Algebra

Erzhuo Wang

February 16, 2024

Contents

Chapter 1

Commutative Algebra

1.1 Basic Definition in Ring Thoery

Definition 1.1.1. A zero-divisor in a ring A is an element x which "divides 0", i.e., for which there exists $y \neq 0$ in A such that $xy = 0$.

Definition 1.1.2. An ideal which is maximal among all proper ideals is called a maximal ideal; an ideal m of A is maximal if and only if A/m is a field.

Theorem 1.1.3. If I is a proper ideal then there exists at least one maximal ideal containing I.

Definition 1.1.4. A ring A is an integral domain (or simply a domain) if $A \neq 0$, and A has no zero-divisors other than 0.

Definition 1.1.5. A field F is an integral doamin such that every non-zero element in F is invertible.

Definition 1.1.6. A proper ideal($\neq A$) P of A for which A/P is an integral domain is called a prime ideal. In other words, P is prime if it satisfies:

(1) $P \neq A$.

(2) $x, y \in \ \Rightarrow xy \in P$ for $x, y \in A$.

A field is an integral domain, so that a maximal ideal is prime.

Proposition 1.1.7. There is a one-to-one order-preserving correspondence between the ideals J of A which contain I, and the ideals A/I.More precisely,we can say there are two bijection

$$\{\text{ideals of A that contain I}\} \longleftrightarrow \{\text{ideals of } A/I\}$$

$$\{\text{prime ideals of A that contain I}\} \longleftrightarrow \{\text{prime ideals of } A/I\}$$

given by the correspondences

$$J \longrightarrow J/I = \bar{J}$$

$$\pi^{-1}(\bar{J}) \longleftarrow \bar{J}$$

where π be the natural homomorphism from A to A/I.

Definition 1.1.8. A subset S of A is multiplicative if it satisfies:

(1) $x, y \in S \Rightarrow xy \in S$.

(2) $1 \in S$.

Definition 1.1.9. If I is an ideal of A then the set of elements of A, some power of which belongs to I, is an ideal of A.This set is called the radical of I, and is sometimes written $\sqrt{I}$.

Theorem 1.1.10. the radical $\sqrt{I}$ of I is the interchapter of all prime ideals containing I.

Proof:

Lemma 1.1.11. Let S be a multiplicative set and I an ideal disjoint from S; then there exists a prime ideal containing I and disjoint from S.

Proof of the lemma: If I is an ideal disjoint from S,then the set of ideals containing I and disjoint from S has a maximal element. If P is an ideal which is maximal among ideals disjoint from S then P is prime. For if $x, y \notin P, xy \in P$, then since $P + xA$ and $P + yA$ both meet S, the product $(P + xA)(P + yA)$ also meets S. However, $(P + xA)(P + yA) \subset P + xyA$,a contradiction! □

If $x \notin \sqrt{I}$, $S_x = x^n : n \geq 0$ be a multiplicative subset. By lemma 1.1.11, we can find a prime ideal which contains I disjoint from S_x.

Definition 1.1.12. In particular if we take $I = (0)$ then $\sqrt{(0)}$ is the set of all nilpotent elements of A, and is called the nilradical of A; we will write $nil(A)$ for this. When $nil(A) = 0$ we say that A is reduced, For any ring A we write A_{red} for $A/nil(A)$ is of course reduced.

Definition 1.1.13. The interchapter of all maximal ideals of a ring $A \neq 0$ is called the Jacobson radical, or simply the radical of A and written $rad(A)$.

Proposition 1.1.14. $x \in rad(A)$ if and only if $1 + xy$ is a unit in A for all $y \in A$.

Definition 1.1.15. A ring having just one maximal ideal is called a local ring, and a (non-zero) ring having only finitely many maximal ideals a semilocal ring. We often express the fact that A is a local ring with maximal ideal m by saying that (A, m) is a local ring; if this happens then the field $k = A/m$ is called the residue field of A. We will say that (A, m, k) is a local ring to mean that A is a local ring, $m = rad(A)$ and $k = A/m$.

Proposition 1.1.16. If (A, m) is a local ring then the elements of A not contained in m are units; conversely a (non-zero) ring A whose non-units form an ideal m is a local ring with maximal ideal m.

Theorem 1.1.17. If $I_1, I_2, ..., I_n$ are ideals which are coprime(i.e. $I_i + I_j = A$ for all $i \neq j$) in pairs then $I_1 I_2 \dots I_n = I_1 \cap I_2 \cdots \cap I_n$

Theorem 1.1.18 (Chinese Reminder Theorem)**.** If $I_1, \ldots, I_n$ are ideals which are coprime in pairs then

$$A/I_1 \times \cdots \times A/I_n \simeq A/(I_1 \ldots I_n)$$

and the isomorphism map is given by

$$a + I_1 \ldots I_n \to (a + I_1, \ldots, a + I_n)$$

Theorem 1.1.19 (Prime Avoidance)**.** (1) Let $P_1, \ldots P_n$ be prime ideals and let I be an ideal contained in $\bigcup_{i=1}^{n} P_i$. Then $I \subset P_i$ for some $1 \leq i \leq n$.

(2) Let P be a prime ideal. $P \supset I_1 \ldots I_n$, then $P \supset I_i$ for some $1 \leq i \leq n$.

Proof: (2):If $P \supset IJ$ and $P \not\supseteq I$, there's $a \in I$ such that $a \notin P$. Since $P \supset IJ$, for all $b \in J$, $ab \in P$, then $b \in P$. Hence we have $P \supset J$.

Definition 1.1.20. Let R be an integral domain. Suppose $r \in R$ is nonzero and is not a unit. Then r is called irreducible in R if whenever $r = ab$ with $a, b \in R$, at least one of a or b must be a unit in R. Otherwise r is said to be reducible.The nonzero element $p \in R$ is called prime in R if the ideal (p) generated by p is a prime ideal.Two elements a and b of R differing by a unit are said to be associate in R.

Proposition 1.1.21. In an integral domain, a prime element is always irreducible.

Definition 1.1.22 (U.F.D)**.** A Unique Factorization Domain is an integral domain R in which every nonzero element $r \in R$ which is not a unit has the following two properties:

1. r can be written as a finite product of irreducibles p of R: $r = p_1 \ldots p_n$
2. the decomposition in (1) is unique up to associates.

Proposition 1.1.23. A intergral domain R is U.F.D if and only if every irreducible element is prime and there's no infinite sequence (a_n) in R satisfying: $a_i | a_{i+1}$, a_i and a_j are not associate.

Definition 1.1.24 (P.I.D)**.** A Principal Ideal Domain is an integral domain in which every ideal is principal.

Proposition 1.1.25. Every Principal Ideal Domain is a Unique Factorization Domain.

Proposition 1.1.26. If F is a field, then $F[x]$ is a Principal Ideal Domain.

Lemma 1.1.27 (Gauss' Lemma)**.** Let R be a Unique Factorization Domain with field of fractions F and let $p(x) \in R[x]$. If $p(x)$ is reducible in $F[x]$ then $p(x)$ is reducible in $R[x]$. More precisely, if $p(x) = A(x)B(x)$ for some nonconstant polynomials $A(x), B(x) \in F[x]$, then there are nonzero elements $r, s \in F$ such that $rA(x) = a(x)$ and $sB(x) = b(x)$ both lie in $R[x]$ and $p(x) = a(x)b(x)$ is a factorization in $R[x]$.

Corollary 1.1.28. Let R be a Unique Factorization Domain, let F be its field of fractions and let $p(x) \in R[x]$. Suppose the greatest common divisor of the coefficients of $p(x)$ is 1. Then $p(x)$ is irreducible in $R[x]$ if and only if it is irreducible in $F[x]$. In particular, if $p(x)$ is a monic polynomial that is irreducible in $R[x]$, then $p(x)$ is irreducible in $F[x]$.

Proposition 1.1.29. If R is a U.F.D, then $R[x]$ is a U.F.D.

Proof: By Proposition 1.1.26, Lemma 1.1.27 and Corollary 1.1.28.

1.2 Basic Definition in Module

Proposition 1.2.1. A R-module M can be view as a ring homomorphism from R to endmorphism ring of M(as an abelian group) which is in general not necessarily commutative:

$$R \to \mathrm{End}(M)$$
$$r \to (x \to rx)$$

Conversely, if M is an abelian group, Given a ring homomorphism $f : R \to End(M)$, we have

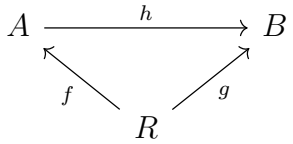
$$R \times M \to M$$
$$(r, m) \to f(r)m$$

is a R-module structure.

Remark 1.2.2. By Proposition 1.2.1, if we have a B-mdule M and a ring homomorphism $f : A \to B$, M has naturally a A-module structure.

Definition 1.2.3. $f : R \to B$ is a ring homomorphism, then B naturally has a R-module structure, we call B(with both a ring structure and A-module sturcte) a R-algebra.

And the morphism in R-algerba category between object $(A, f : R \to A)$ and $(B, g : R \to B)$, is the ring homomorphism $h : A \to B$ making the following diagram commute:



Definition 1.2.4. Let A be a ring and M an A-module. Given submodules N, N' of M, the set $\{a \in A : aN' \subset N\}$ is an ideal of A, which we write $(N : N')_A$ Similarly, if I is an ideal then $\{x \in M : Ix \subset N\}$ is a submodule of M, which we write $(N : I)_M$.

For $a \in A$ we define $(N : a)_M$ to be $(N : (a))_M$.The ideal $(0 : M)_A$ is called the Annihilator of M, and written $\mathrm{Ann}(M)$. We can consider M as a module over $A/\mathrm{Ann}(M)$. If $\mathrm{Ann}(M) = 0$, we say that M is a faithful A-module. For $x \in M$, we write $\mathrm{Ann}(x) = \{a \in A : ax = 0\}$.

Definition 1.2.5. If M is finitely generated as an A-module, we say simply that M is a finite A-module, or is finite over A.

Theorem 1.2.6 (Nakayama's lemma)**.** Let M be a finite A-module and I an ideal of A. If $M = IM$ then there exists $a \in A$ such that $aM = 0$ and $a \equiv 1 (\mathrm{mod}\, I)$. If in addition $I \subset rad(A)$, then M = 0.

Corollary 1.2.7. (A, m) be a Notherian local ring. If $A = mA$, then $A = 0$.

Corollary 1.2.8. Let A be a ring and I an ideal contained in $rad(A)$. Suppose that M is an A-module and $N \subset M$ a submodule such that M/N is finite over A. Then $M = N + IM$implies $M = N$.

Proof: Consider the identity $M/N = I(M/N)$, then use Theorem 1.2.6.

Definition 1.2.9. If W is a set of generators of an A-module M which is minimal, in the sense that any proper subset of W does not generate M, then W is said to be a minimal basis of M.

Theorem 1.2.10. Let $(A,\ \mathrm{m}, k)$ be a local ring and M a finite A-module; set $\bar{M} = M/\mathrm{m}M$. Now $\bar{M}$ is a finite-dimensional vector space over k, and we write $\boldsymbol{n}$ for its dimension. Then:

(1) If we take a basis $\{\bar{u}_1, \ldots, \bar{u}_n\}$ for $\bar{M}$ over k, and choose an inverse image $u_i \in M$ of each $\bar{u}_i$, then $\{u_1, \ldots, u_n\}$ is a minimal basis of M;

(2) conversely every minimal basis of M is obtained in this way, and so has n elements.

(3) If $\{u_1, \ldots, u_n\}$ and $\{v_1, \ldots, v_n\}$ are both minimal bases of M, and $v_i = \sum a_{ij}u_j$ with $a_{ij} \in A$ then $\det(a_{ij})$ is a unit of A, so that (a_{ij}) is an invertible matrix.

Proof:
(1) and (2): By Corollary 1.2.8
(3):By Proposition 1.1.16

Theorem 1.2.11 (Kaplansky)**.** Let (A, m) be a local ring; then a projective module M over A is free.

Proof: We only prove the case when M is finite. Choose a minimal basis $\omega_1, \ldots, \omega_n$ of M and define a surjective map $\varphi : F \longrightarrow M$ from the free module $F = Ae_1 \oplus \cdots \oplus Ae_n$ to M by $\varphi\left(\sum a_i e_i\right) = \sum a_i\omega_i$; if we set $K = \mathrm{Ker}(\varphi)$ then, from the minimal basis property(1),

$$\sum a_i\omega_i = 0 \Rightarrow a_i \in m \text{ for all } i.$$

Thus $K \subset \mathfrak{m}F$. Because M is projective, there exists $\psi : M \longrightarrow F$ such that $F = \psi(M) \oplus K$, and it follows that $K = mK$. On the other hand, K is a quotient of F, therefore finite over A, so that $K = 0$ by NAK and $F \simeq M$.

Proposition 1.2.12. Let A be a ring$\neq 0$. Show that if $A^m \simeq A^n$, then $m = n$.

Proof: Take a maximal ideal of I, consider a A/I-module isomorphism

$$A^n/IA^n \simeq A^n \otimes A/I \simeq A^m \otimes A/I \simeq A^m/IA$$

It's easy to check that $\{e_i + IA^n : 1 \leq i \leq n\}$ form a basis of A/I-module A^n/IA^n, hence $n = \dim(A^n/IA^n) = \dim(A^m/IA^m) = m$

Definition 1.2.13 (finite representation)**.** We say that an A-module M is of finite presentation if there exists an exact sequence of the form

$$A^p \longrightarrow A^q \longrightarrow M \to 0.$$

Proposition 1.2.14. Let A be a ring, and suppose that M is an A-module of finite presentation. If

$$0 \to K \longrightarrow N \longrightarrow M \to 0$$

is an exact sequence and N is finitely generated then so is K.

