetneq N_1 \supsetneq \cdots \supsetneq N_r = 0 \text{ and } M \supsetneq M'_1 \supsetneq N \supsetneq N_1 \supsetneq \cdots \supsetneq N_r = 0$$

that differ only at the first step; these trivially have the same length and same composition factors. The same observation above (about when the first submodule in two composition series is the same) tells us that the first of these has the same length and the same factors as our original series; in particular, $r = n-2$. This in turn tells us, by looking at the second composition series, that $\ell_R(M'_1) \leq n - 1$, and so by induction the composition series $M'_1 \supsetneq M'_2 \supsetneq \cdots \supsetneq M'_m$ for it must have length $n - 1$, giving us $m = n$. That the multisets of composition factors agree follows immediately (check!). ■

Corollary 10.1.6. Let R be a ring.

(a) If $0 \to M' \to M \to M'' \to 0$ is a short exact sequence of R-modules, then

$$\ell_R(M) = \ell_R(M') + \ell_R(M'').$$

If $\ell_R(M) < \infty$, then the multiset of simple factors of M is the union of those of M' and M''.

(b) If M is an R-module of finite length $\ell_R(M)$, then every proper chain of submodules of M has length at most $\ell_R(M)$ and can be refined to a composition series.

Proof.

(a) First observe that the LHS is finite iff the RHS is: if M' and $M'' = M/M'$ have a finite composition series, then juxtaposing them gives a finite composition series for M; conversely, if M has a finite composition series, then so do M' and M'' by Lemma 10.1.4. The rest of the result follows from juxtaposition of two composition series.

(b) The second claim is clear since every subquotient of M has finite length by Lemma 10.1.4; then the first claim follows from Theorem 10.1.5.

■

The notion of simple modules can be generalized a little to that of *semisimple* modules.

Proposition/Definition 10.1.7. The following conditions on an R-module M are equivalent:

(a) M is the direct sum of some family of simple modules.

(b) M is the sum of some family of simple modules.

(c) Every short exact sequence $0 \to M' \to M \to M'' \to 0$ splits.

A module satisfying these equivalent properties is said to be *semisimple* or *completely reducible.*

Proof. The implication (a) ⇒ (b) is clear.

(b) ⇒ (a) Let $M = \sum_{i \in I} M_i$ with each M_i simple. We claim that there is a subset $I' \subset I$ such that $M = \bigoplus_{i \in I'} M_i$. Indeed, suppose without loss of generality that each $M_i \neq 0$ and consider the collection $\mathcal{C}$ of subsets J of I such that the sum $\sum_{j \in J} M_j$ is a direct sum. This is nonempty since $\emptyset \in \mathcal{C}$, and it is easy to see that Zorn's Lemma applies to $\mathcal{C}$, whence we get some maximal subset $I' \in \mathcal{C}$. Let $N := \bigoplus_{i \in I'} M_i = \sum_{i \in I'} M_i \subset M$. For each $j \in I$, if $M_j \cap N = 0$, then $I' \cup \{j\}$ is a strictly larger element of $\mathcal{C}$; therefore, $M_j \cap N \neq 0$, whence by simplicity of M_j we conclude that $M_j \subset N$. It follows then that $M = \sum_{j \in I} M_j \subset N$, whence $M = N$.

(b) ⇒ (c) Let $M' \hookrightarrow M$ be a submodule of M, and consider the collection

$$\mathscr{N} = \{N \subset M : N \text{ is the sum of simple modules and } N \cap M' = 0\}$$

of submodules of M. Using Zorn's Lemma, pick a maximal element N of $\mathscr{N}$; we claim that $M' \oplus N \xrightarrow{\sim} M$, giving a splitting of $M' \hookrightarrow M$. Indeed, $M' \cap N = 0$ by construction, and if $M' + N \subsetneq M$, then there is a simple module S in the family given that is not contained in $M' + N$. From the simplicity of S we conclude that $S \cap (M' + N) = 0$, whence $S + N \supsetneq N$ is a bigger element of $\mathscr{N}$, contradicting our choice of N.

(c) ⇒ (b) First note that the condition (c) passes to subquotients. Now, let $M' \subset M$ be the sum of all simple submodules of M. If $M' \subsetneq M$, choose a splitting of $M' \hookrightarrow M$ to produce a complementary submodule $M'' \subset M$, and pick a nonzero $m \in M''$. Find by Lemma 10.1.2 a maximal proper submodule $P \subset Rm$. Since (c) applies to Rm, pick a complementary submodule $S \subset Rm$ to P in Rm; then $S \cong Rm/P$ implies that S is simple and hence nonzero. But then $S \subset M'$ by definition of M', contradicting the fact that $M' \cap M'' = 0$.

■

Semisimple modules are the basic objects of study in *representation theory.*

10.2 Classical Algebra: Gauss and Eisenstein

In this section, we review some classical results the reader may have seen in an undergraduate course.

We start with Gauss's Lemma. For this, let R be a UFD and $K := \operatorname{Frac} R$.

Lemma/Definition 10.2.1. An $f \in R[X]$ is said to be *primitive* if the following equivalent conditions hold.

(a) If $\alpha \in R$ is such that $\alpha \mid f$, then $\alpha \in R^\times$.
(b) There is no prime $p \in R$ dividing f.
(c) The greatest common divisor of all the coefficients of f is (1).

Note that 0 is *not* primitive. Any $f \in K[X]$ can be written as $f = \operatorname{cont}(f) \cdot \tilde{f}$ for some $\operatorname{cont}(f) \in K$ and primitive $\tilde{f} \in R[X]$. If $f \neq 0$, then $\operatorname{cont}(f)$ and $\tilde{f}$ are uniquely determined up to units in R; the element $\operatorname{cont}(f) \in K$ is called the content of f, and $\tilde{f} \in R[X]$ is called the primitive part of f, defined uniquely only up to units in R.[2] Here are some basic properties that we will need:

Remark 10.2.2. For $0 \neq f \in K[X]$, we have:

(a) $\deg \tilde{f} = \deg f$,
(b) $\operatorname{cont}(f) = f$ iff f is constant,
(c) $f \in R[X]$ iff $\operatorname{cont}(f) \in R$,
(d) if (c) holds, then f is primitive iff $\operatorname{cont}(f)$ is a unit in R, and
(e) $\tilde{\tilde{f}} = \tilde{f}$.

The key result that allows us to relate $R[X]$ and $K[X]$ is

Lemma 10.2.3 (Gauss's Lemma)**.**

(a) If $f, g \in R[X]$ are primitive, then so is fg. In general, for nonzero $f, g \in K[X]$, we have $\operatorname{cont}(fg) = \operatorname{cont}(f)\operatorname{cont}(g)$ and $\widetilde{fg} = \tilde{f}\tilde{g}$ (up to units). The same holds for any number $f_1, \ldots, f_n$ of elements with $n \geq 1$.
(b) If $f, g \in R[X]$ are nonzero such that $f \mid g$ in $K[X]$ and f is primitive, then $f \mid g$ in $R[X]$.
(c) If $f \in R[X]$ is primitive and prime in $K[X]$, then f is prime in $R[X]$.

Proof.

(a) The general case follows by induction, so we do the case $n = 2$. The first statement follows from Exercise 1.19(b). In general, given nonzero $f, g \in K[X]$, we have $fg = \operatorname{cont}(f)\operatorname{cont}(g) \cdot \tilde{f}\tilde{g}$, and $\tilde{f}\tilde{g}$ is primitive by the first part, so by the uniqueness of this decomposition we must have $\widetilde{fg} = \tilde{f} \cdot \tilde{g}$, and hence that $\operatorname{cont}(fg) = \operatorname{cont}(f) \cdot \operatorname{cont}(g)$.
(b) If $g = fq$ for some nonzero $q \in K[X]$, then $\operatorname{cont}(g) = \operatorname{cont}(f) \cdot \operatorname{cont}(q)$. Since $f, g \in R[X]$, 10.2.2(c) tells us that $\operatorname{cont}(f), \operatorname{cont}(g) \in R$, and since f is primitive, 10.2.2(d) tells us that $\operatorname{cont}(f)$ is a unit, so that $\operatorname{cont}(q) = \operatorname{cont}(g)\operatorname{cont}(f)^{-1} \in R$. Hence, by 10.2.2(c) again we conclude that $q \in R[X]$.
(c) Suppose $f \in R[X]$ is primitive and prime in $K[X]$ (and hence nonzero), and suppose $f|gh$ for some $g, h \in R[X]$. Then $f \mid gh$ also in $K[X]$, and so by primality either $f|g$ or $f|h$ in $K[X]$, and hence also in $R[X]$ by (b), showing that f is prime in $R[X]$.

[2] One way to make this precise is to say that the fractional ideal $(\operatorname{cont} f)$ of R and the (integral) ideal $(\tilde{f})$ of $R[t]$ are uniquely determined. We will not need these notions. When we assert an equality involving $\operatorname{cont}(f)$ or $\tilde{f}$, that equality will always be assumed to hold up to units.

■

In 10.2.3(b), we certainly need f to be primitive; a simple counterexample otherwise is given by taking $R = \mathbb{Z}$ and $f(X) = 2X$ and $g(X) = X$. We are now ready to give

Proof of (a) ⇒ (b) of 1.4.10. Suppose R is a UFD and $K = \operatorname{Frac} R$. By Exercise 1.20(b) it suffices to show that every nonzero nonunit $f \in R[X]$ is a product of finitely many primes. Since $f = \operatorname{cont}(f) \cdot \tilde{f}$, it suffices to show that each of $\operatorname{cont}(f)$ and $\tilde{f}$ is a product of finitely many primes in $R[X]$.[3]

Since $0 \neq \operatorname{cont}(f) \in R$ and R is a UFD, either $\operatorname{cont}(f)$ is a unit in R (and hence in $R[X]$), or it is a product of one or more primes in R. Since primes in R are primes in $R[X]$ (Exercise 1.19(b)), it follows that $\operatorname{cont}(f)$ is a product of finitely many primes in $R[X]$.