Proof: By assumption there exists an exact sequence of the form $L_2 \xrightarrow{g} L_1 \xrightarrow{f} M \to 0$, where L_1 and L_2 are free modules of finite rank. From this we get the following commutative diagram

$$\begin{array}{ccccccccc} & & L_2 & \xrightarrow{f} & L_1 & \xrightarrow{g} & M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 0 & \longrightarrow & K & \xrightarrow{\psi} & N & \xrightarrow{\varphi} & M & \longrightarrow & 0 \end{array}$$

If we write $N = A\xi_1 + \cdots + A\xi_n$, then there exist $v_i \in L_1$ such that $\varphi(\xi_i) = f(v_i)$. Set $\xi_i' = \xi_i - \alpha(v_i)$; then $\varphi(\xi_i') = 0$, so , that we can write $\xi_i' = \psi(\eta_i)$ with $\eta_i \in K$. Let us now prove that

$$K = \beta(L_2) + A\eta_1 + \cdots + A\eta_n.$$

For any $\eta \in K$, set $\psi(\eta) = \sum a_i \xi_i$, then

$$\psi\left(\eta - \sum a_i \eta_i\right) = \sum a_i (\xi_i - \xi_i') = \alpha\left(\sum a_i v_i\right)$$

and since $0 = \varphi\alpha(\sum a_i v_i) = f(\sum a_i v_i)$, we can write $\sum a_i v_i = g(u)$ with $u \in L_2$. Now

$$\psi\beta(u) = \alpha g(u) = \alpha\left(\sum a_i v_i\right) = \psi\left(\eta - \sum a_i \eta_i\right)$$

so that $\eta = \beta(u) + \sum a_i \eta_i$, and this proves our assertion.

Proposition 1.2.15. Let A be a ring and let $A[x]$ be the ring of polynomials in an indeterminate x, with coefficients in A. Let $f = a_0 + a_1 x + \cdots + a_n x^n \in A[x]$. Prove that

(1) f is a unit in $A[x] \Leftrightarrow a_0$ is a unit in A and $a_1, \ldots, a_n$ are nilpotent.

(2) f is nilpotent $\Leftrightarrow a_0, a_1, \ldots, a_n$ are nilpotent.

(3) f is a zero-divisor $\Leftrightarrow$ there exists $a \neq 0$ in A such that $af = 0$.(which implies if A is a domain, $A[x]$ is a domain).

(4) f is said to be primitive if $(a_0, a_1, \ldots, a_n) = (1)$. Prove that if $f, g \in A[x]$, then fg is primitive $\Leftrightarrow f$ and g are primitive.

In the following theorems, R is not necessarily be commutative, but we always assume R has an identity.

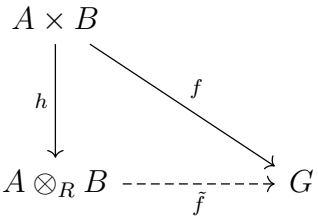
Definition 1.2.16. Let R be a ring, let A_R be a right R-module, let ${}_RB$ be a left R module, and let G be an (additive) abelian group. A function $f : A \times B \to G$ is called R-biadditive if, for all $a, a' \in A, b, b' \in B$, and $r \in R$, we have

$$\begin{aligned} f(a + a', b) &= f(a, b) + f(a', b), \\ f(a, b + b') &= f(a, b) + f(a, b'), \\ f(ar, b) &= f(a, rb). \end{aligned}$$

If R is commutative and A, B, and M are R-modules, then a function $f : A \times B \to M$ is called R-bilinear if f is R-biadditive and also

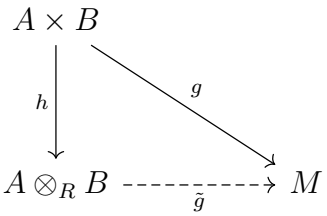
$$f(ar, b) = f(a, rb) = rf(a, b)$$

Definition 1.2.17 (Tensor product)**.** Given a ring R and modules A_R and ${}_RB$, then their tensor product is an abelian group $A \otimes_R B$ and an R-biadditive function $h : A \times B \to A \otimes_R B$



such that, for every abelian group G and every R-biadditive $f : A \times B \to G$, there exists a unique $\mathbb{Z}$-homomorphism $\tilde{f} : A \otimes_R B \to G$ making the following diagram commute.

Proposition 1.2.18. If R is a commutative ring and A, B are R-modules, then $A \otimes_R B$ is an R-module($r(a \otimes b) = (ra \otimes b)$), the function $h : A \times B \to A \otimes_R B$ is R-bilinear, and, for every R-module M and every R-bilinear function $g : A \times B \to M$, there exists a unique R-homomorphism $\tilde{g} : A \otimes_R B \to M$ making the following diagram commute.



Proposition 1.2.19. A is a ring, I is an ideal of A, M is a A-module, then $M \otimes_A (A/I) \simeq M/IM$ as A/I-module.

Proposition 1.2.20. If R is a ring, and $A_R, {}_RB$ are R-modules, then there are R-module isomorphisms:

$$A \otimes_R R \simeq A, \quad R \otimes_R B \simeq B$$

Theorem 1.2.21. If R and S are rings and A_R, ${}_RB_S$, S_C are (bi)modules, then there is an isomorphism:

$$(A \otimes_R B) \otimes_S C \simeq A \otimes_R (B \otimes_S C).$$

Theorem 1.2.22 (Commutativity)**.** If R is a commutative ring and M_R, ${}_RN$ are modules, then there is a R-isomorphism

$$\tau : M \otimes_R N \to N \otimes_R M$$

with $\tau : m \otimes n \mapsto n \otimes m$. The map τ is natural in the sense that the following diagram commutes:

$$\begin{array}{ccc} M \otimes_R N & \xrightarrow{\quad\tau\quad} & N \otimes_R M \\ \Big\downarrow{\scriptstyle f\otimes g} & & \Big\downarrow{\scriptstyle g\otimes f} \\ M' \otimes_R N' & \xrightarrow[\tau']{\quad\quad} & N' \otimes_R M' \end{array}$$

Theorem 1.2.23. Let R be a ring, A,$\{A_i\}_{i\in I}$ are right R-modules, B and $\{B_j\}_{j\in J}$ left R-modules. Then there are group isomorphisms:

$$\left(\sum_{i\in I} A_i\right) \otimes_R B \simeq \sum_{i\in I} (A_i \otimes_R B)$$
$$A \otimes_R \left(\sum_{j\in J} B_j\right) \simeq \sum_{j\in J} (A \otimes_R B_j)$$

Theorem 1.2.24 (Adjoint Associativity)**.** Let R and S be rings, let A be a right R-module, let B be an (R, S)-bimodule and let C be a right S-module. Then there is an natural bijection(acturally a isomorphism of abelian groups):

$$\mathrm{Hom}_S (A \otimes_R B, C) \cong \mathrm{Hom}_R (A, \mathrm{Hom}_S(B, C))$$

given by

$$\alpha : f \in \mathrm{Hom}_S (A \otimes_R B, C) \mapsto (a \mapsto (\Phi : b \mapsto f(a \otimes b)))$$

and

$$\beta : g \in \mathrm{Hom}_R (A, \mathrm{Hom}_S(B, C)) \mapsto (a \otimes b \mapsto g(a)(b))$$

Remark 1.2.25. 'natrual' in above theorem means: ${}_RB_S$ is a bi-module, then $(\_\_ \otimes_R B, \mathrm{Hom}_S(B, \_\_))$ is a adjoint pair between right R-module category and right S-module category.

Remark 1.2.26. (1) If ${}_RB_S$ is a bi-module, C is a right R-module, $\mathrm{Hom}_S(B, C)$ has a natrual right R-module sturct. Notice that we can define $fr(b) = f(rb)$, then $fr(bs) = f(r(bs)) = f((rb)s) = f(rb)s = (fr(b))s$,$f(r_1r_2)(b) = (fr_1)r_2(b)$. It makes $\mathrm{Hom}_S(B, C)$ to be a right R-module.

(2) If ${}_SB_R$ is a bi-module, C is a left S-module, then $\mathrm{Hom}_S(B, C)$ has a natrual left R-module sturct.

(3) If ${}_SB_R$ is a bi-module, C is a left S-module, then $B \otimes_R A$ has a natrual left S-module structure.

Proposition 1.2.27. If M is a left R-module, then there's left R-module isomorphism

$$\mathrm{Hom}_R(R, M) \simeq M$$

Theorem 1.2.28. If R is a ring with identity and A_R and ${}_RB$ are free R-modules with bases X and Y respectively, then $A \otimes_R B$ is a free (right) R-module($(a \otimes b)r = ar \otimes b$) with basis $W = \{x \otimes y : x \in X, y \in Y\}$.

Proposition 1.2.29. If k is a commutative ring and A and B are k-algebras, then the tensor product $A \otimes_k B$ is a k-algebra if we define

$$(a \otimes b)\,(a' \otimes b') = aa' \otimes bb'.$$

Lemma 1.2.30 (The Short Five Lemma)**.** Let R be a ring and

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{u} & M & \xrightarrow{v} & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & N' & \xrightarrow{u'} & N & \xrightarrow{v'} & N'' & \longrightarrow & 0 \end{array}$$

a commutative diagram of R-modules and R-module homomorphisms such that each row is a short exact sequence. Then

(1) α, γ monomorphisms $\Rightarrow \beta$ is a monomorphism(injective);

(2) α, γ epimorphisms $\Rightarrow \beta$ is an epimorphism(surjective);

(3) α, γ isomorphisms $\Rightarrow \beta$ is an isomorphism.

Definition 1.2.31 (Spilt exact sequence)**.** Let R be a ring and $0 \to A_1 \xrightarrow{f} B \xrightarrow{g} A_2 \to 0$ a short exact sequence of R-module homomorphisms. Then the following conditions are equivalent:

(1) There is an R-module homomorphism $h : A_2 \to B$ with $gh = 1_{A_2}$;

(2) There is an R-module homomorphism $k : B \to A_1$ with $kf = 1_{A_1}$;

(3) the given sequence is isomorphic (with identity maps on A_1 and A_2) to the direct sum short exact sequence $0 \to A_1 \xrightarrow{l_1} A_1 \oplus A_2 \xrightarrow{\pi_2} A_2 \to 0$; in particular B $\simeq A_1 \oplus A_2$.

(4)
$$0 \to \mathrm{Hom}_R(D, A) \xrightarrow{\bar{f}} \mathrm{Hom}_R(D, B) \xrightarrow{\bar{g}} \mathrm{Hom}_R(D, C) \to 0$$
is a spilt exact sequence of abelian groups for all R-module D.

(5)
$$0 \leftarrow \mathrm{Hom}_R(A, J) \xleftarrow{\bar{f}} \mathrm{Hom}_R(B, J) \xleftarrow{\bar{g}} \mathrm{Hom}_R(C, J) \to 0$$
is a spilt exact sequence of abelian groups for all R-module D.

A short exact sequence that satisfies the equivalent conditions is said to be split or a split exact sequence.

Lemma 1.2.32 (Snake lemma)**.** Let

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{u} & M & \xrightarrow{v} & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} & & \\ 0 & \longrightarrow & N' & \xrightarrow{u'} & N & \xrightarrow{v'} & N'' & \longrightarrow & 0 \end{array}$$

be a commutative diagram of A-modules and homomorphisms, with the rows exact. Then there exists an exact sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Ker}(f') & \xrightarrow{\bar{u}} & \mathrm{Ker}(f) & \xrightarrow{\bar{v}} & \mathrm{Ker}(f'') & & \\ & & & & & \overset{d}{\swarrow} & & & \\ & & \mathrm{Coker}(f') & \xrightarrow[\bar{u}']{} & \mathrm{Coker}(f) & \xrightarrow[\bar{v}']{} & \mathrm{Coker}(f'') & \longrightarrow & 0 \end{array}$$

in which $\bar{u}, \bar{v}$ are restrictions of u, v, and $\bar{u}', \bar{v}'$ are induced by u', v'. The boundary homomorphism d is defined as follows: if $x'' \in \mathrm{Ker}\,(f'')$, we have $x'' = v(x)$ for some $x \in M$, and $v'(f(x)) = f''(v(x)) = 0$, hence $f(x) \in \mathrm{Ker}\,(v') = \mathrm{Im}\,(u')$, so that $f(x) = u'\,(y')$ for some $y' \in N'$. Then $d\,(x'')$ is defined to be the image of y' in Coker (f').

Proposition 1.2.33.

(1)
$$0 \to A \xrightarrow{f} B \xrightarrow{g} C$$
is any short exact sequence of R-modules, if and only if for all R-module D
$$0 \to \mathrm{Hom}_R(D, A) \xrightarrow{\bar{f}} \mathrm{Hom}_R(D, B) \xrightarrow{\bar{g}} \mathrm{Hom}_R(D, C)$$
is an exact sequence of abelian groups.

(2)
$$A \xrightarrow{f} B \xrightarrow{g} C \to 0$$
is any short exact sequence of R-modules, is any short exact sequence of R-modules, if and only if for all R-module D
$$\mathrm{Hom}_R(A, D) \xleftarrow{\bar{f}} \mathrm{Hom}_R(B, D) \xleftarrow{\bar{g}} \mathrm{Hom}_R(C, D) \to 0$$
is an exact sequence of abelian groups.

Definition 1.2.34 (Projective module)**.** Let R be a ring. The following conditions on an R-module P are equivalent.

(1) given a diagram as follow with row exact, there's h making the diagram commute.

$$\begin{array}{ccccc} & & P & & \\ & \overset{h}{\swarrow} & \downarrow{\scriptstyle f} & & \\ A & \xrightarrow{g} & B & \longrightarrow & 0 \end{array}$$

(2) every short exact sequence $0 \to A \xrightarrow{f} B \xrightarrow{g} P \to 0$ is split exact.

(3) there is a free module F and an R-module K such that F $\cong$ K$\oplus$P.(summand of free module)

(4) if $f : B \to C$ is any R-module epimorphism then $\bar{f} : \mathrm{Hom}_R(P, B) \to \mathrm{Hom}_R(P, C)$ is an epimorphism of abelian groups;

(5) if

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

is any short exact sequence of R-modules, then

$$0 \to \mathrm{Hom}_R(P, A) \xrightarrow{\bar{f}} \mathrm{Hom}_R(P, B) \xrightarrow{\bar{g}} \mathrm{Hom}_R(P, C) \to 0$$

is an exact sequence of abelian groups.

Proposition 1.2.35. Every free module F over a ring R is projective.

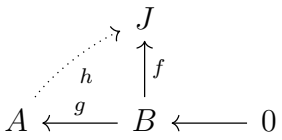
Proposition 1.2.36. Let R be a ring. A direct sum of R-modules $\sum_i P_i$ is projective if and only if each P_i is projective.

Proposition 1.2.37. If R is commutative then the tensor product of two projective R-modules (with a natural R-module structure) is projective.

Proof: By Adjoint Associativity.

Definition 1.2.38 (Injective module)**.** Let R be a ring with identity. The following conditions on a unitary R-module R are equivalent:

(1) given a diagram as follow with row exact, there's h making the diagram commute.



(2) every short exact sequence $0 \to J \xrightarrow{f} B \xrightarrow{g} C \to 0$ is split exact.

(3) J is a direct summand of any module B of which it is a submodule.

(4) if $f : B \to C$ is any R-module monomorphism then $\bar{f} : \mathrm{Hom}_R(A, J) \leftarrow \mathrm{Hom}_R(B, J)$ is an epimorphism of abelian groups;

(5) if

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

is any short exact sequence of R-modules, then

$$0 \leftarrow \mathrm{Hom}_R(A, J) \xleftarrow{\bar{f}} \mathrm{Hom}_R(B, J) \xleftarrow{\bar{g}} \mathrm{Hom}_R(C, J) \to 0$$

is an exact sequence of abelian groups.

(6) for every left ideal L of R, any R-module homomorphism $L \to J$ can be extended to $R \to J$(Baer's Criterion)

Proposition 1.2.39. A direct product of R-modules $\prod_{i\in I} J_i$ is injective ifand only if J_i is injective for every $J_i, i \in I$.

Proposition 1.2.40. If R is a P.I.D., then Q is injective if and only if $rQ = Q$ for every nonzero $r \in R$.

Proof: By Baer's Criterion.

Proposition 1.2.41. Suppose that D is a right R-module and that L, M and N are left R-modules. If

$$0 \longrightarrow L \xrightarrow{\psi} M \xrightarrow{\varphi} N \longrightarrow 0 \text{ is exact,}$$

then the associated sequence of abelian groups

$$D \otimes_R L \xrightarrow{1\otimes\psi} D \otimes_R M \xrightarrow{1\otimes\varphi} D \otimes_R N \longrightarrow 0 \quad \text{ is exact.}$$

Proposition 1.2.42. Let R be a ring and let M be an R-module. Then M is contained in an injective R-module.

Proposition 1.2.43. Any modules over a PID, it is a projective module if and only if it is a free module.

Definition 1.2.44 (Flat module)**.** Let A be a right R-module. Then the following are equivalent:

(1) For any left R-modules L, M, and N, if

$$0 \longrightarrow L \xrightarrow{\psi} M \xrightarrow{\varphi} N \longrightarrow 0$$

is a short exact sequence, then

$$0 \longrightarrow A \otimes_R L \xrightarrow{1\otimes\psi} A \otimes_R M \xrightarrow{1\otimes\varphi} A \otimes_R N \longrightarrow 0$$

is also a short exact sequence.

(2) For any left R-modules L and M, if $0 \to L \xrightarrow{\psi} M$ is an exact sequence of left R-modules (i.e., $\psi : L \to M$ is injective) then $0 \to A\otimes_R L \xrightarrow{1\otimes\psi} A\otimes_R M$ is an exact sequence of abelian groups (i.e., $1 \otimes \psi : A \otimes_R L \to A \otimes_R M$ is injective).

Similarly, we can define left flat R-module.

Proposition 1.2.45. Projective modules are flat.

Example 1.2.46. $\mathbb{Q}/\mathbb{Z}$ is not flat.

Proof: Since $\mathbb{Q}/\mathbb{Z} \otimes \mathbb{Z} \simeq \mathbb{Q}/\mathbb{Z}$, we have $\frac{1}{2} + \mathbb{Z} \otimes 1$ is non-zero. Consider a exact sequence

$$0 \to \mathbb{Z} \xrightarrow{\times 2} \mathbb{Z}$$

, tensor the exact sequence with $\mathbb{Q}/\mathbb{Z}$. Notice that $\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z} \xrightarrow{1\otimes(\times 2)} \mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}$ is not injective since $\frac{1}{2} + \mathbb{Z} \otimes 1$ in its kernel. Hence $\mathbb{Q}/\mathbb{Z}$ is not flat.

Proposition 1.2.47. $\sum_{i\in I} A_i$ flat if and only if each $A_i, i \in I$ flat.

Proof: Since tensor product commute with direct sum.

Example 1.2.48.

	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{Q}/\mathbb{Z}$	$\mathbb{Z} \oplus \mathbb{Q}$
flat	✓	✓(By 1.8.2)	×(1.2.46)	✓(1.2.47)
projective	✓	×(By 1.2.43)	×	×(1.2.36)
injective	×(By 1.2.40)	✓(By 1.2.40)	✓(By 1.2.40)	×(1.2.39)

1.3 Basic Definition in Field Thoery

Theorem 1.3.1. Let $p(x) \in F[x]$ be an irreducible polynomial of degree n over the field F and let K be the field $F[x]/(p(x))$. Let $\theta = x \bmod (p(x)) \in K$. Then the elements

$$1, \theta, \theta^2, \ldots, \theta^{n-1}$$

are a basis for K as a vector space over F, so the degree of the extension is n, i.e., $[K : F] = n$. Hence

$$K = \left\{a_0 + a_1\theta + a_2\theta^2 + \cdots + a_{n-1}\theta^{n-1} \mid a_0, a_1, \ldots, a_{n-1} \in F\right\}$$

consists of all polynomials of degree $< n$ in θ.

Definition 1.3.2. Let K be an extension of the field F and let S be a subset of K. Then the smallest subfield of K containing both F and the elements $s \in S$, denoted $F(S)$ is called the field generated by S over F. If the field K is generated by a single element α over $F, K = F(\alpha)$, then K is said to be a simple extension of F and the element α is called a primitive element for the extension.

Theorem 1.3.3. Let F be a field and let $p(x) \in F[x]$ be an irreducible polynomial. Suppose K is an extension field of F containing a root α of $p(x) : p(\alpha) = 0$. Let $F(\alpha)$ denote the subfield of K generated over F by α. Then

$$F(\alpha) \cong F[x]/(p(x))$$

Suppose that $p(x)$ is of degree n. Then

$$F(\alpha) = \left\{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} \mid a_0, a_1, \ldots, a_{n-1} \in F\right\} \subseteq K$$

Theorem 1.3.4. Let $\varphi : F \xrightarrow{\sim} F'$ be an isomorphism of fields. Let $p(x) \in F[x]$ be an irreducible polynomial and let $p'(x) \in F'[x]$ be the irreducible polynomial obtained by applying the map φ to the coefficients of $p(x)$. Let α be a root of $p(x)$ (in some extension of F) and let β be a root of $p'(x)$ (in some extension of F'). Then there is an isomorphism

$$\begin{aligned} \sigma : F(\alpha) &\xrightarrow{\sim} F'(\beta) \\ \alpha &\longmapsto \beta \end{aligned}$$

mapping α to β and extending φ, i.e., such that σ restricted to F is the isomorphism φ.

In the following statements, we always assume F be a field and let K be an extension of F, $\alpha, \beta \in K$ be an element.

Definition 1.3.5. The element $\alpha \in K$ is said to be algebraic over F if α is a root of some nonzero polynomial $f(x) \in F[x]$. If α is not algebraic over F, then α is said to be transcendental over F. The extension K/F is said to be algebraic if every element of K is algebraic over F.

Let α be algebraic over F. Then there is a unique monic irreducible polynomial $m_{\alpha,F}(x) \in F[x]$ which has α as a root. A polynomial $f(x) \in F[x]$ has α as a root if and only if $m_{\alpha,F}(x)$ divides $f(x)$ in $F[x]$.

Theorem 1.3.6. Let α be algebraic over the field F and let $F(\alpha)$ be the field generated by α over F. Then

$$F(\alpha) \cong F[x]/\left(m_\alpha(x)\right)$$

so that in particular

$$[F(\alpha) : F] = \deg m_\alpha(x) = \deg \alpha,$$

i.e., the degree of α over F is the degree of the extension it generates over F.

Proposition 1.3.7. The element $\alpha \in K$ is algebraic over F if and only if the simple extension $F(\alpha)/F$ is finite. More precisely, if α is an element of an extension of degree n over F then α satisfies a polynomial of degree at most n over F and if α satisfies a polynomial of degree n over F then the degree of $F(\alpha)$ over F is at most n.

Definition 1.3.8. Let K_1 and K_2 be two subfields of a field K. Then the composite field of K_1 and K_2, denoted K_1K_2, is the smallest subfield of K containing both K_1 and K_2. Similarly, the composite of any collection of subfields of K is the smallest subfield containing all the subfields.

Proposition 1.3.9. $F(\alpha, \beta) = (F(\alpha))(\beta)$, i.e., the field generated over F by α and β is the field generated by β over the field $F(\alpha)$ generated by α. In general, if $a_1, \ldots, a_n$ be elements of K, then $F(a_1, \ldots, a_n) = ((F(a_1)(a_2)) \ldots)(a_n)$

Corollary 1.3.10. If $K \subset L \subset M$ are field extensions, $L/K, M/L$ are algebraic extensions, then M/K is algerbaic.

Definition 1.3.11 (spilting field)**.** The extension field K of F is called a splitting field for the polynomial $f(x) \in F[x]$ if $f(x)$ factors completely into linear factors (or splits completely) in $K[x]$ and $f(x)$ does not factor completely into linear factors over any proper subfield of K containing F.

Theorem 1.3.12. For any field F, if $f(x) \in F[x]$ then there exists an extension K of F which is a splitting field for $f(x)$.

Proof: We first show that there is an extension E of F over which $f(x)$ splits completely into linear factors by induction on the degree n of $f(x)$. If $n = 1$, then take $E = F$. Suppose now that $n > 1$. If the irreducible factors of $f(x)$ over F are all of degree 1 , then F is the splitting field for $f(x)$ and we may take $E = F$. Otherwise, at least one of the irreducible factors, say $p(x)$ of $f(x)$ in $F[x]$ is of degree at least 2 . Hence, there is an extension E_1 of F containing a root α of $p(x)$. Over E_1 the polynomial $f(x)$ has the linear factor $x - \alpha$. The degree of the

remaining factor $f_1(x)$ of $f(x)$ is $n-1$, so by induction there is an extension E of E_1 containing all the roots of $f_1(x)$. Since $\alpha \in E, E$ is an extension of F containing all the roots of $f(x)$. Now let K be the interchapter of all the subfields of E containing F which also contain all the roots of $f(x)$. Then K is a field which is a splitting field for $f(x)$.

Theorem 1.3.13. Let $\varphi : F \xrightarrow{\sim} F'$ be an isomorphism of fields. Let $f(x) \in F[x]$ be a polynomial and let $f'(x) \in F'[x]$ be the polynomial obtained by applying φ to the coefficients of $f(x)$. Let E be a splitting field for $f(x)$ over F and let E' be a splitting field for $f'(x)$ over F'. Then the isomorphism φ extends to an isomorphism $\sigma : E \xrightarrow{\sim} E'$, i.e., σ restricted to F is the isomorphism φ :

$$\begin{array}{ccc} \sigma : E & \xrightarrow{\sim} & E' \\ \uparrow & & \uparrow \\ \varphi : F & \xrightarrow{\sim} & F' \end{array}$$

Definition 1.3.14. The field $\bar{F}$ is called an algebraic closure of F if $\bar{F}$ is algebraic over F and if every polynomial $f(x) \in F[x]$ splits completely over $\bar{F}$ (so that $\bar{F}$ can be said to contain all the elements algebraic over F).

A field K is said to be algebraieally closed if every polynomial with coefficients in K has a root in K.

Theorem 1.3.15. Let $\bar{F}$ be an algebraic closure of F. Then F is algebraically closed.

Proof: By Corollary 1.3.10.

Theorem 1.3.16. For any field F, algebraic closure of F exists and is unique up to isomorphism.

Proof: Existence: For each polynomial $f \in F[X]$, choose a splitting field E_f, and let

$$\Omega = \left(\bigotimes_{f \in F[x]} E_f \right) / M$$

where M is a maximal ideal. It is clear that Ω is a F-algebra and E_f can be embedded into Ω. Since f splits in E_f, it must also split in the larger field Ω. Then all the algebraic elements in Ω is therefore an algebraic closure of F.

Uniqueness: It is suffice to show:

Lemma 1.3.17. Let $\varphi : F \xrightarrow{\sim} F'$ be an isomorphism of fields, $\bar{F}'$ bethe algebraic closure of F', E/F is a algebraic extension, then there's $\sigma : E \to \bar{F}'$ ring homomorphism satisfying $\sigma|_F = \varphi$

Proof of the lemma: By Zorn's Lemma and Theorem 1.3.4. □

In the following statements, F is a field, and we fix an algebraic closure of F and denote it by $\bar{F}$.

Definition 1.3.18 (separable)**.** A polynomial $f(x) \in F[x]$ is separable if $f(x)$ has no multiple root in $\bar{F}$.

Proposition 1.3.19. A polynomial $f(x)$ has a multiple root $\alpha \in \bar{F}$ if and only if α is also a root of $f'(x)$. In particular, $f(x)$ is separable if and only if it is relatively prime to its derivative: $(f(x), D_x f(x)) = 1$.

Remark 1.3.20. For any two polynomials $f(x), g(x) \in F[x]$, they have the same g.c.d in $F[x]$ and $\bar{F}[x]$ since Euclidean division doesn't change if we replace F by any extension field of F.

Definition 1.3.21. $\alpha \in \bar{F}$ is separable if $m_\alpha(x) \in F[x]$ is separable polynomial.

$F \subset E \subset \bar{F}$ are field extensions, E/F is a separable extension if for all $\alpha \in E$, α is separable.

Definition 1.3.22 (perfect field)**.** A field $F \subset \bar{F}$ is perfect if and only if every finite extension of F is separable.

Lemma 1.3.23. Let $p(x)$ be an irreducible polynomial over a field F of characteristic p. Then there is a unique integer $k \geq 0$ and a unique irreducible separable polynomial $p_{\text{sep}}(x) \in F[x]$ such that

$$p(x) = p_{sep}\left(x^{p^k}\right)$$

Proposition 1.3.24. A field F is perfect if and only if it is a field of characteristic 0 or a field of characteristic $p > 0$ such that every element has a p-th root.

Proof: '$\Longleftarrow$': case 1: If $\operatorname{chap} F = 0$, then by Proposition 1.3.19, F is perfect.

case 2: If $\operatorname{chap} F = p$, $\alpha \in \bar{F}$, and $p(x) = m_\alpha(x) \in F[x]$ is inseparable, by Lemma 1.3.23, there's irreducible polynomial $q(x)$ such that $p(x) = q(x^p)$. Hence

$$p(x) = a_m x^{pm} + \cdots + a_1 x^p + a_0 = b_m^p x^{pm} + \ldots b_1^p x^p + b_0^p = (b_m x^m + \ldots b_0)^p$$

where $b_i^p = a_i$ for $i = 0, \ldots m$. A contradiction!