Now consider the primitive part $0 \neq \tilde{f} \in R[X]$. Since $K[X]$ is a UFD, it follows that either $\tilde{f}$ is a unit in $K[X]$ or it is the product of one or more primes in $K[X]$. In the former case, $\tilde{f}$ is constan; since it is primitive, it must be a unit in R (by 10.2.2(b) and (d)). In the latter case, $\tilde{f}$ is the product of one or more primes in $K[X]$, say $\tilde{f} = f_1 \cdots f_n$ for some $n \geq 1$, where for $1 \leq j \leq n$, each $f_j \in K[X]$ is prime. Then using 10.2.2(e) and 10.2.3(a), we find that

$$\tilde{f} = \tilde{\tilde{f}} = \tilde{f}_1 \cdots \tilde{f}_n.$$

For each j, the element $\tilde{f}_j \in R[X]$ is primitive and prime in $K[X]$ (since it is a nonzero constant, i.e., unit, times the prime f_j in $K[X]$), and so by 10.2.3(c) is a prime in $R[X]$. Therefore, we have exhibited $\tilde{f}$ as a product of one or more primes in $R[X]$, finishing the proof. ■

Analyzing the above proof more carefully gives us a way to produce irreducible decompositions of elements of $R[X]$: factor the content in R, and the "polynomial part" in $K[X]$. Explicitly, we have

Lemma 10.2.4.

(a) If $f \in R[X]$ is irreducible and of positive degree, then f is irreducible in $K[X]$.
(b) If $f \in R[X]$ is primitive and irreducible in $K[X]$, then f is irreducible in $R[X]$.

Proof.

(a) In this case, f is a nonzero nonunit in $K[X]$. If $f = gh$ for $g, h \in K[X]$, then 10.2.3(a) tells us that $\tilde{f} = \tilde{g}\tilde{h}$, and then $f = (\operatorname{cont}(f) \cdot \tilde{g}) \cdot \tilde{h}$. Since f is irreducible in $R[X]$, either $\operatorname{cont}(f) \cdot \tilde{g}$ is a unit in R, in which case $\tilde{g}$ is a (nonzero) constant and hence $g \in K[X]^\times$ by 10.2.2(a), or simlarly $\tilde{h}$ is a unit in R, in which case $h \in K[X]^\times$.
(b) This is 10.2.3(c), given that the terms "prime" and "irreducible" are interchangable in both $R[X]$ and $K[X]$ thanks to 1.4.3(b) and 1.4.10.

■

Let us record here one last result which is often very useful. In any UFD R, we say that two elements $f, g \in R$ are relatively prime iff $\gcd(f, g) = 1$.

Lemma 10.2.5. If $f, g \in R[X]$ are relatively prime in $R[X]$, then

(a) they are relatively prime in $K[X]$, and
(b) there are $a, b \in R[X]$ and $0 \neq c \in R$ such that $af + bg = c$.

[3] Note that finitely many also includes zero many–i.e. it is okay for $\operatorname{cont}(f)$ or $\tilde{f}$ to be a unit in $R[X]$, but if both are units in $R[X]$, then so is $f = \operatorname{cont}(f) \cdot \tilde{f}$.

Proof.

(a) If there is a prime $q \in K[X]$ such that $q \mid f$ and $q \mid g$ in $K[X]$, then by rescaling we can assume without loss of generality that $q \in R[X]$ is primitive, and then 10.2.3(b) tells us that $q \mid f$ and $q \mid g$ in $R[X]$, and 10.2.3(c) tells us that q is prime in $R[X]$. This can't happen if $f, g \in R[t]$ are relatively prime in $R[t]$.

(b) This is clear from the Euclidean algorithm and backward substitution if R is a field. In general, clear denominators.

■

Let's now use these ideas to classify primes in a ring of the form $R[X]$ when R is a PID.

Theorem 10.2.6. If R is a PID, and $\mathfrak{p} \subseteq R[X]$ a prime, then $\mathfrak{p}$ is of one of the following forms:

(a) (0).

(b) (f) for some $f \in R[X]$ irreducible.

(c) (p) for some $p \in R$ nonzero prime.

(d) (p, f) for some $p \in R$ nonzero prime and $f \in R[X]$ monic such that f is irreducible modulo p. These primes are maximal, since the quotient by each such prime is an algebraic extension of the field R/p.

In particular, if R is a PID that is not a field, then $\dim R[X] = 2$.

The proof proceeds by analyzing the fibers of the projection $\mathbb{A}^1_R = \operatorname{Spec} R[X] \to \operatorname{Spec} R$.

Proof. Let $K = \operatorname{Frac} R$. Either $\mathfrak{p} \cap R = (0)$ or $\mathfrak{p} \cap R = (p)$ for some nonzero prime $p \in R$.

(a) If $\mathfrak{p} \cap R = (0)$, look at $(\mathfrak{p}) = \mathfrak{p}K[X] \subseteq K[X]$. By $\mathfrak{p} \cap (R \smallsetminus \{0\}) = \emptyset$, the prime $(\mathfrak{p}) \subseteq K[X]$ is proper. Since $K[X]$ is a PID, either $(\mathfrak{p}) = (0)$, in which case $\mathfrak{p} = (0)$, or $(\mathfrak{p}) = (f)$ for some $f \neq 0 \in K[X]$ irreducible. Now write $f = \operatorname{cont}(f)\tilde{f}$ for $\tilde{f} \in R[X]$ primitive, so that $(\mathfrak{p}) = (\tilde{f}) \subseteq K[X]$. We claim that $\mathfrak{p} = (\tilde{f}) \subseteq R[X]$; then $\tilde{f}$ is a nonzero prime and hence irreducible. For one direction, observe that $\tilde{f} \in (\mathfrak{p})$, so there is a $0 \neq r \in R$ such that $r\tilde{f} \in \mathfrak{p}$, but $r \notin \mathfrak{p}$ implies $\tilde{f} \in \mathfrak{p}$. For the other direction, if $g \in \mathfrak{p}$, then $g \in (\mathfrak{p}) = (\tilde{f}) \in K[X]$, so that $\tilde{f}$ divides g in $K[X]$. By 10.2.3(b), this means that $\tilde{f}$ divides g in $R[X]$, so that $g \in (\tilde{f}) \subseteq R[X]$.

(b) Suppose now that $\mathfrak{p} \cap R = (p)$ for some $p \in R$ nonzero prime. Then R/p is a field, and we can look at $\overline{\mathfrak{p}} \subseteq R[X]/(p) \cong (R/p)[X]$, which is a again a PID. Therefore, either $\overline{\mathfrak{p}} = (0)$, in which case $\mathfrak{p} = (p)$, else $\overline{\mathfrak{p}} = (\overline{f})$ for some $\overline{f} \in (R/p)[X]$ irreducible, which can without loss of generality be taken to be monic. Then lifting back to $R[X]$, we get that $\mathfrak{p} = (p, f)$ for some $f \in R[X]$ monic such that it remains irreducible mod p.

■

In particular, we now understand all primes of, for instance, $\mathbb{Z}[X]$. Similarly, we understand all the irreducible closed subschemes (and hence points!) of $\mathbb{A}^2_k$ for any field k.

We finish by recalling a famous irreducibility criterion and giving one application.

Theorem 10.2.7 (Eisenstein Irreducibility)**.** Let R be a ring and let $f = a_0X^n + \cdots + a_n \in R[X]$ be a polynomial for some $n \geq 1$. If there is a prime $\mathfrak{p} \subset R$ such that the following hold:

(a) The coefficient $a_0 \notin \mathfrak{p}$.

(b) For each $j = 1, \dots, n$, we have $a_j \in \mathfrak{p}$.
(c) We have $a_n \notin \mathfrak{p}^2$.

Then f is irreducible.

Proof. Examine the reduction of $f = gh$ in $R/\mathfrak{p}$ and use the following result: if R is a domain, and for some $n \geq 1$ we have $X^n = gh$ for some $g, h \in R[X]$, then there are $r, s \geq 0$ such that $r + s = n$ and $g = X^r, h = X^s$. Prove this by examining the first nonzero coefficient of g and h. ■

Such a polynomial f is said to be *Eisenstein* at the prime $\mathfrak{p}$.

Corollary 10.2.8. Prime-power cyclotomic polynomials are irreducible in $\mathbb{Q}[X]$.

Proof. We have for prime p and integer $r \geq 1$ that

$$(X^{p^{r-1}} - 1)\Phi_{p^r}(X) = X^{p^r} - 1 \Rightarrow \Phi_{p^r}(X+1) \equiv X^{p^{r-1}(p-1)} \pmod{p\mathbb{Z}[X]}$$

using that $(X+Y)^p = X^p + Y^p$ in $\mathbb{F}_p[X, Y]$. Also, $\Phi_{p^r}(1) = p \notin (p^2)$, so we are done by 10.2.7 and 10.2.4(a). ■

10.3 Dependence Relations

In this section we develop the fundamentals of abstract dependence relations that serve as the foundation for a lot of key concepts in commutative algebra and combinatorics.

Definition 10.3.1. Let S be a set. A *closure operator* on S is a map $\mathrm{Cl} : 2^S \to 2^S$ that is

(a) *extensive*, i.e. $X \subset \mathrm{Cl}\, X$ for all $X \subset S$,
(b) *increasing*, i.e. $X \subset Y \Rightarrow \mathrm{Cl}\, X \subset \mathrm{Cl}\, Y$ for all $X \subset Y \subset S$, and
(c) *idempotent*, i.e. $\mathrm{Cl}\,\mathrm{Cl}\, X = \mathrm{Cl}\, X$ for all $X \subset S$.

A closure operation Cl is said to

(d) be *finitary*, if for any $X \subset S$ we have $\mathrm{Cl}\, X = \bigcup_{\substack{X' \subset X \\ |X'| < \infty}} \mathrm{Cl}\, X'$.
(e) satisfy *MacLane-Steinitz exchange* if $x \in X \subset S$ and $y \in \mathrm{Cl}\, X \smallsetminus \mathrm{Cl}(X \smallsetminus \{x\})$ together imply that $x \in \mathrm{Cl}(X \smallsetminus \{x\} \cup \{y\})$,

Closure operators are ubiquitous in mathematics, with some examples being integral closure, algebraic closure, separable closure, abelian closure, unramified closure, differential closure, topological closure, graph closure, etc. Closure operators satisfying MacLane-Steinitz exchange are called *matroid closure operations*; readers familiar with matroids will recognize that the above conditions are reformulations of the matroid axioms.[4]

Definition 10.3.2. A *dependence relation* on a set S is a finitary closure operation satisfying MacLane-Steinitz exchange, i.e. a map $\mathscr{D} : 2^S \to 2^S$ satisfying (a)-(e). Given such a pair $(S, \mathscr{D})$, we say that a subset $X \subset S$ is

(a) *a spanning set* if $\mathscr{D}X = S$,
(b) *independent* if for all $x \in X$ we have $x \notin \mathscr{D}(X \smallsetminus \{x\})$, and
(c) *a basis* if it is both independent and a spanning set.