'$\Longrightarrow$': if $\operatorname{chap} F = p$ and $\alpha \in \bar{F}$ is not a p-th root, consider $p(x) = x^p - \alpha$. Notice that $(p(x), p'(x)) = p(x)$, then $p(x)$ is inseparable. However, if $\beta \in \bar{F}$ is a root of $p(x)$, then $p(x) = x^p - \alpha = x^p - \beta^p = (x - \beta)^p$. If $p(x)$ is reducible in $F[x]$, $p(x) = a(x)b(x)$ where $\deg a(x), \deg b(x) < p$.

Notice that $a(x) = (x - \beta)^s, b(x) = (x - \beta)^t \in F[x]$ with $s + t = p$, then $\beta^s \in F, \beta^t \in F$. Hence by Bezout Theorem, we have $\beta^{(s,t)} = \beta \in F$ which contradict to the fact that α is not a p-th root. Hence $p(x)$ is irreducible inseparable polynomial, and contradict to the fact F is perfect!

Corollary 1.3.25. In the proof of above Proposition, we can get: If $\operatorname{chap} F = 0$ and $p(x) = x^p - \alpha \in F[x]$, either $p(x)$ is irreducible or $p(x) = (x - \beta)^p$ for some $\beta \in F$.

Example 1.3.26. $\mathbb{Q}, \mathbb{F}_q$ are perfect fields and $\mathbb{F}_p(t)$ is not perfect field.

Definition 1.3.27. Given field extensions $F \subset E \subset \bar{F}$, E is called purely inseparable if for each $\alpha \in E$ the minimal polynomial of α over F has only one distinct root. It is easy to see that the following are equivalent:

(1) E/F is purely inseparable

(2) if $\alpha \in E$ is separable over F, then $\alpha \in F$

(3) if $\alpha \in E$, then $\alpha^{p^n} \in F$ for some n (depending on α), and $m_{\alpha,F}(x) = x^{p^n} - \alpha^{p^n}$.

Definition 1.3.28. Let $F \subset E \subset \bar{F}$ be field extensions, we call E/F normal if for all $\alpha \in E$, all the roots of $m_\alpha(x)$ lie in E.

Definition 1.3.29. Let $F \subset E \subset \bar{F}$ be field extensions. Let $\mathrm{Aut}(E/F)$ be the collection of automorphisms of K which fix F.

Theorem 1.3.30. Let $F \subset E \subset \bar{F}$ be field extensions, the following statements are equivalent:

(1) E/F is normal.

(2) every F-algebra homomorphism from E to $\bar{F}$ is a F-algebra homomorphism from E to E.

Moreover, if $[K : F] < \infty$, then the above statements are equivalent to that K is a splitting field of some $p(X) \in F[x]$.

Proof: (1)$\Longrightarrow$(2) is clear.

(2)$\Longrightarrow$(1): By Lemma 1.3.16

Now suppose $[E : F] < \infty$. First we assume $F \subseteq E$ is normal and choose $u_1 \in E - F$. Then its minimal polynomial is P_{u_1} and $[E : F(u_1)] < [E : F]$. Next we choose $u_2 \in E - F(u_1)$. Continuing this process, we conclude $E = F(u_1, \ldots, u_n)$. Let $P = \prod_{i=1}^n P_{u_i}$, and then E is the splitting field of P.

On the other hand, if E is the splitting field of $P \in F[X]$ whose roots in $\bar{F}$ are $\{u_1, \ldots, u_n\}$. Then $E = F(u_1, \ldots, u_n)$. Consider an F-algebra homomorphism $\iota : F(u_1, \ldots, u_n) \to \bar{F}$, since $\iota(u_i)$ is a root of P as well, $\iota(u_i) \in E$. Hence $\iota(E) \subseteq E$.

Proposition 1.3.31. Given field extensions $F \subset E \subset \bar{F}$, then all F-algerba homomorphisms from E to E are in $\mathrm{Aut}(E/F)$ i.e. $\mathrm{Aut}(E/F) = \{F\text{-algebra homomorphism between } E \text{ and } E\}$

Proof: Given any F-algebra homorphism $\tau : K \to K$, we know it's injective and it' enough to prove it's surjective. We assume $u \in K$ and $P \in F[X]$ is its minimal polynomial over F. If $u_1, \ldots, u_n$ are its different roots in $\bar{F}$, we assume only $u_1, \ldots, u_r$ are in K. Then $u \in \{u_1, \ldots, u_r\}$. Since τ fixes $F, \tau(u_i)$ is also a root of P in K where $1 \leq i \leq r$. Then $\tau : \{u_1, \ldots, u_r\} \to \{u_1, .., u_r\}$. That τ is injective implies it's surjective on this subset as well, which means $\exists u_i, \tau(u_i) = u$.

Theorem 1.3.32. Let E be the splitting field over F of the polynomial $f(x) \in F[x]$. Then

$$|\operatorname{Aut}(E/F)| \leq [E : F]$$

with equality if $f(x)$ is separable over F.

Definition 1.3.33. Let E/F be a finite extension. Then E is said to be Galois over F and E/F is a Galois extension if $|\operatorname{Aut}(E/F)| = [E : F]$. If E/F is Galois the group of automorphisms $\operatorname{Aut}(E/F)$ is called the Galois group of E/F, denoted $\operatorname{Gal}(E/F)$.

Proposition 1.3.34. We have 4 characterizations of Galois extensions E/F :

(1) splitting fields of separable polynomials over F

(2) fields where F is precisely the set of elements fixed by $\operatorname{Aut}(E/F)$ (in general, the fixed field may be larger than F)

(3) fields with $[E : F] = |\operatorname{Aut}(E/F)|$ (the original definition)

(4) finite, normal and separable extensions.

Theorem 1.3.35 (Fundamental Theorem of Galois Theory)**.** $F \subset K \subset \bar{F}$ be field extensions. K/F be a Galois extension and set $G = \operatorname{Gal}(K/F)$. Then there is a bijection:

$$\{\text{subfield of } K \text{containing } F\} \longleftrightarrow \{\text{subgroup of } G\}$$

given by the correspondences

$$E \longrightarrow \{\text{elements of } G \text{ fixing } E\}$$

$$\text{fix field of } H \longleftarrow H$$

which are inverse to each other. Under this correspondence,

(1) there's a one-to-one correspondence:

$$\begin{array}{ccc} \{F\text{-algebra homomorphism between } E \text{ and } \bar{F}\} & & \\ \uparrow{\scriptstyle \sigma H \mapsto \sigma|_E} & \searrow^{\text{Extended by 1.3.16 and 1.3.31}} & \\ \{\text{left cosets of } H \text{ in } G\} & \xrightarrow{\sigma H \mapsto \sigma|_E} & \{\sigma|_E : \sigma \in G\} \end{array}$$

(2) (inclusion reversing) If E_1, E_2 correspond to H_1, H_2, respectively, then $E_1 \subseteq E_2$ if and only if $H_2 \leq H_1$

(3) $[K : E] = |H|$ and $[E : F] = [G : H]$

(4) K/E is always Galois, with Galois group $\operatorname{Gal}(K/E) = H$:

(5) For all $\sigma \in G$,

$$\sigma(E) \longleftrightarrow \sigma H \sigma^{-1}$$

In particular, by (1) and Theorem 1.3.30, E is normal(hence Galios) over F if and only if H is a normal subgroup in G. If this is the case, then the Galois group is isomorphic to the quotient group

$$\mathrm{Gal}(E/F) \cong G/H$$

(6) If E_1, E_2 correspond to H_1, H_2, respectively, then the interchapter $E_1 \cap E_2$ corresponds to the group $(H_1, H_2\ )$ generated by H_1 and H_2 and the composite field E_1E_2 corresponds to the interchapter $H_1 \cap H_2$.

In the following statements, we fix a algebraic closure of F, and K, F', K_1, K_2 containing F are subfield of $\bar{F}$.

Theorem 1.3.36. Suppose K/F is a Galois extension and F'/F is any extension. Then KF'/F' is a Galois extension, with Galois group

$$\mathrm{Gal}\,(KF'/F') \cong \mathrm{Gal}\,(K/K \cap F')$$

isomorphic to a subgroup of $\mathrm{Gal}(K/F)$.

Corollary 1.3.37. Suppose K/F is a Galois extension and F'/F is any finite extension. Then

$$[KF' : F] = \frac{[K : F]\,[F' : F]}{[K \cap F' : F]}$$

Theorem 1.3.38. Let K_1 and K_2 be Galois extensions of a field F. Then

(1) The interchapter $K_1 \cap K_2$ is Galois over F.

(2) The composite K_1K_2 is Galois over F. The Galois group is isomorphic to the subgroup

$$H = \left\{(\sigma, \tau) | \sigma|_{K_1 \cap K_2} = \tau|_{K_1 \cap K_2}\right\}$$

of the direct product $\mathrm{Gal}\,(K_1/F) \times \mathrm{Gal}\,(K_2/F)$ consisting of elements whose restrictions to the interchapter $K_1 \cap K_2$ are equal.

Corollary 1.3.39. E/F be finite separable extension, there's Galois extension K_1 contains E(for example, the composite of the splitting fields of the minimal polynomials for a basis for E over F). Take S be the set of all the Galios extenison of F which contains E, then

$$\bar{E} = \bigcap_{K \in S} K = \bigcap_{K \in S} (K \cap K_1)$$

is acturally finite many interchapter of Galios extenison of F which contains E by Fundamental Theorem of Galios Theory.

Hence, there's minimal Galios extension of F that contains E.

Corollary 1.3.40. If K/F is finite and separable, then K/F is simple. In particular, any finite extension of fields of characteristic 0 is simple.

Corollary 1.3.41. K_1 and K_2 are separable extensions over F, then K_1K_2 also separable over F. In particular, all the separable elements in $\bar{F}$ form a field. We call it separable closure of F and denote it by F_{sep}.

Proposition 1.3.42. $\bar{F}/F_{sep}$ is pruely inseparable extension and F_{sep} is separable and normal extension.

Proof: By characterizations of purely inseparable extension and definition of normal extension.

Theorem 1.3.43. Let G be a topological group, and let $\mathcal{N}$ be a neighbourhood base for the identity element e of G. Then

(1) for all $N_1, N_2 \in \mathcal{N}$, there exists an $N' \in \mathcal{N}$ such that $e \in N' \subset N_1 \cap N_2$;

(2) all $a \in N \in \mathcal{N}$, there exists an $N' \in \mathcal{N}$ such that $N'a \subset N$;

(3) all $N \in \mathcal{N}$, there exists an $V \in \mathcal{N}$ such that $V^{-1}V \subset N$;

(4) all $N \in \mathcal{N}$ and all $g \in G$, there exists an $N' \in \mathcal{N}$ such that $g^{-1}N'g \subset N$;

Conversely, if G is a group and $\mathcal{N}$ is a nonempty set of subsets of G contain e satisfying $(1), (2), (3), (4)$, then there is a (unique) topology on G such that G is a topological group and $\mathcal{N}$ form a neighborhood base at e.

Morover, if subsets in $\mathcal{N}$ are all subgroup of G, we only need (1) and (4)

Definition 1.3.44. Given field extensions $F \subset E \subset \bar{F}$, E/F is called Galios extension iff E/F is separable and normal.

Theorem 1.3.45. $(L_i)_{i\in I}$ are all finite Galios extenison of F contained in E, notice that $\mathrm{Gal}(E/L_iL_j) \subset \mathrm{Gal}(E/L_i) \cap \mathrm{Gal}(E/L_j)$ for $i, j \in I$ and for all $\sigma \in \mathrm{Gal}(E/F)$, $\sigma^{-1}\mathrm{Gal}(E/L_i)\sigma = \mathrm{Gal}(E/L_i)$. Hence $(\mathrm{Gal}(E/L_i)_{i\in I}$ induce a topological group structure on $\mathrm{Gal}(E/F)$ such that $(\mathrm{Gal}(E/L_i)_{i\in I}$ form a neighborhood at e of G. We call it Krull topology.

E/F be a field extension, and not necessarily be algebraic.

Theorem 1.3.46 (infinite Galios correspondence)**.**

Definition 1.3.47 (transcendental degree)**.** (1) A subset $\{a_1, a_2, \ldots, a_n\}$ of E is called algebraically independent over F if there is no nonzero polynomial

$$f(x_1, x_2, \ldots, x_n) \in F[x_1, x_2, \ldots, x_n]$$

such that $f(a_1, a_2, \ldots, a_n) = 0$. An arbitrary subset S of E is called algebraically independent over F if every finite subset of S is algebraically independent. The elements of S are called independent transcendentals over F.

(2) A transcendence base for E/F is a maximal subset (with respect to inclusion) of E which is algebraically independent over F.

Theorem 1.3.48. The extension E/F has a transcendence base and any two transcendence bases of E/F have the same cardinality.

Definition 1.3.49. The cardinality of a transcendence base for E/F is called the transcendence degree of E/F.

Proposition 1.3.50. E/F be a field extension, $\alpha_1, \ldots, \alpha_n \in E$, $F_i = F(a_1, \ldots, a_i)$, then $\{\alpha_1, \ldots, \alpha_n\}$ is algebracally independent over F, if and only if α_i is transcendental over F_{i-1} for all $i = 1, \ldots, n$.

1.4 Specturm

Proposition 1.4.1. Let A be a ring and let X be the set of all prime ideals of A. For each subset E of A, let $V(E)$ denote the set of all prime ideals of A which contain E.

(1) if a is the ideal generated by E, then $V(E) = V(a) = V(r(a))$.

(2) $V(\varnothing) = X$,$V((1)) = \varnothing$

(3) if $(E_i)_{i\in I}$ is any family of subsets of A, then

$$V(E_i)_{i\in I} = \bigcap_{i\in I} V(E_i)$$

(4) $V(I \cap J) = V(IJ) = V(I) \cup V(J)$ for any ideals I,J of A. These results show that the sets $V(E)$ satisfy the axioms for closed sets in a topological space. The resulting topology is called the Zariski topology. The topological space X is called the prime spectrum of A, and is written Spec(A).

Proof: By Theorem 1.1.19

Proposition 1.4.2. $X = \text{Spec}(A)$, $D(f) = X - V(f)$.

(1) $D(f)$ form a basis of X.

(2) $D(fg) = D(f) \cap D(g)$.

(3) X is compact.

(4) $D(f) = \varnothing \Leftrightarrow f$ is a unit.

(5) $D(f) = X \Leftrightarrow f$ is nilpotent.

(6) An open subset of X is open if and only if it is finite union of sets $D(f)$.