We say that $(S, \mathscr{D})$ is of *finite dependency* if it admits a finite spanning set. Finally, we define the *fundamental set* of the dependence relation to be $\mathscr{D}(\emptyset)$.

Here we think of $\mathscr{D}X$ as the set of elements of S which are *dependent* on those in X. We will show below that any two bases of S have the same cardinality; this cardinality is then called the *dependence* of S. The classic example of this phenomenon is

Example 10.3.3 (Linear Dependence)**.** Let V be a vector space over a field k. Then the map $\langle\cdot\rangle : 2^V \to 2^V$ taking a subset $X \subset V$ to its linear span $\langle X \rangle$ is a dependence relation on V, namely the relation of *linear dependence*, often written LD. In this case, the fundamental set is $\{0\}$ and the dependence of (V, LD) is exactly $\dim_k V$.

Lemma 10.3.4. Let $(S, \mathscr{D})$ be a set with a dependence relation. Then

(a) if $X, Y \subset S$ are subsets, then $X \subset \mathscr{D}Y \Rightarrow \mathscr{D}X \subset \mathscr{D}Y$,
(b) if $X \subset S$ is independent and $y \in S \smallsetminus \mathscr{D}X$, then $X \cup \{y\}$ is independent,
(c) if $X \subset S$ is any subset, then the following are equivalent:

[4] Usually, matroids are defined on finite sets because duality theory is an essential feature of finite matroids that the above set of axioms do not provide in the infinite case. A recent workaround has been found by Bruhn et al. ([17]), which replaces axiom (d) by the axiom that for any independent set X and any set Y, the collection $\mathscr{A}$ of independent $Z \subset S$ such that $X \subset Z \subset X \cup Y$ has a maximal element. As the reader can verify, with this replacement, the theory below proceeds with minimal changes–the only results below which essentially use axiom (d) are Lemma 10.3.4(d) and Proposition/Definition 10.3.7(b) in the infinite case; notably, Theorem 10.3.5 goes through, with the first line in the proof even easier. However, since the only matroids we will come across in this course satisfy the above axioms (and we will hardly have any direct use for duality of infinite matroids), we will restrict ourselves to looking at these only.

(1) X is a basis,
(2) X is a minimal spanning set,
(3) X is a maximal independent set, and

(d) if (X_α) is a totally ordered collection of independent subsets, then $\bigcup_\alpha X_\alpha$ is also independent.

Proof.

(a) We have $X \subset \mathscr{D}Y \Rightarrow \mathscr{D}X \subset \mathscr{D}^2 Y = \mathscr{D}Y$.

(b) Let $X' := X \cup \{y\}$. We have to show that for all $x \in X'$ that $x \notin \mathscr{D}(X' \smallsetminus \{x\})$. This is clear if $x = y$ by hypothesis. If $x \in X \cap \mathscr{D}(X' \smallsetminus \{x\})$, then $x \in \mathscr{D}((X \smallsetminus \{x\}) \cup \{y\}) \smallsetminus \mathscr{D}(X \smallsetminus \{x\})$ implies by exchange that $y \in \mathscr{D}X$, again contrary to hypothesis.

(c) For (1) $\Rightarrow$ (2), let X be a basis, so it is certainly spanning; if there were a proper spanning subset $X' \subsetneq X$, then picking an $x \in X \smallsetminus X'$ would give $x \in S = \mathscr{D}(X') \subset \mathscr{D}(X \smallsetminus \{x\})$, contradicting the independence of X. For (2) $\Rightarrow$ (1), suppose that X is a minimal spanning set and that for some $x \in X$ we have $x \in \mathscr{D}(X \smallsetminus \{x\})$. Then $X \subset \mathscr{D}(X \smallsetminus \{x\})$ implies by (a) that $S = \mathscr{D}X \subset \mathscr{D}(X \smallsetminus \{x\})$, so that $X \smallsetminus \{x\}$ is a proper subset that is also spanning, which is a contradiction. To show (1) $\Rightarrow$ (3), let X be a basis, so it is certainly independent; if there were a proper independent superset $X' \supsetneq X$, then picking an $x \in X' \smallsetminus X$ would show $x \in S = \mathscr{D}(X) \subset \mathscr{D}(X' \smallsetminus \{x\})$, contradicting the independence of X'. For (3) $\Rightarrow$ (1), suppose that X is a maximal independent set. If there is a $y \in S \smallsetminus \mathscr{D}X$, then by (b), $X \cup \{y\} \supsetneq X$ is still independent, which is a contradiction.

(d) Let $X := \bigcup_\alpha X_\alpha$. If there is an $x \in X$ such that $x \in \mathscr{D}(X \smallsetminus \{x\})$, then, since $\mathscr{D}$ is finitary, there is a finite subset $X' \subset X \smallsetminus \{x\}$ such that $x \in \mathscr{D}X'$. By the total ordering, there is an α with $X' \cup \{x\} \subset X_\alpha$, and then $x \in \mathscr{D}X' \subset \mathscr{D}(X_\alpha \smallsetminus \{x\})$ contradicts the independence of X_α.

■

Theorem 10.3.5 (MacLane-Steinitz Exchange)**.** Let $(S, \mathscr{D})$ be a set with a dependence relation. If $X, Y \subset S$ are subsets with X independent and Y spanning, then X can be completed to a basis by borrowing elements from Y: there is a subset $Y' \subset Y$ such that $X \cap Y' = \emptyset$ and $X \cup Y'$ is a basis.

Proof. Let $\mathscr{A}$ be the collection of independent $Z \subset S$ such that $X \subset Z \subset X \cup Y$; then $\mathscr{A}$ is nonempty because $X \in \mathscr{A}$. By Lemma 10.3.4(d) and Zorn's Lemma, this has a maximal element Z. We claim that Z is a basis; indeed, it is independent since $Z \in \mathscr{A}$. If there is a $y \in Y \smallsetminus \mathscr{D}Z$, then by Lemma 10.3.4(b) we have $Z \subsetneq Z \cup \{y\} \subset Y$ with $Z \cup \{y\}$ still independent, a contradiction to maximality. Therefore, $Y \subset \mathscr{D}Z$ so by Lemma 10.3.4(a) we have $S = \mathscr{D}Y \subset \mathscr{D}Z$; therefore, Z is spanning as well. ■

Corollary 10.3.6. Let $(S, \mathscr{D})$ be a set with a dependence relation.

(a) Every independent subset of S can be completed to a basis.
(b) Every spanning subset of S contains a basis.
(c) In particular, S admits a basis.

Proof.

(a) Apply Theorem 10.3.5 with X the independent subset and $Y = S$.
(b) Apply Theorem 10.3.5 with $X = \emptyset$ and Y the spanning subset.
(c) Apply (a) to $X = \emptyset$ or (b) to $Y = S$.

■

Proposition/Definition 10.3.7. Let $(S, \mathscr{D})$ be a set with a dependence relation.

(a) If $X, Y \subset S$ are subsets with X independent and Y a finite spanning set , then $|X| \leq |Y|$. In particular, any independent subset in a set with finite dependency is finite.

(b) Any two bases of S have the same cardinality.

The *dependency* of $(S, \mathscr{D})$ is the cardinality of any basis and is denoted $\operatorname{dep} S$.

Proof.

(a) We will show: if $X, Y \subset S$ are subsets with X independent and Y a finite spanning set, then $|X| \leq |Y|$ and there is a $Y' \subset Y$ of size $|Y'| \leq |Y| - |X|$ such that $X \cap Y' = \emptyset$ and $X \cup Y'$ is a basis. First suppose that $|X|$ itself is finite, and show the statement by induction on $|X|$. When $|X| = 0$, then certainly $|X| \leq |Y|$ and by Corollary 10.3.6(b) there is a basis $Y' \subset Y$. If $|X| = n \geq 1$, say $X = \{x_1, \ldots, x_n\}$, then by applying the inductive hypothesis to $X' := X \smallsetminus \{x_n\}$, we conclude that $n-1 \leq |Y|$ and there is a subset $Y_0' \subset Y$ disjoint from X' of size $|Y_0'| \leq |Y| - n + 1$ such that $X' \cup Y_0'$ is a basis. If $x_n \in Y_0'$, then taking $Y' := Y_0' \smallsetminus \{x_n\}$ suffices; else assume that $x_n \notin Y_0'$. In this case, the set $X \cup Y_0'$ is spanning but not independent, since $x_n \in S = \mathscr{D}(X' \cup Y_0') = \mathscr{D}((X \cup Y_0') \smallsetminus \{x_n\})$ where $X' \cup Y_0' = (X \cup Y_0') \smallsetminus \{x_n\}$ because $x_n \notin Y_0'$. Since X is independent and $X \cup Y_0'$ spanning, by Theorem 10.3.5, there is a $Y' \subset Y_0'$ disjoint from X such that $X \cup Y'$ is a basis, and necessarily we must have $Y' \subsetneq Y_0'$. This shows $0 \leq |Y'| < |Y_0'| \leq |Y| - n + 1 \Rightarrow n \leq |Y|$ and that $|Y'| \leq |Y| - n$. The first part of the argument then shows that the assumption that $|X|$ is finite always holds: if $|X|$ were infinite, then we may apply the above argument to any subset $X' \subset X$ of size greater than $|Y|$ to obtain a contradiction.

(b) This follows immediately from (a) if S has finite dependency, so suppose now that S does not have infinite dependency; then no basis of S can be finite. Let X and Y be bases of S. For each $y \in Y$, we have $y \in S = \mathscr{D}X = \bigcup_{\substack{X' \subset X \\ |X'| < \infty}} \mathscr{D}X'$, so there is a finite $X_y \subset X$ such that $y \in \mathscr{D}X_y$. Then $Y \subset \mathscr{D}(\bigcup_{y \in Y} X_y)$. If $x \in X \smallsetminus \bigcup_{y \in Y} X_y$, then $x \in S = \mathscr{D}Y \subset \mathscr{D}(\bigcup_y X_y) \subset \mathscr{D}(X \smallsetminus \{x\})$ contradicts the independence of X; therefore, $X = \bigcup_{y \in Y} X_y$. It follows that

$$|X| = \left| \bigcup_{y \in Y} X_y \right| \leq \left| \coprod_{y \in Y} X_y \right| \leq |Y \times \mathbb{N}| = |Y|$$

where the last uses that Y is infinite. By symmetry, of course, $|Y| \leq |X|$ as well, so we are done by the Cantor-Schröder-Bernstein Theorem.