The sets X_f are called basic open sets of X=Spec$A$

Proposition 1.4.3. It is sometimes convenient to denote a prime ideal of A by a letter such as x or y when thinking of it as a point of X =Spec$A$. When thinking of x as a prime ideal of A, we denote it by P_x. Show that:

(1) the set $\{x\}$ is closed in Spec(A) if and only if P_x is maximal.

(2) $\overline{\{x\}} = V(P_x)$

(3) $\overline{\{x\}}$ dense in X if and only if P_x equals to all the intersection of prime ideals of A.

Definition 1.4.4. A topological space X is said to be irreducible if $X \neq \varnothing$ and satisfies the following three equivalent conditions:

(1) every pair of non-empty open sets intersects.

(2) every non-empty open set is dense in X.

(3) X is not a union of two closed, proper, non-empty sets.

Proposition 1.4.5. Let X be a topological space.

(1) If Y is an irreducible subspace of X, then the closure Y of Y in X is irreducible.

(2) Every irreducible subspace of X is contained in a maximal irreducible subspace.

(3) The maximal irreducible subspaces of X are closed and cover X. They are called the irreducible components of X.

Proposition 1.4.6. A is a ring, Spec$A$ is the specturm of A.

There is a one-to-one order-reversing correspondence between the radical ideals($\sqrt{I} = I$) and the closed subsets of Spec$A$. More precisely,we can say there are three bijections

$$\{\text{radical ideals of } A\} \longleftrightarrow \{\text{closed subset of Spec}A\}$$

$$\{\text{prime ideals }\} \longleftrightarrow \{\text{irreducible closed subset}\}$$

$$\{\text{minimal ideals }\} \longleftrightarrow \{\text{irreducible components}\}$$

given by the correspondences

$$\begin{aligned} I &\longrightarrow V(I) \\ \bigcap_{P\in E} P &\longleftarrow V(E) \end{aligned}$$

Corollary 1.4.7. $X = \text{Spec}(A)$ is irreducible if and only if the nilradical of A is a prime ideal.

Proposition 1.4.8. Let $\varphi : A \to B$ be a ring homomorphism. Let X =Spec$A$ and Y =Spec$B$. Let ϕ to be the map:

$$\begin{aligned} \phi : \text{Spec}B &\to \text{Spec}A \\ P &\mapsto \varphi^{-1}(P) \end{aligned}$$

(1) If $f \in A$, then $\phi^{-1}(X_f) = Y_{\varphi(f)}$,and hence ϕ is continuous.

(2) I is an ideal of A, $\phi^{-1}(V(I)) = V(\varphi(I))$.

(3) J is an ideal of B, $\overline{\phi(V(J))} = V(\phi(J))$

(4) If φ is surjective, then ϕ is a homeomorphism of Y onto the closed subset $V(\text{Ker}(\phi))$ of X.

Definition 1.4.9. Let X be an arbitrary topological space.

(1) A point $x \in X$ is called closed if the set $\{x\}$ is closed,

(2) We say that a point $\eta \in X$ is a generic point if $\overline{\{\eta\}} = X$.

(3) Let x and x' be two points of X. We say that x is a generization of x' or that x' is a specialization of x if $x' \in \overline{\{x\}}$.

(4) A point $x \in X$ is called a maximal point if its closure $\overline{\{x\}}$ is an irreducible component of X.

(5) Thus a point $\eta \in X$ is generic if and only if it is a generization of every point of X. As the closure of an irreducible set is again irreducible, the existence of a generic point implies that X is irreducible.

Proposition 1.4.10. If $X = \operatorname{Spec} A$ is the spectrum of a ring, then

(1) A point $x \in X$ is closed if and only if $\mathfrak{p}_x$ is a maximal ideal.

(2) A point x is a generization of a point x' (in other words, x' is a specialization of x) if and only if $\mathfrak{p}_x \subseteq \mathfrak{p}_{x'}$.

(3) A point $x \in X$ is a maximal point if and only if $\mathfrak{p}_x$ is a minimal prime ideal.

(4) A point $\eta \in X$ is a generic point of X if and only if $\mathfrak{p}_\eta$ is the unique minimal prime ideal. This exists if and only if the nilradical of A is a prime ideal.

Definition 1.4.11. A topological space is called Noetherian if the closed subsets of X satisfy the descending chain condition, i.e., for closed subsets $Y_1, Y_2, Y_3, \ldots$ with $Y_{i+1} \subset Y_i$ for all positive integers i, there exists an integer n such that $Y_i = Y_n$ for all $i \geq n$. An equivalent condition is that the open subsets satisfy the ascending chain condition.

Example 1.4.12. R is a Noetherian ring, then $X = \operatorname{Spec}(R)$ is a Notherian space.

Proof: By Theorem 1.4.6

Theorem 1.4.13 (Decomposition into irreducibles)**.** Let X be a Noetherian topological space.

(1) There exist a nonnegative integer n and closed, irreducible subsets $Z_1, ..., Z_n \subset X$ such that $X = Z_1 \cup \ldots Z_n$ and $Z_i \nsubseteq Z_j$ for $i \neq j$.

(2) If $Z_1, ..., Z_n$ are closed, irreducible subsets satisfying (1), then every irreducible subset $Z \subset X$ is contained in some Z_i.

(3) If $Z_1, ..., Z_n \subset X$ are closed, irreducible subsets satisfying (1), then they are precisely the irreducible components of X. In particular, the Z_i are uniquely determined up to order.

Corollary 1.4.14. A Notherian ring has only finite many minimal prime ideals.

Proof: By Example 1.4.14 and Theorem 1.4.13.

Let $A = k[x_1, \ldots, x_n]$ be the polynomial ring in n variables over k.

Definition 1.4.15. We will interpret the elements of A as functions from the affine n-space to k, by defining $f(P) = f(a_1, \ldots, a_n)$, where $f \in A$ and $P \in \mathbf{A}^n$. Thus if $f \in A$ is a polynomial, we can talk about the set of zeros of f, namely $Z(f) = \{P \in \mathbf{A}^n \mid f(P) = 0\}$. More generally, if T is any subset of A, we define the zero set of T to be the common zeros of all the elements of T, namely

$$Z(T) = \{P \in \mathbf{A}^n \mid f(P) = 0 \text{ for all } f \in T\}.$$

A subset Y of $\mathbf{A}^n$ is an algebraic set if there exists a subset $T \subseteq A$ such that $Y = Z(T)$.

Proposition 1.4.16. The union of two algebraic sets is an algebraic set. The intersection of any family of algebraic sets is an algebraic set. The empty set and the whole space are algebraic sets.

Proof: If $Y_1 = Z(T_1)$ and $Y_2 = Z(T_2)$, then $Y_1 \cup Y_2 = Z(T_1T_2)$, where T_1T_2 denotes the set of all products of an element of T_1 by an element of T_2. Indeed, if $P \in Y_1 \cup Y_2$, then either $P \in Y_1$ or $P \in Y_2$, so P is a zero of every polynomial in T_1T_2. Conversely, if $P \in Z(T_1T_2)$, and $P \notin Y_1$ say, then there is an $f \in T_1$ such that $f(P) \neq 0$. Now for any $g \in T_2, (fg)(P) = 0$ implies that $g(P) = 0$, so that $P \in Y_2$.

If $Y_\alpha = Z(T_\alpha)$ is any family of algebraic sets, then $\bigcap Y_\alpha = Z(\bigcup T_\alpha)$, so $\bigcap Y_\alpha$ is also an algebraic set. Finally, the empty set $\varnothing = Z(1)$, and the whole space $\mathbf{A}^n = Z(0)$.

Definition 1.4.17. We define the Zariski topology on $\mathbf{A}^n$ by taking the open subsets to be the complements of the algebraic sets. This is a topology, because according to the proposition, the intersection of two open sets is open, and the union of any family of open sets is open. Furthermore, the empty set and the whole space are both open.

Definition 1.4.18. For any subset $Y \subseteq \mathbf{A}^n$, let us define the ideal of Y in A by

$$I(Y) = \{f \in A \mid f(P) = 0 \text{ for all } P \in Y\}.$$

Proposition 1.4.19. (1) If $T_1 \subseteq T_2$ are subsets of A, then $Z(T_1) \supseteq Z(T_2)$.

(2) If $Y_1 \subseteq Y_2$ are subsets of $\mathbf{A}^n$, then $I(Y_1) \supseteq I(Y_2)$.

(3) For any two subsets Y_1, Y_2 of $\mathbf{A}^n$, we have $I(Y_1 \cup Y_2) = I(Y_1) \cap I(Y_2)$.

(4) For any subset $Y \subseteq \mathbf{A}^n, Z(I(Y)) = \bar{Y}$, the closure of Y.

(5) an algebraic set Y is irreducible if and only if $I(Y)$ is a prime ideal.

Proof: (4): We note that $Y \subseteq Z(I(Y))$, which is a closed set, so clearly $\bar{Y} \subseteq Z(I(Y))$. On the other hand, let W be any closed set containing Y. Then $W = Z(\mathfrak{a})$ for some ideal $\mathfrak{a}$. So $Z(\mathfrak{a}) \supseteq Y$, and by (b), $IZ(\mathfrak{a}) \subseteq I(Y)$. But certainly $\mathfrak{a} \subseteq IZ(\mathfrak{a})$, so by (a) we have $W = Z(\mathfrak{a}) \supseteq ZI(Y)$. Thus $ZI(Y) = \bar{Y}$

(5): If Y is irreducible, we show that $I(Y)$ is prime. Indeed, if $f_g \in I(Y)$, then $Y \subseteq Z(fg) = Z(f) \cup Z(g)$. Thus $Y = (Y \cap Z(f)) \cup (Y \cap Z(g))$, both being closed subsets of Y. Since Y is irreducible, we have either $Y = Y \cap Z(f)$, in which case $Y \subseteq Z(f)$, or $Y \subseteq Z(g)$. Hence either

$f \in I(Y)$ or $g \in I(Y)$. Conversely, if $Y = Y_1 \cap Y_2$, $Y_1, Y_2 \subsetneqq Y$ are closed subset of A^n, then by (4), $I(Y_1) \supsetneqq I(Y)$. Hence take $f \in I(Y_1)$ such that $f \notin I(Y)$. Similarly, we can take $g \in I(Y_2)$ such that $g \notin I(Y)$, then $fg \in I(Y_1 \cup Y_2) = I(Y)$. A contradiction!

1.5 Chain conditions

Definition 1.5.1 (Notherian)**.** ring(R-module) A is said to be Noetherian if it satisfies the following three equivalent conditions:

(1) Every non-empty set of ideals(submodules) in A has a maximal element.

(2) Every ascending chain of ideals(submodules) in A is stationary.

(3) Every ideal(submodule) in A is finitely generated.

Definition 1.5.2 (Artinian)**.** ring(R-module) A is said to be Artinian if it satisfies the following three equivalent conditions:

(1) Every non-empty set of ideals(submodules) in A has a minimal element.

(2) Every decending chain of ideals(submodules) in A is stationary.

Theorem 1.5.3. Let $0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$ be an exact sequence of A-modules. Then

1. M is Noetherian $\Leftrightarrow$ M' and M'' are Noetherian;
2. M is Artinian $\Leftrightarrow$ M' and M'' are Artinian.

Corollary 1.5.4. If $M_i (1 \leqslant i \leqslant n)$ are Noetherian (resp. Artinian) A-modules, so is $\bigoplus_{i=1}^{n} M_i$.

Proof: Apply Theorem 1.5.3 to the exact sequence

$$0 \to M_n \to \bigoplus_{i=1}^{n} M_i \to \bigoplus_{i=1}^{n-1} M_i \to 0$$

Corollary 1.5.5. Let A be a Noetherian (resp. Artinian) ring, M a finitely generated A-module. Then M is Noetherian (resp. Artinian).

Definition 1.5.6. A chain of submodules of a module M is a sequence $(M_i)\,(0 \leqslant i \leqslant n)$ of submodules of M such that

$$M = M_0 \supset M_1 \supset \cdots \supset M_n = 0 \text{ (strict inclusions)}.$$

The length of the chain is n (the number of "links"). A composition series of M is a maximal chain, that is one in which no extra submodules can be inserted: this is equivalent to saying that each quotient $M_{i-1}/M_i (1 \leqslant i \leqslant n)$ is simple (that is, has no submodules except 0 and itself).

Proposition 1.5.7. Suppose that M has a composition series of length n. Then every composition series of M has length n, and every chain in M can be extended to a composition series.

Proposition 1.5.8. M has a composition series $\Leftrightarrow$ M satisfies both chain conditions.

Proposition 1.5.9. If A is a Artinian ring, A has only finitely many maximal ideals.

Proof: If $P_1, \ldots, P_n, \ldots$ is sequence of distinct maximal ideal. Consider decending chain of ideals:

$$P_1 \supset P_1P_2 \cdots \supset P_1 \ldots P_n \supset \ldots$$

By Theorem 1.1.19, each '$\supset$' is strict. A contradiction!

Proposition 1.5.10. A ring A is Artinian, then the product of all its maximal ideals is nilpotent.

Proof:

Proposition 1.5.11. A ring A is Artinian, then A is Notherian.

Proposition 1.5.12. Let A be a ring and M an A-module. Then if M is a Noetherian module, $/Ann(M)$ is a Noetherian ring.

Proof: If we set $\bar{A} = A/\operatorname{Ann}(M)$ and view M as an $\bar{A}$-module, then the submodules of M as an A-module or $\bar{A}$-module coincide, so that M is also Noetherian as an $\bar{A}$-module. We can thus replace A by $\bar{A}$, and then $Ann(M) = (0)$. Now letting $M = A\omega_1 + \cdots + A\omega_n$, we can embed A in M^n by means of the map $a \mapsto (a\omega_1, \ldots, a\omega_n)$. By Theorem 1, M^n is a Noetherian module, so that its submodule A is also Noetherian.

Theorem 1.5.13 (Hilbert basis theorem)**.** R is Notherian, then $R[x]$ and $R[[x]]$ are Notherian.

Corollary 1.5.14. Let B be a finitely-generated A-algebra. If A is Noetherian, then so is B.

Proof: By Hilbert basis theorem and Theorem 1.5.3.

Theorem 1.5.15 (Cohen)**.** If all the prime ideals of a ring A are finitely generated then A is Noetherian.

Definition 1.5.16 (fractional ideal)**.** Let A be an integral domain with field of fractions K. A fractional ideal I of A is an A-submodule I of K such that $I \neq 0$ and $\alpha I \subset A$ for some $0 \neq \alpha \in K$. The product of two fractional ideals is defined in the same way as the product of two ideals. If I is a fractional ideal of A we set $I^{-1} = \{\alpha \in K \mid \alpha I \subset A\}$; this is also a fractional ideal, and $II^{-1} \subset A$. In the particular case that $II^{-1} = A$ we say that I is invertible.