■

10.4 Trace, Norm, and Discriminant

Definition 10.4.1. Let $R \subset S$ be a finite extension of rings such that S is a finitely generated free R-module. Given an element $\alpha \in S$, define its *trace* (resp. *norm*), denoted $\mathrm{Tr}_R^S(\alpha)$ (resp. $\mathrm{N}_R^S(\alpha)$) to be the trace (resp. determinant) of the R-module endomorphism of S given by multiplication by α.

Example 10.4.2. Finite field extensions K/k, or more generally finite-dimensional algebras over fields, e.g. étale algebras, and rings of integers $\mathbb{Z} \subset \mathcal{O}_K$ are primary examples (see Example 10.4.8). For instance, for $\mathbb{R} \subset \mathbb{C}$ and $z \in \mathbb{C}$ we have $\mathrm{Tr}_{\mathbb{R}}^{\mathbb{C}}(z) = z + \overline{z} = 2\operatorname{Re} z$ and $\mathrm{N}_{\mathbb{R}}^{\mathbb{C}}(z) = z\overline{z} = |z|^2$.

Observation 10.4.3. Let $R \subset S$ be a ring extension such that S is a finitely generated free R-module of rank $n \geq 1$.

(a) For any $\alpha, \beta \in S$ and $\lambda, \mu \in R$ we have

$$\begin{aligned} \mathrm{Tr}_R^S(\lambda\alpha + \mu\beta) &= \lambda \mathrm{Tr}_R^S(\alpha) + \mu \mathrm{Tr}_R^S(\beta), \\ \mathrm{N}_R^S(\alpha\beta) &= \mathrm{N}_R^S(\alpha)\,\mathrm{N}_R^S(\beta), \\ \mathrm{Tr}_R^S(\lambda) &= n\lambda, \text{ and} \\ \mathrm{N}_R^S(\lambda) &= \lambda^n. \end{aligned}$$

(b) (Base Change) Suppose that R is an A-algebra for some ring A. Then if T is any other A-algebra, then the ring extension $R \otimes_A T \subset S \otimes_A T$ still satisfies the above condition, and we have for any $\alpha \in S$ that

$$\mathrm{Tr}_{R\otimes_A T}^{S\otimes_A T}(\alpha \otimes 1) = \mathrm{Tr}_R^S(\alpha) \otimes 1 \text{ and } \mathrm{N}_{R\otimes_A T}^{S\otimes_A T}(\alpha \otimes 1) = \mathrm{N}_R^S(\alpha) \otimes 1.$$

(c) (Transitivity) Let $S \subset T$ be a further ring extension so that T is a finitely generated S-module. Then T is also a finitely generated R-module, and we have further for any $\alpha \in T$ that

$$\mathrm{Tr}_R^T(\alpha) = \mathrm{Tr}_R^S \mathrm{Tr}_S^T(\alpha) \text{ and } \mathrm{N}_R^T(\alpha) = \mathrm{N}_R^S \mathrm{N}_S^T(\alpha).$$

This last is a consequence of the following lemma about block determinants:

Lemma 10.4.4. Let R be any ring, $n \geq 1$, and $S \subset \operatorname{Mat}_n R$ a (commutative, unitary) subring of the $n \times n$ matrix ring over R. For any $m \geq 1$ and matrix $M \in \operatorname{Mat}_m S \subset \operatorname{Mat}_{mn} R$, we have $\det_R^{mn} M = \det_R^n \det_S^m M$.

Proof. We induct on m, with $m = 1$ being clear. Hence assume $m \geq 2$, and write M as

$$M = \begin{bmatrix} A & b \\ c & d \end{bmatrix}$$

where A, b, c, d have dimensions $n(m-1) \times n(m-1)$, and $n(m-1) \times n$, and $n \times n(m-1)$ and $n \times n$ respectively. Since S is commutative, we have that $c \cdot dI_{m-1}^S = dc$, and similarly $A \cdot dI_{m-1}^S = dA$. Therefore,

$$\begin{bmatrix} A & b \\ c & d \end{bmatrix} \begin{bmatrix} dI_{m-1}^S & 0 \\ -c & I_1^S \end{bmatrix} = \begin{bmatrix} dA - bc & b \\ 0 & d \end{bmatrix},$$

so that taking $\det_S$ gives $\det_S M \cdot d^{m-1} = \det_S(dA - bc) \cdot d$ and hence taking $\det_R$ gives

$$(\det_R \det_S M)(\det_R d)^{m-1} = (\det_R \det_S(dA - bC))(\det_R d) = (\det_R(dA - bc))(\det_R d).$$

On the other hand, taking $\det_R = \det_R^{mn}$ directly gives

$$(\det_R M)(\det_R d)^{m-1} = (\det_R(dA - bc))(\det_R d).$$

Putting these together gives us

$$(\det_R \det_S M - \det_R M)(\det_R d)^{m-1} = 0.$$

If $\det_R d$ is not a zero divisor in R, we are done; we can now either reduce to this case by working in the "universal case" of polynomial rings over $\mathbb{Z}$, or replace our base ring R by $R[x]$ and use $d_x := xI_n^R + d$ instead. Then $\det_R d_x$ is a monic polynomial of degree n and the above holds as a polynomial identity with M_x replacing M; in a polynomial ring, a monic polynomial is never a zero divisor, and so we conclude that other factor is 0, and now specialize to $x = 0$. ■

Theorem 10.4.5. Let L/K be a finite field extension and let $\overline{K}$ be an algebraic closure of K. Let $\Sigma := \operatorname{Hom}_K(L, \overline{K})$.

(a) For all $\alpha \in L$ we have

$$\operatorname{Tr}_K^L(\alpha) = [L:K]_i \sum_{\sigma\in\Sigma} \sigma\alpha \text{ and } \operatorname{N}_K^L(\alpha) = \left(\prod_{\sigma\in\Sigma} \sigma\alpha\right)^{[L:K]_i}.$$

(b) Given a $0 \neq \alpha \in L$, let $d := [K(\alpha) : K]$ and let its minimal polynomial be $\mu_\alpha(X) = X^d + a_1X^{d-1} + \cdots + a_d = \prod_{i=1}^d (X - \alpha_i)$, where the last is the factorization in $\overline{K}[X]$. If $n := [L : K]$ and $e = [L : K(\alpha)]$, then

$$\operatorname{Tr}_K^L(\alpha) = \sum_{i=1}^d e\alpha_i = -ea_1 \text{ and } \operatorname{N}_K^L(\alpha) = \prod_{i=1}^d \alpha_i^e = (-1)^n a_d^e.$$

Proof. This belongs to elementary field theory; see [15, Propositions 8.6, 8.12]. ■

The trace map $\operatorname{Tr}_R^S : S \to R$ is an R-linear map; since S is a ring, we get a bilinear pairing on S given by $\langle x, y\rangle \mapsto \operatorname{Tr}_R^S(xy)$ called the *trace pairing*. This gives us an R-linear map $S \to S^*$ (where S^* is its dual as an R-module, i.e. $\operatorname{Hom}_R(S, R)$) given by $x \mapsto \operatorname{Tr}_R^S(x\cdot)$.

Definition 10.4.6. Given an ordered free basis $s := (s_1, \ldots, s_n)$ of S over R, define the *discriminant* $D(s)$ to be the determinant of the linear map $S \to S^*$ with respect to the bases s and s^*, i.e. in other words,

$$D(s) := \det\bigl[\operatorname{Tr}_R^S(s_is_j)\bigr]_{i,j=1}^n.$$

As usual for bilinear pairings, choosing a different basis s' changes $D(s)$ by the square of a unit (namely, the determinant of the change of basis matrix), and so in general, we get a well-defined element $D_{S/R} \in R/(R^\times)^2$ depending only on S, which we call the relative discriminant of S over R. When $R = \mathbb{Z}$, we have $(\mathbb{Z}^\times)^2 = \{1\}$, and so this gives an honest element of $\mathbb{Z}$. In general, we get a well-defined ideal $D_{S/R} \subset R$ called the discriminant ideal.

Now suppose that R is a domain, $K = \operatorname{Frac} R$ and L/K a finite extension with $\operatorname{char} K \nmid [L : K]$. In this case, the trace map $\operatorname{Tr}_K^L : L \to K$ is not identically zero (since $\operatorname{Tr}_K^L(1) = [L : K] \neq 0$) and hence the trace pairing is nondegenerate (since $\operatorname{Tr}_K^L(x \cdot x^{-1}) \neq 0$ for every nonzero x). In particular, we get an isomorphism $L \to L^* = \operatorname{Hom}_K(L, K)$ given by $x \mapsto \operatorname{Tr}_K^L(x\cdot)$.

Definition 10.4.7. Given any R-submodule $M \subset L$, we define its *trace dual* to be

$$M^* := \{x \in L : \operatorname{Tr}_K^L(xy) \in R \text{ for all } y \in M\}.$$

This is another R-submodule of L. If M is free with basis $s_1, \dots, s_n$, then M^* is free with basis $s_1^*, \dots, s_n^*$, where s_i^* are such that $s_i^* s_j = \delta_{ij}$.

Example 10.4.8. Let K be a number field. We'll show that $\mathcal{O}_K := \mathrm{Cl}_K(\mathbb{Z})$ is a free $\mathbb{Z}$-module of rank $n := [K : \mathbb{Q}]$. Indeed, the above conditions are automatically satisfied. The key point is that if $\alpha \in \mathcal{O}_K$, then $\mathrm{Tr}_{\mathbb{Q}}^{K}(\alpha) \in \mathbb{Z}$; this follows immediately from 3.1.10 and 10.4.5. Let $v_1, \dots, v_n \in K$ be a $\mathbb{Q}$-basis lying in $\mathcal{O}_K$ (this can always be achieved by rescaling) and let $M := \sum_{i=1}^{n} \mathbb{Z} v_i$. Then it suffices to observe that $M \subset \mathcal{O}_K \subset M^*$, and we are done by the structure theorem for finitely generated abelian groups. The discriminant $D_K := D_{\mathcal{O}_K/\mathbb{Z}} \in \mathbb{Z}$ is a fundamental invariant of K.

10.5 Derived Functors in Abelian Categories

In this section, we review the generalities of (the naive approach to) derived functors on abelian categories; this is sufficient for our present purposes (to define Tor and Ext), and in the definition of sheaf cohomology.[5] We use cohomological terminology, and the translation into homological language (i.e. left-derived functors, etc.) is left to the reader. In the following, a functor is always covariant.