Proposition 1.5.17. An invertible fractional ideal of A is finitely generated as an A-module.

Proof: Let $1 = \sum a_i b_i$, where $a_i \in I, b_i \in I^{-1}$. Then $a_1, \ldots, a_n$ generate I.

1.6 Localization

Definition 1.6.1 (Localization of Ring)**.** Let R be a ring, and S a multiplicative subset. Define a relation on $R \times S$ by $(x, s) \sim (y, t)$ if there is $u \in S$ such that $xtu = ysu$.Denote by $S^{-1}R$ the set of equivalence classes, and by $x/$ the class of (x, s)

It is easy to check that $S^{-1}R$ is a ring, with $0/1$ for 0 and $1/1$ for 1. It is called the ring of fractions with respect to S or the localization at S.

Let $\varphi_S : R \to S^{-1}R$ be the map given by $\varphi_S(x) = x/1$. Then φ_S is a ring homomorphism between R and $S^{-1}R$

Example 1.6.2 (Localization at a prime ideal)**.** Let R be a ring, p be a prime ideal. Set $S_p := R - p$. We call the ring $S_p^{-1}R$ the localization of R at p, and set $R_p := S_p^{-1}R$, $\varphi_p = \varphi_{S_p}$.

Example 1.6.3 (Localization at a element)**.** Let R be a ring, $f \in R$. Set $S_f := \{f^n : n \geq 0\}$. We call the ring $S_f^{-1}R$ the localization of R at f, and set $R_f := S_f^{-1}R$ and $\varphi_f := \varphi_{S_f}$.

Example 1.6.4. Let $f : A \to B$ be a ring homomorphism, S be a multiplicative subset of A, then denote $f(S)$ is a multiplicative subset of B. Denote the localization at $f(S)$ by $S^{-1}B$. Respectively, if P is a prime ideal of A, denote the localization at $S = f(A - P)$ by B_P.

Proposition 1.6.5. Every ideal in $S^{-1}A$ of the form $S^{-1}I$.

Proof: Notice that if $\bar{I}$ is an ideal of $S^{-1}A$, then $S^{-1}\varphi_S^{-1}(\bar{I}) = \bar{I}$.

Proposition 1.6.6. A is Notherian, then $S^{-1}A$ is Notherian.

Proposition 1.6.7. Let R be a ring, S be a multiplicative subset of R,
$S^{-1}I = \{x/s : s \in I, s \in S\}$. Then $S^{-1}I$ is the ideal generated by $\varphi_S(I)$, and the following conditions are equivalent:

(1) $S^{-1}I = S^{-1}R$

(2) $I \cap S \neq \varnothing$

(3) $\varphi_S^{-1}(S^{-1}I) = R$

Proof: Obviously, $S^{-1}I$ is the ideal generated by $\varphi_S(I)$.
(1)⇒(2):Consider $1/1 \in S^{-1}I$.
(2)⇒(3):Take $a \in I \cap S$, notice that $a/a = 1/1$.
(3)⇒(1):Consider $1/1 \in S^{-1}I$.

Proposition 1.6.8. Let R be a ring, S be a multiplicative subset of R, there's a one-to-one order-preserving bijection:

$$\{P \in \mathrm{Spec}R : P \cap S = \varnothing\} \longleftrightarrow \mathrm{Spec}(S^{-1}R)$$

given by the following maps:

$$P \longrightarrow S^{-1}P$$

$$\varphi_S^{-1}(\bar{P}) \longrightarrow \overline{P} \in \mathrm{Spec}(S^{-1}R)$$

Proof: Step 1 (well-defined): If $P \in \mathrm{Spec}(R)$ and $P \cap S = \varnothing$, then $S^{-1}P$ is a prime of $S^{-1}R$.

Step 2 (injective): $\varphi_S^{-1}(S^{-1}P) = P$.

Step 3 (surjective): Let J be a prime ideal of $S^{-1}R$, then $P = \varphi_S^{-1}(J)$ is a prime ideal of R. We show that $S^{-1}P = J$. For all $x/s \in J$, since J is an ideal, $x/1 = x/s \times s/1 \in J$, hence $x \in P$ and $x/s \in S^{-1}P$. It is clear that $\varphi_S(\varphi_S^{-1}(J)) \subset J$. Hence, we have $J = S^{-1}P$.

Definition 1.6.9 (Localization of Module)**.** The construction of $S^{-1}A$ can be carried through with an A-module M in place of the ring A. Define a relation $=$ on $M \times S$ as follows: $(m, s) = (m', s')$ if and only if there's $t \in S$ such that $t(sm' - s'm) = 0$.

In particular, if P is a prime ideal of A, $S = A - P$, we call $M_P = S^{-1}M$ the localization at P.

Proposition 1.6.10. $S^{-1}M$ has both A-module structure and $S^{-1}A$-module structure by the natrual way:

$$S^{-1}A \times S^{-1}M \to S^{-1}M$$

$$(a/s, m/s_1) \to am/(ss_1)$$

$$A \times S^{-1}M \to S^{-1}M$$

$$(a, m/s_1) \to a/(ss_1)$$

Let $f : M \to N$ be an A-module homomorphism. Then it gives rise to an $S^{-1}A$-module and A-module homomorphism:

$$S^{-1}M \to S^{-1}N$$

$$m/s_1 \to f(m)/s$$

And, if $M \xrightarrow{f} N \xrightarrow{g} P$ is exact, then $S^{-1}M \xrightarrow{S^{-1}f} S^{-1}N \xrightarrow{S^{-1}g} S^{-1}P$ is exact.

Remark 1.6.11. It follows from Proposition 1.6.10 that if N is a submodule of M, the map $S^{-1}M \xrightarrow{S^{-1}f} S^{-1}M$ is injective, where $f : N \to M$ be the embeding. Therefore $S{-}1N$ can be regarded as a submodule of $S^{-1}M$.

Remark 1.6.12. If P is a prime ideal of A, $S = A - P$,$f : M \to N$ be a A-module homomorphism, we usually denote $S^{-1}f$ by f_P.

Proposition 1.6.13. If N, P are submodule of M,then

(1) $S^{-1}(N + P) = S^{-1}M + S^{-1}P$

(2) $S^{-1}(N \cap P) = S^{-1}N \cap S^{-1}P$

(3) the map $S^{-1}f : S^{-1}M \to S^{-1}(M/N)$ given by the natrual homomorphism $f : M \to M/N$ is an surjective.In particular,$S^{-1}M/S^{-1}N \simeq S^{-1}(M/N)$ as $S^{-1}A$-module and A-mdoule.

Theorem 1.6.14. Let M be an A-module. Then the $S^{-1}A$ modules $S^{-1}M$ and $S^{-1}A \otimes_A M$ are naturally isomorphic. The isomorphisc map is given by the bi-linear map:

$$S^{-1}A \times M \to S^{-1}M$$

$$\varphi : (a/s, m) \to am/s$$

and the universal property of tensor product.

Remark 1.6.15. 'natrually' in above theorem means: given two covariant functors:$S^{-1}A \otimes \_\_$ and $S^{-1}\_\_$, then the isomorphic map induced by φ induce a natrual transformation between these two functors.

Proposition 1.6.16 (localization commute with tensor product)**.** Let R be a ring, S a multiplicative subset, M, N modules. Show $S^{-1}(M \otimes_R N) \simeq S^{-1}M \otimes_R N \simeq S^{-1}M \otimes_{S^{-1}R} S^{-1}N$.

Proof:

$$S^{-1}(M \otimes_R N) \simeq S^{-1}R \otimes_R (M \otimes_R N) \simeq S^{-1}M \otimes_R N \simeq$$
$$(S^{-1}M \otimes_{S^{-1}A} S^{-1}A) \otimes_A N \simeq S^{-1}M \otimes_{S^{-1}R} S^{-1}N$$

Proposition 1.6.17 (M=0 is a local property)**.** Let M be an A-module. Then the following are equivalent:

(1) $M = 0$

(2) $M_P = 0$ for all prime ideals P.

(3) $M_m = 0$ for maximal ideals m.

Proposition 1.6.18 (injective homomorphism is a local property)**.** Let $f : M \to N$ be A-module homomorphism, $f_P : M_P \to N_P$ be homomorphism induced by prime ideal P. Then the following are equivalent:

(1) f is injective

(2) f_P is injective for all prime ideals P.

(3) f_m is injective for maximal ideals m.

Proposition 1.6.19 (flat is a local property)**.** Let $f : M \to N$ be A-module homomorphism, $f_P : M_P \to N_P$ be homomorphism induced by prime ideal P. Then the following are equivalent:

(1) f is flat A-module.

(2) f_P is flat A_P-module for all prime ideals P.

(3) f_m is flat A_m-module for all maximal ideals m.

Proposition 1.6.20. Let M be a finitely generated A-module, S a multiplicatively closed subset of A. Then $S^{-1}(\mathrm{Ann}(M) = \mathrm{Ann}(S^{-1}M)$.

Definition 1.6.21 (support of a module)**.** Let A be a ring, M an A-module. The support of M is defined to be the set $\mathrm{Supp}(M) = \{P \in \mathrm{Spec}(A) : M_P \neq 0\}$.

Proposition 1.6.22. M is a R-module, A is a ring, I is an ideal of A.

(1) $M \neq 0 \Leftrightarrow \mathrm{Supp}(M) = \varnothing$

(2) $V(I) = \mathrm{Supp}(A/I)$

(3) If $0 \to M' \to M \to M'' \to 0$ is an exact sequence, then $\mathrm{Supp}(M) = \mathrm{Supp}(M') \cup \mathrm{Supp}(M'')$.

(4) If M is finitely generated, then $\mathrm{Supp}(M) = V(\mathrm{Ann}(M))$

(5) If M, N are finitely generated, then $\mathrm{Supp}(M \otimes_A N) = \mathrm{Supp}(M) \cap \mathrm{Supp}(N)$.

(6) If $M = \sum_{i\in I} M_i$, then $\mathrm{Supp}(M) = \bigcap_{i\in I} \mathrm{Supp}(M_i)$

Proof:

(1):By Theorem 1.6.17

(2):By Proposition 1.6.13 and Proposition 1.6.7.

(3):By Theorem 1.6.10.

(4):Notice that $M_P \neq 0 \Leftrightarrow \mathrm{Ann}(M_P) \neq R$. Then Proposition 1.6.20.

(5):Since localization commute with tensor product, it suffice to show:

Lemma 1.6.23. M, N are finitely generated R-module, in which (R, m, k) be a local ring, $M \otimes_R N = 0$, then $M = 0$ or $N = 0$.

Proof of the lemma: Notice that $M \otimes_R R/m \simeq M/mM$. Hence, by Theorem 1.2.28, and Nakayama's lemma, define $M_k = M \otimes_A k$, it suffice to show $M_k \otimes_k N_k \simeq (M \otimes_R N)_k$ as k-vector space. Notice that

$$\begin{aligned} M_k \otimes_k N_k &= (M \otimes_R k) \otimes_k (k \otimes_R N) \\ \cong M \otimes_R (k \otimes_k k) \otimes_R N &\cong (M \otimes_R N) \otimes_R k = (M \otimes_R N)_k \end{aligned}$$

□

(6):trivial.

Proposition 1.6.24 (universal property of localization)**.** Let $g : A \to B$ be a ring homomorphism such that $g(s)$ is a unit in B for all $s \in S$. Then there exists a unique ring homomorphism $h : S^{-1}A \to B$ such that $g = h \circ f$.

Theorem 1.6.25. let A be a ring, $S \subset A$ a multiplicative set, I an ideal of A and $\bar{S}$ the image of S in A/I; then there's ring isomorphism

$$S^{-1}A/S^{-1}I \simeq \bar{S}^{-1}(A/I)$$

given by

$$a/s + S^{-1}I \mapsto a + I/(s + I)$$

In particular, if $\mathfrak{p}$ is a prime ideal of A then

$$A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} \simeq (A/\mathfrak{p})_{\overline{A-p}}.$$

where $\mathfrak{p}A_{\mathfrak{p}}$ is the ideal generated by $\varphi_{\mathfrak{p}}(\mathfrak{p})$. The left-hand side is the residue field of the local ring A_p, whereas the right-hand side is the field of fractions of the integral domain $A/\mathfrak{p}$. This field is written $\kappa(\mathfrak{p})$ and called the residue field of $\mathfrak{p}$.

Proof: By theorem 1.6.13 and universal property of localization.

Theorem 1.6.26. Let A be a ring, $S \subset A$ a multiplicative set, and $f : A \longrightarrow S^{-1}A$ the canonical map. If B is a ring, with ring homomorphisms $g : A \longrightarrow B$ and $h : B \longrightarrow S^{-1}A$ satisfying

(1) $f = hg$

(2) for every $b \in B$ there exists $s \in S$ such that $g(s) \cdot b \in g(A)$

Then $S^{-1}A \simeq g(S)^{-1}B \simeq T^{-1}B$, where $T = \{t \in B \mid h(t) \text{ is a unit of } S^{-1}A\}$.

Proof: By universal property of localization and condition (1) and (2), there are ring homomorphisms:

$$S^{-1}A \to g(S)^{-1}B$$
$$\varphi : a/s \mapsto g(a)/g(s)$$

$$g(S)^{-1}B \to S^{-1}A$$
$$\psi : b/g(s) \mapsto h(b) \cdot (1/s)$$

such that $\varphi \circ \psi = \mathrm{id}, \psi \circ \varphi = \mathrm{id}$. Hence $S^{-1}A \simeq g(S)^{-1}B$.

Since $T \supset g(S)$, by universal property of localization, there are ring homomorphisms:

$$S^{-1}A \to T^{-1}B$$
$$\varphi : a/s \mapsto g(a)/g(s)$$

$$T^{-1}B \to S^{-1}A$$
$$\psi : b/t \mapsto h(b)h(t)^{-1}$$

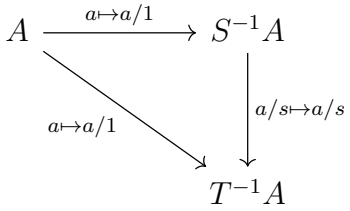
Notice that if $g(s_1)b = g(a_1), g(s_2) = tg(b_2)$, then $h(b)(s_1/1) = a_1/1, h(t)(s_2/1) = a_2/1$ and $\psi(b/t) = a_1/s_1 \cdot (a_2/s_2)^{-1}$. And it's easy to cheack that $\varphi(\psi(b/t)) = \varphi(a_1/s_1 \cdot (a_2/s_2)^{-1}) = g(a_1)/g(s_1) \cdot (g(a_2)/g(s_2))^{-1} = b/t$. Hence $S^{-1}A \simeq g(S)^{-1}B \simeq T^{-1}B$.