Definition 10.5.1. Let $\mathcal{A}, \mathcal{B}$ be abelian categories and $F : \mathcal{A} \to \mathcal{B}$ be an additive functor. A (cohomological) *δ-functor extending* F is a triple $(F^\bullet, \iota, \delta)$, where

(a) $F^\bullet = (F^q)_{q \in \mathbb{Z}_{\geq 0}}$ is a sequence of additive functors $F^q : \mathcal{A} \to \mathcal{B}$ indexed by $q \in \mathbb{Z}_{\geq 0}$, and
(b) ι is a natural isomorphism $\iota : F \Rightarrow F^0$,
(c) δ is a natural assignment $\underline{A} \to \delta^\bullet_{\underline{A}} = (\delta^q_{\underline{A}})_{q \in \mathbb{Z}_{\geq 0}}$ to each short exact sequence

$$\underline{A} : 0 \to A' \to A \to A'' \to 0$$

in $\mathcal{A}$, a sequence of morphisms $\delta^q_{\underline{A}} : F^q(A'') \to F^{q+1}(A')$ in $\mathcal{B}$ indexed by $q \in \mathbb{Z}_{\geq 0}$ such that the sequence

$$\cdots \to F^q(A') \to F^q(A) \to F^q(A'') \xrightarrow{\delta^q_{\underline{A}}} F^{q+1}(A') \to \cdots \qquad (*)$$

(with $F^{-1} := 0$) is a cochain complex.[6]

If for each short exact sequence $\underline{A}$, the sequence $(*)$ is exact, we say further that this δ-functor is *exact.*

A δ-functor is often denoted simply by $F^\bullet : \mathcal{A} \to \mathcal{B}$, with ι and δ implicit (in writing δ, the sub- and superscripts are often dropped too). The morphisms $\delta^\bullet$ are called the *connecting homomorphisms.* Further, ι is often used to identify F and F^0; we will sometimes use this convention to make life simpler.[7]

Now, let $F, G : \mathcal{A} \to \mathcal{B}$ be additive functors between abelian categories, $F^\bullet, G^\bullet : \mathcal{A} \to \mathcal{B}$ be δ-functors extending F and G respectively, and $\eta : F \Rightarrow G$ be a natural transformation. A *δ-transformation from $F^\bullet$ to $G^\bullet$ extending* η is a sequence $\eta^\bullet = (\eta^q)_{q \in \mathbb{Z}_{\geq 0}}$ of natural transformations $\eta^q : F^q \Rightarrow G^q$ such that $\iota_{G^\bullet} \circ \eta = \eta^0 \circ \iota_{F^\bullet}$ as natural transformations $F \Rightarrow G^0$, and $\eta^\bullet$ commutes with connecting morphisms, i.e., for each short exact sequence $\underline{A}$ in $\mathcal{A}$ and $q \in \mathbb{Z}_{\geq 0}$, the following diagram commutes:

$$\begin{tikzcd}
F^q(A'') \arrow[r, "\delta^q"] \arrow[d, "\eta^q_{A''}"] & F^{q+1}(A') \arrow[d, "\eta^{q+1}_{A'}"] \\
G^q(A'') \arrow[r, "\delta^q"] & G^{q+1}(A').
\end{tikzcd}$$

It is clear what the notion of a composition of δ-transformations should mean. The δ-transformation $\eta^\bullet$ is said to be a *δ-isomorphism* if there is a natural transformation $\theta : G \Rightarrow F$ and a δ-transformation $\theta^\bullet$ extending it such that $\theta^\bullet \circ \eta^\bullet = 1_{F^\bullet}$ and $\eta^\bullet \circ \theta^\bullet = 1_{G^\bullet}$.

Finally, suppose $F : \mathcal{A} \to \mathcal{B}$ is an additive functor and $F^\bullet : \mathcal{A} \to \mathcal{B}$ a δ-functor extending F. The δ-functor $F^\bullet$ is said to be *universal* if it is exact, and if $G : \mathcal{A} \to \mathcal{B}$ is

[5] More sophisticated treatments require the development of the theory of derived categories, which we wish to avoid.

[6] Naturality means that given a morphism $\underline{f} = (f', f, f'') : \underline{A} \to \underline{B}$ of short exact sequences in $\mathcal{A}$ and for each $q \geq 0$, we have $F^{q+1}(f') \circ \delta^q_{\underline{A}} = \delta^q_{\underline{B}} \circ F^q(f'')$ as maps $F^q(A'') \to F^{q+1}(B')$ in $\mathcal{B}$.

[7] Sometimes it *is* important to keep this distinction and the natural isomorphism ι in mind; in this case, we'll point it out. [TODO]

any other additive functor, $G^\bullet : \mathcal{A} \to \mathcal{B}$ a δ-functor extending G and $\eta : F \Rightarrow G$ a natural transformation, there is a unique δ-transformation $\eta^\bullet : F^\bullet \to G^\bullet$ extending η.

It follows that there is at most one universal δ-functor extending a given functor $F : \mathcal{A} \to \mathcal{B}$, up to unique δ-isomorphism extending the identity transformation $1_F : F \Rightarrow F$; in fact, any δ-transformation extending 1_F between universal δ-functors extending a given functor F must be a δ-isomorphism. A/"the" universal δ-functor extending $F : \mathcal{A} \to \mathcal{B}$ is called a/"the" *right derived functor* of F, and denoted $\mathsf{R}^\bullet F : \mathcal{A} \to \mathcal{B}$. Note that if F admits a right derived functor, then F is left-exact.

Remark 10.5.2. If $\mathsf{R}^\bullet F$ exists, then F is exact iff $\mathsf{R}^q F = 0$ for each $q \geq 1$ iff $\mathsf{R}^1 F = 0$.

Here's a simple criterion to check the universality of a δ-functor:

Definition 10.5.3. Let $F : \mathcal{A} \to \mathcal{B}$ be an additive functor between abelian categories.

- Given an $A \in \mathrm{Ob}(\mathcal{A})$, an *$F$-effacement* of A is a monomorphism $i : A \to I$ such that $F(i) = 0$.
- The functor F is said to be *effaceable* if every $A \in \mathrm{Ob}(\mathcal{A})$ admits an F-effacement.

If F is effaceable, then F-effacements can be constructed functorially:

Lemma 10.5.4. Let $F : \mathcal{A} \to \mathcal{B}$ be an effaceable functor, and let $f : A \to A'$ be a morphism in $\mathcal{A}$. If $i : A \to I$ is any F-effacement, then there is an F-effacement $i' : A' \to I'$ and a morphism $\tilde{f} : I \to I'$ such that the following diagram commutes:

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "i"] & A' \arrow[d, "i'"] \\
I \arrow[r, "\tilde{f}"] & I'.
\end{tikzcd}$$

Proof. Let $j : I \oplus A' \hookrightarrow J$ be an F-effacement, and let $I' := \mathrm{coker}(A \xrightarrow{j \circ (i,f)} J)$. Let $i' : A' \to I'$ be the negative of the composite $A' \xrightarrow{\iota_{A'}} I \oplus A' \xrightarrow{j} J \twoheadrightarrow I'$, and $\tilde{f} : I \to I'$ be the composite $I \xrightarrow{\iota_I} I \oplus A' \xrightarrow{j} J \twoheadrightarrow I'$. ■

Theorem 10.5.5. If $F^\bullet : \mathcal{A} \to \mathcal{B}$ is an exact δ-functor such that F^q is effaceable for each $q \geq 1$, then $F^\bullet$ is universal, and hence the right derived functor $\mathsf{R}^\bullet F^0$.

Proof. Given a δ-functor $G^\bullet$ and a natural transformation $\eta^0 : F^0 \Rightarrow G^0$, we recursively construct natural transformations $\eta^q : F^q \Rightarrow G^q$ that commute with the connecting homomorphisms. The base $q = 0$ is given; suppose $q \geq 1$. By effaceability, there is a monomorphism $i : A \to I$ with $F^q(i) = 0$. Consider the short exact sequence $0 \to A \xrightarrow{i} I \to I/A \to 0$ and the corresponding long sequences to get

$$\begin{tikzcd}
\cdots \arrow[r] & F^{q-1}I \arrow[r] \arrow[d, "\eta^{q-1}I"] & F^{q-1}(I/A) \arrow[r, "\delta_F^{q-1}"] \arrow[d, "\eta^{q-1}(I/A)"] & F^qA \arrow[r] \arrow[d, dashed, "\exists!"] & 0 \\
\cdots \arrow[r] & G^{q-1}I \arrow[r] & G^{q-1}(I/A) \arrow[r, "\delta_G^{q-1}"] & G^qA \arrow[r] & \cdots
\end{tikzcd}$$

The exactness of the top row proves the unique such a δ-transformation if one exists. We use the above to define the map $\eta^q A : F^q A \to G^q A$.

(a) This map is independent of the choice of effacement. Suppose that $i : A \to I$ and $i' : A \to I'$ are both F^q-effacements. Then so is $(i, i') : A \to I \oplus I'$ because $(i, i') = \iota_I \circ i + \iota_{I'} \circ i'$ and F^q is additive. Consider the morphism of SES's given by

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "{(i,i')}"] \arrow[d, equal] & I \oplus I' \arrow[r] \arrow[d, "\pi_I"] & (I \oplus I')/A \arrow[r] \arrow[d, dashed, "\exists"] & 0 \\
0 \arrow[r] & A \arrow[r, "i"] & I \arrow[r] & I/A \arrow[r] & 0
\end{tikzcd}$$

Using this, the naturality of LES's for $F^\bullet$ and $G^\bullet$ and the naturality of η^{q-1}, it follows that the map $F^q A \to G^q A$ obtained in this way is the same for the effacement $i : A \to I$ and $(i, i') : A \to I \oplus I'$.

(b) The map η^q is a natural transformation. Suppose $f : A \to A'$ is a morphism. Then pick any effacements $i : A \to I$ and $i' : A' \to I'$ and morphism $\tilde{f} : I \to I'$ as in 10.5.4, and consider the morphism of SES's given by

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "i"] \arrow[d, "f"] & I \arrow[r] \arrow[d, "\tilde{f}"] & I/A \arrow[r] \arrow[d, dashed, "\exists"] & 0 \\
0 \arrow[r] & A' \arrow[r, "i'"] & I' \arrow[r] & I'/A' \arrow[r] & 0.
\end{tikzcd}$$

Using this, the naturality of LES's for $F^\bullet$ and $G^\bullet$ and the naturality of η^{q-1}, we conclude that η^q is a natural transformation.

(c) Finally, η^q commutes with δ^{q-1}, i.e. given an SES $0 \to A' \to A \to A'' \to 0$ in $\mathcal{A}$, the diagram

$$\begin{tikzcd}
F^{q-1}A'' \arrow[r, "\delta_F^{q-1}"] \arrow[d, "\eta^{q-1}A''"] & F^q A' \arrow[d, "\eta^q A'"] \\
G^{q-1}A'' \arrow[r, "\delta_G^{q-1}"] & G^q A'
\end{tikzcd}$$

commutes. Indeed, note that if $i : A \to I$ is any F-effacement, then the map $A' \to A \xrightarrow{i} I$ is also an F-effacement. Then we get a morphism of SES's given by

$$\begin{tikzcd}
0 \arrow[r] & A' \arrow[r] \arrow[d, equal] & A \arrow[r] \arrow[d, "i"] & A'' \arrow[r] \arrow[d, dashed, "\exists"] & 0 \\
0 \arrow[r] & A' \arrow[r] & I \arrow[r] & I/A' \arrow[r] & 0
\end{tikzcd}$$

Using this, the naturality of LES's for $F^\bullet$ and $G^\bullet$ and the naturality of η^{q-1}, we get the result.

■

One general situation in which right derived functors of left-exact functors exists is when category $\mathcal{A}$ has enough injectives (so that every object has an injective resolution). This is a standard consequence of

Lemma 10.5.6 (Fundamental Lemma of Homological Algebra)**.** In an abelian category $\mathcal{A}$, if $T[0] \to J^\bullet$ is any resolution and $A[0] \to I^\bullet$ an injective resolution, then any morphism $f : T \to A$ lifts to a morphism $f^\bullet : J^\bullet \to I^\bullet$ of complexes that extends f, and this extension is unique up to chain homotopy.

Proof. Augment the complexes J and I so that $J^{-1} := T$ and $I^{-1} := A$. For $n \in \mathbb{Z}_{\geq 0}$, we recursively construct $f^n : J^n \to I^n$ such that $f^n \partial_J^{n-1} = \partial_I^{n-1} f^{n-1}$, with $f^{-1} := f$. For this, use 8.1.9(c) to construct an $f^0 : J^0 \to I^0$ extending $T \xrightarrow{f} A \xrightarrow{\partial_I^{-1}} I^0$. Given $n \geq 0$, if we have constructed an f^n, then the composite $\partial_I^n f^n : J^n \to I^{n+1}$ vanishes on $\operatorname{Im} \partial_J^{n-1}$ and hence descends to a map $\operatorname{Im} \partial_J^n \cong J^n / \operatorname{Im} \partial_J^{n-1} \to I^{n+1}$, which then extends to a morphism $f^{n+1} : J^{n+1} \to I^{n+1}$ by the injectivity of I^{n+1} and 8.1.9(c).

For the second part, it suffices to show $f = 0$ and $f^\bullet$ any lift, then there are morphisms $H^n : J^n \to I^{n-1}$ such that $\partial_I^{n-2} H^{n-1} + H^n \partial_J^{n-1} = f^{n-1}$ for $n \geq 0$, where $H^{-1} := 0$. We produce these H^n recursively, with $H^0 := 0$. Given $n \geq 0$, if we have constructed an H^n, then the morphism $f^n - \partial_I^{n-1} H^n : J^n \to I^n$ vanishes on $\operatorname{Im} \partial_J^{n-1}$ and hence descends to a map $\operatorname{Im} \partial_J^n \cong J^n / \operatorname{Im} \partial_J^{n-1} \to I^n$, which then again extends to a morphism $H^{n+1} : J^{n+1} \to I^n$ by the injectivity of I^n and 8.1.9(c). ■

Remark 10.5.7. When $\mathcal{A} = R\text{-}\mathsf{Mod}$ for some ring R, then, given that we have proved the existence of lifts, the uniqueness of lifts up to chain homotopy can also be proven as follows. Consider the complex I given by

$$0 \to R \xrightarrow{1} R \to 0,$$

with R's in degrees -1 and 0. Given any complex $K^\bullet$, the tensor product $I \otimes_R K$ is the complex with $(I \otimes_R K)^n = K^n \oplus K^{n+1}$ and differential $\partial^n : K^n \oplus K^{n+1} \to K^{n+1} \oplus K^{n+2}$ given by

$$\partial^n = \begin{bmatrix} \partial_K^n & (-1)^n \\ 0 & \partial_K^{n+1} \end{bmatrix}$$

for $n \geq -1$. Given a morphism $f = f^\bullet : K^\bullet \to L^\bullet$ of complexes, a contracting homotopy H for f is the same thing as a morphism of complexes $F : I \otimes_R K \to L$ with $F^{-1} = 0$ and translation $F^n = [f^n, (-1)^n H^{n+1}]$. Therefore, the existence of a chain homotopy as above follows from the existence result as well.

Corollary 10.5.8. Let $F : \mathcal{A} \to \mathcal{B}$ be a left-exact additive functor of abelian categories. Suppose that $\mathcal{A}$ has enough injectives. Then the right derived functor $\mathsf{R}^\bullet F$ of F exists.

Proof. For each object A, pick an injective resolution $A[0] \to I^\bullet$ of A, apply F to this resolution to get the complex $F(I^\bullet)$, and define $F^q(A)$ to be the q^{th}-cohomology object of the complex $F(I^\bullet)$, namely

$$F^q(A) := \mathrm{H}^q(F(I^\bullet)) := \ker(FI^q \to FI^{q+1}) / \operatorname{im}(FI^{q-1} \to FI^q).$$

Then 10.5.6 guarantees that the isomorphism type of $F^q(A)$ is independent of the choice of resolution, and that the construction F^q is functorial. Left-exactness of F implies that for each A, the map $F(A) \to F(I^0)$ induces an isomorphism $\iota_A : F(A) \to F^0(A)$, and naturality of ι_A in A follows again from 10.5.6. Finally, δ can be constructed by taking simultaneous resolutions and taking the long exact cohomology sequence corresponding to a short exact sequence of resolutions, with naturality following again from 10.5.6 and the naturality of long exact sequences. Finally, each F^q for $q \geq 1$ according to this definition is effaceable because an injective object is its own resolution, and we have assumed that $\mathcal{A}$ has enough injectives; therefore, universality follows from 10.5.5. ■

Example 10.5.9. Let $\mathcal{A}$ be an abelian category with enough injectives. Given a fixed object $M \in \operatorname{Ob}(\mathcal{A})$, the functor $\operatorname{Hom}_{\mathcal{A}}(M, -) : \mathcal{A} \to \mathsf{Ab}$ is left exact. The (components of the) right derived functor of this functor are called the Ext functors $\operatorname{Ext}^q_{\mathcal{A}}(M, -) : \mathcal{A} \to \mathsf{Ab}$ for $q \geq 0$, i.e. $\operatorname{Ext}^\bullet_{\mathcal{A}}(M, -) = \mathsf{R}^\bullet \operatorname{Hom}_{\mathcal{A}}(M, -)$. The reason for this name is that $\operatorname{Ext}^1_{\mathcal{A}}(M, N)$ classifies the extensions of M by N: given an extension $0 \to N \to E \to M \to 0$, the class in $\operatorname{Ext}^1_{\mathcal{A}}(M, N)$ is given by taking the image of $1_M \in \operatorname{Hom}_{\mathcal{A}}(M, M)$ under δ^0; on the other hand, given an element of $\operatorname{Ext}^1_{\mathcal{A}}(M, N)$, pick an SES $0 \to N \to I \to I/N \to 0$ with I injective to lift it to an element of $\varphi \in \operatorname{Hom}_{\mathcal{A}}(M, I/N)$, and then form the extension E as the pullback of $I \to I/N$ and $\varphi : M \to I/N$.

Unfortunately, this method is not very useful in practice because injective resolutions, even when they exist, are hard to write down by hand. To compute these derived functors in practice, one usually uses *acyclic resolutions*:

Definition 10.5.10. Let $F : \mathcal{A} \to \mathcal{B}$ be a left exact functor and suppose $\mathcal{A}$ has enough injectives, so that the right derived functor $\mathsf{R}^\bullet F$ exists.

(a) An object A of $\mathcal{A}$ is said to be *F-acyclic* if $\mathsf{R}^q F(A) = 0$ for all $q \geq 1$.
(b) A resolution $A[0] \to J^\bullet$ of A is an *F-acyclic resolution* if all the J^q for $q \geq 0$ are F-acyclic.

Lemma 10.5.11. In the set-up of the previous definition, if $A[0] \to J^\bullet$ is an F-acyclic resolution of an object A, then the right derived functors of F can be computed by taking the cohomology of $F(J^\bullet)$, i.e. for each $q \geq 0$, there is an isomorphism

$$\mathrm{H}^q(F(J^\bullet)) \xrightarrow{\sim} \mathsf{R}^q F(A).$$

Proof. Induct on q; the case $q = 0$ follows from the left exactness of F and the exact sequence $0 \to A \to J^0 \to J^1$. Next, to show $q = 1$, use $0 \to A \to J^0 \to J^0/A \to 0$ and $\mathsf{R}^1 F J^0 = 0$ to get

$$\operatorname{coker}\left(\mathsf{R}^0 F J^0 \to \mathsf{R}^0 F(J^0/A)\right) \xrightarrow{\sim} \mathsf{R}^1 F A,$$

and $0 \to J^0/A \to J^1 \to J^2$ to get

$$\mathsf{R}^0 F(J^0/A) \xrightarrow{\sim} \ker\left(\mathsf{R}^0 F J^1 \to \mathsf{R}^0 F J^2\right);$$

putting these together, we get $\mathrm{H}^1(F(J^\bullet)) \xrightarrow{\sim} \mathsf{R}^1 F A$. Finally, for $q \geq 2$, use inductively that there is an acyclic resolution $(J^0/A)[0] \to J^{\bullet+1}$ and the exact sequence $0 \to A \to J^0 \to J^0/A \to 0$ to get

$$\mathrm{H}^q(F(J^\bullet)) = \mathrm{H}^{q-1}(F(J^{\bullet+1})) \xrightarrow{\sim} \mathsf{R}^{q-1} F(J^0/A) \xrightarrow{\sim} \mathsf{R}^q F A.$$

■

Therefore, to compute derived functors of a functor F, it remains to identify appropriate F-acyclic objects. This can often be done using:

Lemma 10.5.12 (Acyclic Cohomology)**.** Let $F : \mathcal{A} \to \mathcal{B}$ be a left exact functor between abelian categories and suppose $\mathcal{A}$ has enough injectives. Let $\mathcal{T} \subset \mathrm{Ob}(\mathcal{A})$ be a class of objects in $\mathcal{A}$ such that:

(a) every injective object of $\mathcal{A}$ is in $\mathcal{T}$, and
(b) if $0 \to A' \to A \to A'' \to 0$ is exact and $A', A \in \mathcal{T}$, then $A'' \in \mathcal{T}$, and the resulting sequence $0 \to FA' \to FA \to FA'' \to 0$ is exact.