Corollary 1.6.27. If $\mathfrak{p}$ is a prime ideal of $A, S = A - \mathfrak{p}$ and B satisfies the conditions of the theorem, then setting $P = \mathfrak{p}A_{\mathfrak{p}} \cap B$ we have $A_{\mathfrak{p}} \simeq B_{\mathrm{P}}$.

Proof: Under these circumstances the T in the theorem is exactly $B - P$ because $A_{\mathfrak{p}}$ is a local ring.

Corollary 1.6.28. If S and T are two multiplicative subsets of A with $S \subset T$, then writing T' for the image of T in $S^{-1}A$, we have $(T')^{-1}S^{-1}A \simeq T^{-1}A$.

Proof: Consider the following commutative diagram:



1.7 Intergral Extension

Definition 1.7.1. Let B be a ring, A a subring of B (so that $1 \in A$). An element x of B is said to be integral over A if x is a root of a monic polynomial with coefficients in A, that is if x satisfies an equation of the form

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

where the a_4 are elements of A.

Proposition 1.7.2. The following are equivalent:

(1) $x \in B$ is integral over A;

(2) $A[x]$ is a finitely generated A-module;

(3) $A[x]$ is contained in a subring C of B such that C is a finitely generated A-module;

(4) There exists a faithful $A[x]$-module M which is finitely generated as an A-module.

Proposition 1.7.3. Let $x_i (1 \leqslant i \leqslant n)$ be elements of B, each integral over A. Then the ring $A[x_1, \ldots, x_n]$ is a finitely-generated A-module.

Proposition 1.7.4. The set C of elements of B which are integral over A is a subring of B containing A.

Definition 1.7.5. The ring C containing all the integral elements in B is called the integral closure of A in B. If $C = A$, then A is said to be integrally closed in B. If $C = B$, the ring B is said to be integral over A.

Proposition 1.7.6. Let $A \subseteq B \subseteq C$ be rings. Suppose that A is Noetherian, that C is finitely generated as an A-algebra and that C is either finitely generated as a B-module or integral over B. Then B is finitely generated as an A-algebra.

1.8 Flatness

Theorem 1.8.1 (Base Change)**.** If $f : A \to B$ is a ring homomorphism and M is a flat A-module, then $M_B = B \otimes_A M$ is a flat B-module.

Proof: By Theorem 1.2.20.

Theorem 1.8.2 (Localization)**.** $S^{-1}A$ is a flat A-module.

Proof: By Theorem 1.6.14.

Theorem 1.8.3 (Transitivity)**.** $f : A \to B$ is a ring homomorphism,B is flat A-module, N is flat B-module, then N is flat over A.

Proof: By Theorem 1.2.20.

Definition 1.8.4 (faithfully flat)**.**

1.9 Dimension Theory and Hilbert's Nullstellensatz

Definition 1.9.1. Let X be a topological space; we consider strictly decreasing (or strictly increasing) chains $Z_0, Z_1, \ldots, Z_r$ of length r of irreducible closed subsets of X. The supremum of the lengths, taken over all such chains, is called the combinatorial dimension of X and denoted $\dim X$. If X is a Noetherian space then there are no infinite strictly decreasing chains, but it can nevertheless happen that $\dim X = \infty$.

Let Y be a subspace of X. If $S \subset Y$ is an irreducible closed subset of Y then its closure in X is an irreducible closed subset $\bar{S} \subset X$ such that $\bar{S} \cap Y = S$(Analysis Point-set topology section). Indeed, if $\bar{S} = V \cup W$ with V and W closed in X then

$$S = \bar{S} \cap Y = (V \cap Y) \cup (W \cap Y)$$

, so that we may assume $S = V \cap Y$, but then $V = \bar{S}$. It follows easily from this that $\dim Y \leqslant \dim X$.

Let A be a ring. The supremum of the lengths r, taken over all strictly decreasing chains $\mathfrak{p}_0 \supset \mathfrak{p}_1 \supset \cdots \supset \mathfrak{p}_r$ of prime ideals of A, is called the Krull dimension, or simply the dimension of A, and denoted $\dim A$. It is clear that the Krull dimension of A is the same thing as the combinatorial dimension of $\operatorname{Spec} A$. For a prime ideal p of A, the supremum of the lengths, taken over all strictly decreasing chains of prime ideals $\mathfrak{p} = \mathfrak{p}_0 \supset \mathfrak{p}_1 \supset \cdots \supset \mathfrak{p}_r$ starting from $\mathfrak{p}$, is called the height of $\mathfrak{p}$, and denoted $\operatorname{ht} \mathfrak{p}$;. Moreover, the supremum of the lengths, taken over all strictly increasing chain of prime ideals $\mathfrak{p} = \mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_r$ starting from $\mathfrak{p}$, is called the coheight of p, and written $\operatorname{coht} p$. It follows from the definitions that

$$\operatorname{ht} \mathfrak{p} = \dim A_{\mathfrak{p}}, \quad \operatorname{coht} \mathfrak{p} = \dim A/\mathfrak{p} \text{ and } \operatorname{ht} \mathfrak{p} + \operatorname{coht} \mathfrak{p} \leqslant \dim A$$

Example 1.9.2. A is a Artinian ring, then $\dim A = 0$.

Proof: Since there's only a finite number of maximal ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$, and that the product of all of these is nilpotent. If then $\mathfrak{p}$ is a prime ideal, $\mathfrak{p} \supset (0) = (\mathfrak{p}_1 \ldots \mathfrak{p}_r)^v$, by Theorem 1.1.19 so that $\mathfrak{p} \supset \mathfrak{p}_i$ for some i; hence, $\mathfrak{p} = \mathfrak{p}_i$, so that every prime ideal is maximal.

Example 1.9.3. A is Artinian if and only if A is Notherian and $\dim A = 0$

Definition 1.9.4. For an ideal I of a ring A we define the height of I to be the infimum of the heights of prime ideals containing I :

$$\operatorname{ht} I = \inf\{ \operatorname{ht} \mathfrak{p} \mid I \subset \mathfrak{p} \in \operatorname{Spec} A\}.$$

Here also we have the inequality

$$\operatorname{ht} I + \dim A/I \leqslant \dim A.$$

If M is an A-module we define the dimension of M by

$$\dim M = \dim(A/\operatorname{ann}(M)).$$

Proposition 1.9.5. If M is finitely generated then $\dim M$ is the combinatorial dimension of the closed subspace $\mathrm{Supp}(M) = V(\mathrm{ann}(M))$ of $\mathrm{Spec}\, A$.

Proof: By Proposition 1.4.8,

$$\dim M = \dim(A/ann(M)) = \dim V(ann(M))$$

Theorem 1.9.6 (Ratliff, 1972)**.** A strictly increasing (or decreasing) chain $\mathfrak{p}_0, \mathfrak{p}_1, \ldots$ of prime ideals is said to be saturated if there do not exist prime ideals strictly contained between any two consecutive terms. We say that A is a catenary ring if the following condition is satisfied; for any prime ideals $\mathfrak{p}$ and $\mathfrak{p}'$ of A with $\mathfrak{p} \subset \mathfrak{p}'$, there exists a saturated chain of prime ideals starting from $\mathfrak{p}$ and ending at $\mathfrak{p}'$, and all such chains have the same (finite) length.

If a local domain $(A, \mathfrak{m})$ is catenary then for any prime ideal p we have $\mathrm{ht}\, \mathfrak{p} + \mathrm{coht}\, \mathfrak{p} = \dim A$. Conversely, if A is a Noetherian local domain and this equality holds for all $\mathfrak{p}$ then A is catenary.

Theorem 1.9.7. Let k be a field, L an algebraic extension of k and $\alpha_1, \ldots, \alpha_n \in L$; then

(1) $k[\alpha_1, \ldots, \alpha_n] = k(\alpha_1, \ldots, \alpha_n)$.

(2) Write $\varphi : k[X_1, \ldots, X_n] \longrightarrow k(\alpha_1, \ldots, \alpha_n)$ for the homomorphism over k which maps X_i to α_i; then $\mathrm{Ker}\, \varphi$ is the maximal ideal generated by n elements of the form

$$f_1(X_1), f_2(X_1, X_2), \ldots, f_n(X_1, \ldots, X_n)$$

, where each f_i can be taken to be monic in X_i with coefficient in $k[X_1, \ldots, X_{i-1}]$

Proof: Let $g_i(X_i)$ be the monic minimal polynomial of α_i over $k(\alpha_1, \ldots, \alpha_{i-1})$, take a lift f_i of $g_i(X_i)$ in $k[X_1, \ldots, X_i]$ such that $\varphi(f_i) = g_i$. Then $\ker \varphi = (f_1, \ldots, f_n)$

Theorem 1.9.8. Let k be a field and domain A is an finitely generated k-algebra, if A is a field, then A is a finite extension of k.

Proof: Let $E = k[x_1, \ldots, x_n]$. If E is not algebraic over k, by Proposition 1.3.50, we can renumber the x_1 so that $x_1, \ldots, x_r$ are algebraically independent over k, where $r \geqslant 1$, and each of $x_{r+1}, \ldots, x_n$ is algebraic over the field $F = k(x_1, \ldots, x_r)$. Hence E is a finite algebraic extension of F and therefore finitely generated as an F-module. Applying Proposition 1.7.6 to $k \subseteq F \subseteq E$, it follows that F is a finitely generated k-algebra, say $F = k[y_1, \ldots, y_3]$. Each y_j is of the form f_j/g_j, where f_j and g_j are polynomials in $x_1, \ldots, x_r$. It contradicts to the fact that there are infinitely many irreducible polynomials in the ring $k[x_1, \ldots, x_r]$ (adapt Euclid's proof of the existence of infinitely many prime numbers).

Theorem 1.9.9. Let k be a field, and let m be any maximal ideal of the polynomial ring $k[X_1, \ldots, X_n]$; then the residue class field $k[X_1, \ldots, X_n]/m$ is algebraic over k. Hence m can be generated by n elements, and in particular if k is algebraically closed then m is of the form $m = (X_1 - \alpha_1, \ldots, X_n - \alpha_n)$ for $\alpha_i \in k$.

Proof: Set $k[X_1, \ldots, X_n]/m = K$, and write α_i for the image of X_i in K; then $K = k[\alpha_1, \ldots, \alpha_n]$. By the previous theorem, since K is a field it is algebraic over k, and then by Theorem 1.9.7, m is generated by n elements. If k is algebraically closed then $k = K$, so that each X_i is congruent modulo m to some $\alpha_i \in k$; then $(X_1 - \alpha_1, \ldots, X_n - \alpha_n) \subset m$. On the other hand $(X_1 - \alpha_1, \ldots, X_n - \alpha_n)$ is obviously a maximal ideal, so that equality must hold.

Theorem 1.9.10 (Hilbert's Nullstellensatz)**.** If k is algebracally closed, then

$$I(V(A)) = \sqrt{A}.$$

Proof: It is clear that $\sqrt{A} \subset I(V(A))$. The problem is to show the other inclusion. Put concretely this means the following: Let $A = (f_1, \ldots, f_m)$. If $g \in k[X_1, \ldots, X_n]$ satisfies:

$$\{f_1(a_1, \ldots, a_n) = \ldots = f_m(a_1, \ldots, a_n) = 0\} \Longrightarrow g(a_1, \ldots, a_n) = 0$$

then there is an integer ℓ and polynomials $h_1, \ldots, h_m$ such that

$$g^\ell(X) = \sum_{i=1}^{m} h_i(X) \cdot f_i(X).$$

To prove this, introduce the ideal

$$B = A \cdot k[X_1, \ldots, X_n, X_{n+1}] + (1 - g \cdot X_{n+1})$$

in $k[X_1, \ldots, X_{n+1}]$ where $A \cdot k[X_1, \ldots, X_n, X_{n+1}]$ be the ideal generated by A. There are 2 possibilities: either B is a proper ideal, or $B = k[X_1, \ldots, X_{n+1}]$. In the first case, let M be a maximal ideal in $k[X_1, \ldots, X_{n+1}]$ containing B. By Theorem 1.9.9,

$$M = (X_1 - a_1, \ldots, X_n - a_n, X_{n+1} - a_{n+1})$$

for some elements $a_i \in k$. Since M is the kernel of the homomorphism:

$$\begin{aligned} k[X_1, \ldots, X_n, X_{n+1}] &\longrightarrow k \\ f &\longmapsto f(a_1, \ldots, a_{n+1}), \end{aligned}$$

$B \subset M$ means that:

$$f_1(a_1, \ldots, a_n) = \ldots = f_m(a_1, \ldots, a_n) = 0 \tag{1.1}$$

and

$$1 = g(a_1, \ldots, a_n) \cdot a_{n+1}.$$

But by our assumptionon g, (1.1) implies that $g(a_1, \ldots, a_n) = 0$.A contradiction! Hence we can only conclude that the ideal B would not have been a proper ideal.

But then $1 \in B$. This means that there are polynomials $h_1, \ldots, h_m, h_{m+1} \in k[X_1, \ldots, X_{n+1}]$ such that:

$$\begin{aligned} 1 = &\sum_{i=1}^{m} h_i(X_1, \ldots, X_{m+1}) \cdot f_i(X_1, \ldots, X_n) \\ &+ (1 - g(X_1, \ldots, X_n) \cdot X_{n+1}) \cdot h_{m+1}(X_1, \ldots, X_{n+1}). \end{aligned}$$

Substituting g^{-1} for X_{n+1} in this formula, we get:

$$1 = \sum_{i=1}^{m} h_i\left(X_1, \ldots, X_n, 1/g\right) \cdot f_i\left(X_1, \ldots, X_n\right).$$

Clearing denominators, this gives:

$$g^{\ell}\left(X_1, \ldots, X_n\right) = \sum_{i=1}^{m} h_i^*\left(X_1, \ldots, X_n\right) \cdot f_i\left(X_1, \ldots, X_n\right)$$

for some new polynomials $h_i^* \in k\left[X_1, \ldots, X_n\right]$, i.e., $g \in \sqrt{A}$.