Then all elements of $\mathcal{T}$ are F-acyclic, so $\mathcal{T}$-resolutions can be used to compute the derived functor $\mathsf{R}^\bullet F$.

Proof. We show by induction on $q \geq 1$ that $\mathsf{R}^q F T = 0$ for all $T \in \mathcal{T}$. For $q = 1$, given a T, take a monomorphism $T \hookrightarrow I$ for injective I and consider the SES $0 \to T \to I \to I/T \to 0$. By the LES and (b), we get that $0 \to \mathsf{R}^1 F T \to \mathsf{R}^1 F I$ is exact, but $\mathsf{R}^1 F I = 0$ since I is injective and hence F-acyclic. For $q \geq 2$, the sequence $\mathsf{R}^{q-1} F(I/T) \to \mathsf{R}^q F T \to \mathsf{R}^q F I$ is exact, but the first term is zero by (a), (b), and induction; the last term is zero since I is F-acyclic as before. ■

10.6 Pathologies, or Counterexamples in Commutative Algebra

Example 10.6.1. A UFD R such that $R[\![X]\!]$ is not a UFD. Consider $S := k[x,y,z] := k[X,Y,Z](X^2+Y^3+Z^7)$, and the localization $R = S_{(x,y,z)}$. By Exercise 1.21(c), S and hence R is a UFD.

Example 10.6.2. A ring R and a prime $\mathfrak{p} \subset R$ such that $\operatorname{ht}\mathfrak{p} + \operatorname{coht}\mathfrak{p} < \dim R$. Consider the ring $R := k[\![X,Y,Z]\!]/(XY, XZ)$. Then $\dim R = 2$. If $\mathfrak{p} = (y,z) \subset R$, then $\mathfrak{p}$ is prime with $\operatorname{ht}\mathfrak{p} = 0$ but $\operatorname{coht}\mathfrak{p} = 1$. Also $R = A[X]$ for DVR A.

Example 10.6.3. A zero-dimensional non-Noetherian ring. Take k to be a field and

$$R = k[\varepsilon_1, \varepsilon_2, \dots] := k[X_1, X_2, \dots]/(X_1^2, X_2^2, \dots).$$

This has a unique prime, namely $(\varepsilon_1, \varepsilon_2, \dots)$ and is hence zero dimensional; the increasing chain $0 \subset (\varepsilon_1) \subset (\varepsilon_1, \varepsilon_2) \subset \cdots$ show that R is non-Noetherian.

Example 10.6.4. A positive finite-dimensional non-Noetherian ring, and a domain in which the Krull intersection theorem fails. Valuation rings of dimension at least two are not Noetherian ([TO CITE]). The Krull dimension of a valuation ring is the height (i.e. number of isolated subgroups) of its value group. A standard example is the valuation ring of the $\mathbb{Z}^2$-valued valuation on $k(x,y)$ with $v(x^n y^m) = (n,m)$. This is also an example of a domain in which the Krull intersection theorem fails.

Example 10.6.5. (Nagata) An infinite-dimensional Noetherian ring. Let $R := k[X_1, X_2, \dots]$ and $m_1, m_2, \dots$ an increasing sequence of positive integers such that $m_{i+1} - m_i > m_i - m_{i-1}$ for all $i \geq 1$. Let $\mathfrak{p}_i := (x_{m_i} + 1, \dots, x_{m_{i+1}})$, and let $S := R \smallsetminus \bigcup_i \mathfrak{p}_i$. Then $S^{-1}R$ is the required example.

Example 10.6.6. A nonzero module with no associated primes. We give two examples of a nonzero ring R such that $\operatorname{Ass}_R(R) = \emptyset$.

(a) Let $R = \mathcal{C}(\mathbb{R}, \mathbb{R})$ be the ring of continuous functions $f : \mathbb{R} \to \mathbb{R}$. If $f \in R$ is a nonzero element, then there are $x \neq y \in \mathbb{R}$ such that $f(x)f(y) \neq 0$. Let $g, h \in R$ be functions such that $g(x) = h(y) = 1$ and $gh = 0$, then $g, h \notin \operatorname{Ann}(f)$ but $gh \in \operatorname{Ann}(f)$; consequently, $\operatorname{Ann}(f)$ is not prime. In particular, $\operatorname{Ass}_R(R) = \emptyset$.

(b) Let R be the ring of Example 10.6.3. Then R has a unique prime ideal, but this prime ideal is not associated to R, since for any nonzero element $f \in R$, only finitely many of the ε_i's (namely a subset of those which appear in f) can be elements of $\operatorname{Ann}_R(f)$.

Example 10.6.7. A separable field extension K/k that is not separably generated. Let $p > 0$ be a prime, $k = \mathbb{F}_p$ be a field let $K = k(X, X^{1/p}, X^{1/p^2}, \dots)$. On the one hand, k is perfect, and hence every extension K/k is separable. On the other hand, $k(X) \hookrightarrow K$ with K algebraic over $k(X)$ implies that $\operatorname{trdeg}_k K = 1$. If $f \in K$ is a separating transcendence basis, then K is separably algebraic over $k(f)$; but there is an $N \geq 1$ such that $f \in k(X^{1/p^N})$ and then $K/k(X^{1/p^N})$ is a nontrivial purely inseparable superextension, which is a contradiction.

Example 10.6.8. ([16, p. 73]) A divisible module that is not injective. Let $R := \mathbb{Z}[X]$ with fraction field $K = \mathbb{Q}(X)$. The R-module $M := K/R$ is divisible (8.1.12(a)), but is not injective. For this, consider the ideal $\mathfrak{a} := (2, X) \subset R$. We produce an R-module morphism $f : \mathfrak{a} \to M$ that cannot be extended to R; indeed, it suffices to take f to be the morphism taking $2 \mapsto [0]$ and $X \mapsto [1/2]$. (Check that this is well-defined!) Suppose there is an extension $\tilde{f} : R \to M$, and pick a lift $p(X) \in K$ of $\tilde{f}(1)$. Then $2p(X), Xp(X) - 1/2 \in \mathbb{Z}[X]$. The first of these says that $p(X)$ does not have a pole at $X = 0$, and so evaluating the second at $X = 0$ tells us that $-1/2 \in \mathbb{Z}$, which is absurd.

Example 10.6.9. A valuation ring R with principal maximal ideal $\mathfrak{m}$ that is not a DVR.

10.7 Exercises

Exercise 10.1. Show that for any finite field $\mathbb{F}_q$, the only group homomorphism $(\mathbb{Q}, +) \to (\mathbb{F}_q, +)$ is the trivial one.

Exercise 10.2. Let R be a ring. If $0 \to M_1 \to M_2 \to \cdots \to M_n \to 0$ is an exact sequence of R-modules, each of finite length, then the lengths of these modules are related by $\sum_{i=1}^{n}(-1)^i \ell_R(M_i) = 0$.

Exercise 10.3. Using the structure theorem for finitely generated abelian groups, determine which of these have finite lengths (as $\mathbb{Z}$-modules). For the ones that do, determine their lengths and multisets of simple factors.

Exercise 10.4. Let $(R, \mathfrak{m}, k)$ be a Noetherian local ring.

(a) Show that for each $i \geq 1$, the quotient $\mathfrak{m}^{i-1}/\mathfrak{m}^i$ is a finite-dimensional vector space over k.

(b) Show that for any $n \geq 0$,

$$\ell_R(R/\mathfrak{m}^n) = \sum_{i=1}^{n} \dim_k(\mathfrak{m}^{i-1}/\mathfrak{m}^i).$$

Exercise 10.5. Show that if k is a field, and $f, g \in k[X, Y]$ are relatively prime, then there are only finitely many primes of $k[X, Y]$ containing both f and g.

Exercise 10.6.

(a) Let S be a set with a dependence relation $\mathscr{D}$ and let $\varphi : T \to S$ be any set map. Show that the map $\varphi^*\mathscr{D} : 2^T \to 2^T$ defined by $(\varphi^*\mathscr{D})(X) = \varphi^{-1}(\mathscr{D}(\varphi(X))$ for any $X \subset T$ is a dependence relation on T. This is called the *pullback of the relation* $\mathscr{D}$ under the map φ. What are the spanning sets of $\varphi^*\mathscr{D}$? What are the independent sets? What is its fundamental set? What can you say about the special situation in which the map φ is injective?

(b) Let V, W be vector spaces and $\varphi : V \to W$ be a linear map. If LD is the linear dependence relation on W, then what is the dependency of the pullback relation $\varphi^*\mathrm{LD}$? What is its fundamental set?

Exercise 10.7. Let $\mathscr{D}$ and $\mathscr{E}$ be two dependence relations on the same set S. Consider the following conditions on S.

(a) For every subset $X \subset S$, we have $\mathscr{E}X \subset \mathscr{D}X$.

(b) For every subset $i_T : T \hookrightarrow S$, each $i_T^*\mathscr{E}$-spanning subset of T is $i_T^*\mathscr{D}$-spanning.

(c) Each $\mathscr{D}$-independent subset is $\mathscr{E}$-independent (and hence $\operatorname{dep}\mathscr{D} \leq \operatorname{dep}\mathscr{E}$).

Show that (a) ⇔ (b) ⇒ (c). Are all the conditions equivalent?

Exercise 10.8. Let $\mathscr{D}$ and $\mathscr{E}$ be two dependence relations on the same set S. Prove or disprove and salvage if possible: if the $\mathscr{D}$-independent subsets and $\mathscr{E}$-independent subsets coincide, then $\mathscr{D} = \mathscr{E}$.

Exercise 10.9. Let $G = (V, E)$ be a graph. Consider the map $\mathrm{Cl} : 2^E \to 2^E$ defined by saying that for any $X \subset E$, the set $\mathrm{Cl}\, X$ is the set edges whose endpoints are connected to each other by a path in X. Check that this defines a dependence relation on E; this is often called the graph closure operator. Explore the properties of this operator. What are spanning (resp. independent) subsets? What is a basis? When does it have finite dependency? What is the dependency of this relation? What is its fundamental set?

Exercise 10.10. Let V be a real vector space. A subset $K \subset V$ is said to be *convex* if for all $x, y \in K$ and $t \in [0,1]$ we have $tx + (1-t)y \in K$. Is the map $\mathrm{Conv} : 2^V \to 2^V$ sending a subset $X \subset V$ to its convex hull $\mathrm{Conv}(X)$, i.e. the intersection of all convex subsets of V containing X, a closure operator? Is it finitary? Does it satisfy MacLane-Steinitz exchange? How far can you generalize the notion of spanning sets, independent sets, bases, etc. for this operation?

Chapter 11

Possible Hints to Selected Exercises

Exercise 1.13(a). First replace the V_i by $U \cap V_i$ to reduce to the case $U = V$. Draw a picture.

Exercise 1.17. For the counterexample, consider the ring $R = \mathcal{C}[0,1]$ of continuous functions $f : [0,1] \to \mathbb{R}$. For more on this, see [18].

Exercise 1.20. For (c) $\Rightarrow$ (b), show that the localization of R at the multiplicative subset generated by all primes in R is a field. For the alternative proof of implication (b) $\Rightarrow$ (a) in Corollary 1.4.5, suppose $\mathfrak{p} \subset R$ is a nonzero prime ideal but $\mathfrak{p} \cap S = \emptyset$. Use (c) and the ACCP hypothesis on R to produce a prime element $\pi \in S^{-1}\mathfrak{p}$ which lies in R and is not divisible by any element in S; then use Corollary 1.1.12(c). For the alternative proof of the key implication (a) $\Rightarrow$ (b) in Corollary 1.4.10, let $\mathfrak{p} \subset R[X]$ be a nonzero prime. If $\mathfrak{p} \cap R \neq (0)$, use Exercise 1.19(b). If $\mathfrak{p} \cap R = (0)$, then $\mathfrak{p}K[X]$ is prime by Corollary 1.1.12, and so contains an irreducible polynomial $f(X)$ in $K[X]$; then consider the primitive part of $f(X)$ and use Gauss's Lemma as in the proof of Corollary 1.4.10 given. See [15, Theorem A.4.5].

Exercise 1.21. We give hints for (b); (c) is similar. Work with the ring

$$S = \mathbb{C}[z, w, x_3, \ldots, x_n] := \mathbb{C}[Z, W, X_3, \ldots, X_n]/(ZW + X_3^2 + \cdots + X_n^2)$$

instead. Show that S is a domain, $z \in S$ is a prime element, and the elements $z, x_3, \ldots, x_n \in S$ are algebraically independent over $\mathbb{C}$ (this can be done by hand here, or using Example 5.2.4), whence $S[z^{-1}] \cong \mathbb{C}[Z, X_3, \ldots, X_n, Z^{-1}]$ is a UFD. Now finish using Corollary 1.4.5. In fact, the result in (b) is true over any field k of characteristic not two; this can be done first by adjoining a $\sqrt{-1}$ if needed and reducing to the above case, and then using "descent" from the field $k[\sqrt{-1}]$ to k. See [19, Theorem 6.2]. This ring (coordinate ring of the affine cone over smooth quadric three-fold) is the standard example of a ring that is factorial (i.e. a UFD) but not regular.

Exercise 2.2(b). Let $\mathfrak{b} := (f) \cap \mathfrak{a}$; use that if $f \notin \mathfrak{a}$, then $\mathfrak{a} \subset (\mathfrak{b} : f) \subset \mathfrak{m}$.

Exercise 2.9. Consider an ideal with the property that it does not contain a product of primes, and which is maximal with respect to inclusion.

Exercise 2.11. When $\mathfrak{p}$ is minimal, the localization $R_{\mathfrak{p}}$ is Artinian and hence for $n \gg 0$ we have that $\mathfrak{p}^{(n)} = \{r \in R : \operatorname{Ann}(r) \not\subset \mathfrak{p}\}$.

Exercise 2.13 For the last part, show that if R is a ring and M a finite-length R-module, then M is finitely generated and $\operatorname{Supp} M \subset \operatorname{Spec} R$ is finite and consists only of maximal ideals; then use Theorem 2.3.1.

Exercise 3.2(c). Consider $f(X) = X^5 + X^4 + X^2 + 1$, when $\sqrt{X} \in S$. If $f_0 \in k[X]$ is the polynomial of least degree such that $K(\sqrt{f_0}) = K(\sqrt{f})$, then $S = R[\sqrt{f_0}]$. When k is perfect, we can always choose $f_0 = X$. In general, f_0 can be found in terms of f; see [20, Example 4.23] (but beware the errors).

Exercise 5.4. Either consider a maximal ideal of $K \otimes_k L$, or fix a set Γ of sufficiently large cardinality and consider $\overline{k(\Gamma)}$.

Exercise 5.6. If L/k is finite, use the Theorem on Natural Irrationalities ([15, Theorem 5.5]).

Exercise 5.7(b). Here's one outline. Show that the natural map $\mathbb{F}[X,Y] \to K$ is injective and so yields an isomorphism $\mathbb{F}(X,Y) \to K$ of field extensions of $\mathbb{F}$; this reduces the problem to showing that $\mathbb{F}(X^p + sY^p) \subset \mathbb{F}(X,Y)$ is algebraically closed. Next, show that there is an $\mathbb{F}$-algebra homomorphism $\varphi : \mathbb{F}[X,Y] \to \mathbb{F}[s^{1/p}][T]$ with $\ker\varphi = (X^p + sY^p)$. Finally, suppose there is an $f \in \mathbb{F}(X,Y) \smallsetminus \mathbb{F}(X^p + sY^p)$ algebraic over the latter, and write $f = g/h$ for some nonzero coprime $g, h \in \mathbb{F}[X,Y]$ chosen so as to minimize the "size" $|f| = \deg_X g + \deg_X h$. Applying φ to a suitable equation adapted from the one demonstrating the algebraicity of f, produce another algebraic element of smaller size.

Exercise 5.11. When K is finite, a power of the minimal polynomial over L of a generator of K/k lies in $k[X]$.

Exercise 5.15. Consider an open subset $V \subset \mathrm{GL}_n \mathbb{C}$ containing the identity such that V does not contain any nontrivial subgroup of $\mathrm{GL}_n \mathbb{C}$.

Exercise 7.1. One proof uses 7.2.1(s). For another, by 7.2.1(m), there is a nonzero ideal $\mathfrak{c} \subset R$ such that $\mathfrak{a} + \mathfrak{c} = (1)$ and $\mathfrak{a} \cdot \mathfrak{c}$ is principal, say $\mathfrak{a} \cdot \mathfrak{c} = (a)$ for some $a \in R$. Then $a \neq 0$, and $\mathfrak{a} \cdot \mathfrak{c} \not\subset a\mathfrak{b}$, so there is a $c \in \mathfrak{c}$ such that $c\mathfrak{a} \not\subset a\mathfrak{b}$. Take $\gamma := a/c$.

Exercise 8.3. For (h) ⇒ (d), use Baer's criterion. For (h) ⇒ (a), use that a semisimple module has finite length iff it is finitely generated, and that if R is a direct simple of simple ideals, then the kernel of each projection map onto a factor is a maximal ideal.

Exercise 10.7. The conditions in (a) and (b) are said to define a *strong map* of matroids $\mathscr{E} \Rightarrow \mathscr{D}$, and (c) a *weak map* of matroids $\mathscr{E} \to \mathscr{D}$.

Exercise 10.9. First try to answer these questions when G is finite.

Bibliography

[1] A. Zaks, "Atomic Rings without a.c.c. on Principal Ideals," *Journal of Algebra*, vol. 74, pp. 223–231, 1982.

[2] K. Conrad, "Remarks about Euclidean Domains." Available online here.

[3] H. Perdry, "An Elementary Proof of Krull's Intersection Theorem," *The American Mathematical Monthly*, vol. 111, no. 4, pp. 356–357, 2004.

[4] M. F. Atiyah and I. G. MacDonald, *Introduction to Commutative Algebra.* Addison-Wesley Publishing Company, 1969.

[5] R. Vakil, *The Rising Sea: Foundations of Algebraic Geometry.* Princeton University Press, 2025.

[6] The Stacks Project Authors, "*Stacks Project.*" `https://stacks.math.columbia.edu`, 2018.

[7] H. Matsumura, *Commutative Ring Theory*, vol. 8 of *Cambridge studies in advanced mathematics.* Cambridge University Press, 1986/2008.

[8] D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, vol. 150 of *Graduate Texts in Mathematics.* Springer, 1995.

[9] I. S. Cohen and A. Seidenberg, "Prime Ideals and Integral Dependence," *Bulletin of the American Mathematical Society*, vol. 52, pp. 252–261, 1946.

[10] I. Swanson and C. Huneke, *Integral Closure of Ideals, Rings, and Modules*, vol. 336 of *London Mathematical Society Lecture Note Series.* Cambridge University Press, 2006.

[11] A. Critch, "What does "linearly disjoint" mean for abstract field extensions?." MathOverflow. `https://mathoverflow.net/q/8324`(version: 2009-12-09).

[12] grghxy (https://math.stackexchange.com/users/239509/grghxy), "Does an inseparable extension have a purely inseparable element?." Mathematics Stack Exchange. URL:https://math.stackexchange.com/q/1276333 (version: 2015-05-10).

[13] J. Harris, *Algebraic Geometry: A First Course*, vol. 133 of *Graduate Texts in Mathematics.* Springer, 1992.

[14] Q. Liu, *Algebraic Geometry and Arithmetic Curves*, vol. 6 of *Oxford Graduate Texts in Mathematics.* Oxford University Press, 2002.

[15] P. Morandi, *Fields and Galois Theory*, vol. 167 of *Graduate Texts in Mathematics.* Springer, 1996.

[16] T. Y. Lam, *Lectures on Modules and Rings*, vol. 189 of *Graduate Texts in Mathematics.* Springer, 1999.

[17] H. Bruhn, R. Diestel, M. Kriesell, R. Pendavingh, and P. Wollan, "Axioms for Infinite Matroids," *Advances in Mathematics*, vol. 239, pp. 18–46, 2013.

[18] D. D. Anderson, M. Axtell, S. J. Forman, and J. Stickles, "When are associates unit multiples?," *Rocky Mountain J. Math.*, vol. 34, no. 3, Fall 2004. Available online here.

[19] G. Scheja and U. Storch, *Lehrbuch der Algebra: Unter Einschluß der linearen Algebra, Teil 2.* Mathematische Leitfäden, Vieweg+Teubner Verlag Wiesbaden, 1988.

[20] D. Lorenzini, *An Invitation to Arithmetic Geometry*, vol. 9 of *Graduate Studies in Mathematics.* American Mathematical Society, 1996.