Theorem 1.9.11. If k is algebraically closed, then there is a one-to-one inclusion-reversing correspondence between algebraic sets(irreducible algebraic sets, points) in $\mathbf{A}^n$ and radical ideals(prime ideals, maximal ideals) in A, given by $Y \mapsto I(Y)$ and $\mathfrak{a} \mapsto Z(\mathfrak{a})$.

Proof: By Theorem 1.4.19 and Hilbert's Nullstellensatz.

Theorem 1.9.12. Let k be a field and A an integral domain which is finitely generated over k. Define the transcendental degree of A to be transcendence degree of extension $\mathrm{Frac}(A)/k$. For convenience, we denote it by $\deg_k A$.

$$\dim A = \mathrm{tr} \cdot \deg_k A$$

Proof: Let $A = k\left[X_1, \ldots, X_n\right]/P$, and set $r = \mathrm{tr} \cdot \deg_k A$. To prove that $r \geqslant \dim A$ it is enough to show that if P and Q are prime ideals of $k[X] = k\left[X_1, \ldots, X_n\right]$ with $Q \supset P$ and $Q \neq P$ then

$$\mathrm{tr}\,.\deg_k k[X]/Q < \mathrm{tr}\,.\deg_k k[X]/P.$$

The k-algebra homomorphism $k[X]/P \longrightarrow k[X]/Q$ is onto, so that $\mathrm{tr}.\ \deg_k k[X]/Q \leqslant \mathrm{tr}\,.\deg_k k[X]/P$ is obvious. Suppose that equality holds. Let $k[X]/P = k\left[\alpha_1, \ldots, \alpha_n\right]$ and $k[X]/Q = k\left[\beta_1, \ldots, \beta_n\right]$.

By Proposition 1.3.50, we may assume that $\beta_1, \ldots, \beta_r$ is a transcendence basis for $k(\beta_1, \ldots, \beta_n)/k$. Then $\alpha_1, \ldots, \alpha_r$ are also algebraically independent over k, so that they form a transcendence basis for $k(\alpha_1, \ldots, \alpha_n)$ over k. Now set $S = k\left[X_1, \ldots, X_r\right] - \{0\}$; S is a multiplicative set in $k[X_1, \ldots, X_n]$ with $P \cap S = \varnothing$ and $Q \cap S = \varnothing$. Setting $R = k\left[X_1, \ldots, X_n\right]$ and $K = k\left(X_1, \ldots, X_r\right)$, we have $R_S \simeq K\left[X_{r+1}, \ldots, X_n\right]$, and

$$R_S/PR_S \simeq S^{-1}A \simeq k\left(\alpha_1, \ldots, \alpha_r\right)\left[\alpha_{r+1}, \ldots, \alpha_n\right]$$

so that R_S/PR_S is algebraic over $K = k\left(X_1, \ldots, X_r\right) \simeq k\left(\alpha_1, \ldots, \alpha_r\right)$, and therefore PR_S is a maximal ideal of R_S. Similarly, QR_S is a maximal ideal of R_S. This contradicts to Proposition 1.6.8.

Now let us prove that $r \leqslant \dim A$ by induction on r. If $r = 0$ then, by Theorem 1.9.8, A is a field, so $\dim A = 0$ and the assertion holds. Now let $r > 0$, and suppose that $A = k\left[\alpha_1, \ldots, \alpha_n\right]$ with α_1 transcendental over k; setting $S = k\left[X_1\right] - \{0\}$ and $R = k\left[X_1, \ldots, X_n\right]$ we get

$$R_S = k\left(X_1\right)\left[X_2, \ldots, X_n\right] \text{ and } R_S/PR_S \simeq k\left(\alpha_1\right)\left[\alpha_2, \ldots, \alpha_n\right].$$

Hence R_S/PR_S has transcendence degree $r-1$ over $k(X_1)$, so that by induction $\dim R_S/PR_S \geqslant r-1$. Thus there exists a strictly increasing chain $PR_S = Q_0 \subset Q_1 \subset \cdots \subset Q_{r-1}$ of prime ideals of R_S. If we set $P_i = \varphi_S^{-1}(Q_i)$ then P_i is a prime ideal of R disjoint from S; in particular, the residue class of X_1 in fractional field of R/P_{r-1} is not algebraic over k, and so $\mathrm{tr.deg}_k R/P_{r-1} > 0$. Then P_{r-1} is not a maximal ideal of R by Theorem 1.9.8, and therefore R has a maximal ideal P_r strictly bigger than P_{r-1}. Hence $\dim A = \operatorname{coht} P \geqslant r$.

1.10 Completion

Definition 1.10.1. Let A be a ring and M an A-module; for a directed set Λ, suppose that $\mathscr{F} = \{M_\lambda\}_{\lambda\in\Lambda}$ is a family of submodules of M indexed by Λ and such that $\lambda < \mu \Rightarrow M_\lambda \supset M_\mu$. Then $\mathscr{F}$ is a family of subgroups of M containing 0 and making M into a topological group under addition. In this topology, for any $x \in M$ a system of neighbourhoods of x is given by $\{x + M_\lambda\}_{\lambda\in\Lambda}$. In addition, when $M = A$, each M_λ is an ideal, then multiplication is also continuous:

$$(a + M_\lambda)(b + M_\lambda) \subset ab + M_\lambda.$$

This type of topology is called a linear topology on M. Each $M_\lambda \subset M$ is an open set, each coset $x + M_\lambda$ is again open, and the complement $M - M_\lambda$ of M_λ is a union of cosets, so is also open. Hence M_λ is an open and closed subset; the quotient module M/M_λ is then discrete in the quotient topology.

Definition 1.10.2. Since for $\lambda < \mu$ there is a natural linear map $\varphi_\lambda^\mu : M/M_\mu \longrightarrow M/M_\lambda$, we can construct the inverse system $\{M/M_\lambda; \varphi_{\lambda\mu}\}$ of A-modules; its inverse limit $\varprojlim M/M_\lambda$ is called the completion of M, and is written $\hat{M}$. We give each M/M_λ the discrete topology, the direct product $\prod_\lambda M/M_\lambda$ the product topology, and $\hat{M}$ the subspace topology in $\prod_\lambda M/M_\lambda$($\hat{M}$ is the set of the coherent sequences). Let $\psi : M \longrightarrow \hat{M}$ be the natural A-linear map;

Proposition 1.10.3. ψ is continuous, and $\psi(M)$ is dense in $\hat{M}$. If ψ is an isomorphism, we say A is complete.

Proof: Since that I is directed, we can choose a common ancestor for finite many elements $a_\lambda + M_\lambda$.

Proposition 1.10.4. ψ is injective if and only if M is Hausdorff if and only if $\bigcap_\lambda M_\lambda = 0$.

Theorem 1.10.5. Write $p_\lambda : \hat{M} \longrightarrow M/M_\lambda$ for the projection, and set $\operatorname{Ker} p_\lambda = M_\lambda^*$, then the topology of $\hat{M}$ coincides with the linear topology defined by $\mathscr{F} = \{M_\lambda^*\}_{\lambda\in\Lambda}$.

Proof: Notice that

$$M_\lambda^* = (\{0 + M_\lambda\} \times \prod_{\mu\neq\lambda} M/M_\mu) \cap \hat{M}$$

.

Lemma 1.10.6 (Artin-Rees lemma)**.** Let A be a Noetherian ring, M a finite A-module, $N \subset M$ a submodule, and I an ideal of A. Then there exists a positive integer c such that for every $n > c$, we have

$$I^n M \cap N = I^{n-c}(I^c M \cap N)$$

Proof:

Chapter 2

Homological Algerba

2.1 Basic Definition in Category

Definition 2.1.1 (Category)**.** A category $\mathcal{C}$ consists of three ingredients: a class obj $(\mathcal{C})$ of objects, a set of morphisms $\mathrm{Hom}(A, B)$ for every ordered pair (A, B) of objects, and composition $\mathrm{Hom}(A, B) \times \mathrm{Hom}(B, C) \to \mathrm{Hom}(A, C)$, denoted by

$$(f, g) \mapsto gf$$

for every ordered triple A, B, C of objects. [We often write $f : A \to B$ or $A \xrightarrow{f} B$ instead of $f \in \mathrm{Hom}(A, B)$.] These ingredients are subject to the following axioms:

(1) the Hom sets are pairwise disjoint; that is, each $f \in \mathrm{Hom}(A, B)$ has a unique domain A and a unique target B;

(2) for each object A, there is an identity morphism $1_A \in \mathrm{Hom}(A, A)$ such that $f1_A = f$ and $1_B f = f$ for all $f : A \to B$;

(3) composition is associative: given morphisms $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$, then

$$h(gf) = (hg)f$$

Definition 2.1.2 (Subcategory)**.** A category $\mathcal{S}$ is a subcategory of a category $\mathcal{C}$ if

(1) $\mathrm{obj}(\mathcal{S}) \subseteq \mathrm{obj}(\mathcal{C})$

(2) $\mathrm{Hom}_{\mathcal{S}}(A, B) \subseteq \mathrm{Hom}_{\mathcal{C}}(A, B)$ for all $A, B \in \mathrm{obj}(\mathcal{S})$, where we denote Hom sets in $\mathcal{S}$ by $\mathrm{Hom}_{\mathcal{S}}(\square, \square)$,

(3) if $f \in \mathrm{Hom}_{\mathcal{S}}(A, B)$ and $g \in \mathrm{Hom}_{\mathcal{S}}(B, C)$, then the composite $gf \in \mathrm{Hom}_{\mathcal{S}}(A, C)$ is equal to the composite $gf \in \mathrm{Hom}_{\mathcal{C}}(A, C)$,

(4) if $A \in \mathrm{obj}(\mathcal{S})$, then the identity $1_A \in \mathrm{Hom}_{\mathcal{S}}(A, A)$ is equal to the identity $1_A \in \mathrm{Hom}_{\mathcal{C}}(A, A)$. A subcategory $\mathcal{S}$ of $\mathcal{C}$ is a full subcategory if, for all $A, B \in \mathrm{obj}(\mathcal{S})$, we have $\mathrm{Hom}_{\mathcal{S}}(A, B) = \mathrm{Hom}_{\mathcal{C}}(A, B)$.

A subcategory $\mathcal{S}$ of $\mathcal{C}$ is a full subcategory if, for all $A, B \in \text{obj}(\mathcal{S})$, we have $\text{Hom}_{\mathcal{S}}(A, B) = \text{Hom}_{\mathcal{C}}(A, B)$.

Definition 2.1.3. For every category $\mathcal{C}$ the opposite category, denoted by $\mathcal{C}^{\text{opp}}$, is the category with the same objects as $\mathcal{C}$ and where for two objects X and Y of $\mathcal{C}^{\text{opp}}$ we set $\text{Hom}_{\mathcal{C}^{\text{opp}}}(X, Y) := \text{Hom}_{\mathcal{C}}(Y, X)$ with the obvious composition law.

Definition 2.1.4 (covariant functor)**.** If $\mathcal{C}$ and $\mathcal{D}$ are categories, then a covariant functor $T : \mathcal{C} \to \mathcal{D}$ is a function such that

(1) if $A \in \text{obj}(\mathcal{C})$, then $T(A) \in \text{obj}(\mathcal{D})$,

(2) if $f : A \to A'$ in $\mathcal{C}$, then $T(f) : T(A) \to T(A')$ in $\mathcal{D}$,

(3) if $A \xrightarrow{f} A' \xrightarrow{g} A''$ in $\mathcal{C}$, then $T(A) \xrightarrow{T(f)} T(A') \xrightarrow{T(g)} T(A'')$ in $\mathcal{D}$ and

$$T(gf) = T(g)T(f),$$

(4) $T(1_A) = 1_{T(A)}$ for every $A \in \text{obj}(\mathcal{C})$.

Definition 2.1.5 (contravariant functor)**.** A contravariant functor from $\mathcal{C}$ to $\mathcal{D}$ is by definition a covariant functor $F : \mathcal{C}^{\text{opp}} \to \mathcal{D}$, where $\mathcal{C}^{\text{opp}}$ is the opposite category of $\mathcal{C}$. Sometimes we use the notation $F : \mathcal{C} \to \mathcal{D}$ for a contravariant functor, in which case we explicitly state that F is contravariant.

Definition 2.1.6 (faithful functor)**.** A functor $T : \mathcal{C} \to \mathcal{D}$ is faithful if, for all $A, B \in \text{obj}(\mathcal{C})$, the functions $\text{Hom}_{\mathcal{C}}(A, B) \to \text{Hom}_{\mathcal{D}}(TA, TB)$ given by $f \mapsto Tf$ are injections.

Definition 2.1.7 (isomorphism)**.** A morphism $f : A \to B$ in a category $\mathcal{C}$ is an isomorphism if there exists a morphism $g : B \to A$ in $\mathcal{C}$ with

$$gf = 1_A \quad \text{and} \quad fg = 1_B.$$

The morphism g is called the inverse of f.

Definition 2.1.8 (natural transformation)**.** Let $S, T : \mathcal{A} \to \mathcal{B}$ be covariant functors. A natural transformation $\tau : S \to T$ is a one-parameter family of morphisms in $\mathcal{B}$,

$$\tau = (\tau_A : SA \to TA)_{A \in \text{obj}(\mathcal{A})},$$

making the following diagram commute for all $f : A \to A'$ in $\mathcal{A}$:

$$\begin{array}{ccc} SA & \xrightarrow{\tau_A} & TA \\ {\scriptstyle Sf}\downarrow & & \downarrow{\scriptstyle Tf} \\ SA' & \xrightarrow[\tau_{A'}]{} & TA' \end{array}$$

A natural isomorphism is a natural transformation τ for which each τ_A is an isomorphism.

Proposition 2.1.9. Natural transformations can be composed. If $\tau : S \to T$ and $\sigma : T \to U$ are natural transformations, where $S, T, U : \mathcal{A} \to \mathcal{B}$ are functors of the same variance, then define $\sigma\tau : S \to U$ by

$$(\sigma\tau)_A = \sigma_A \tau_A$$

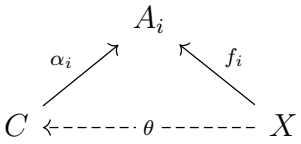
for all $A \in \text{obj}(\mathcal{A})$. It is easy to check that $\sigma\tau$ is a natural transformation

For any functor $S : \mathcal{A} \to \mathcal{B}$, define the identity natural transformation $\omega_S : S \to S$ by setting $(\omega_S)_A : SA \to SA$ to be the identity morphism 1_{SA}. The reader may check, using Exercise 1.15, that a natural transformation $\tau : S \to T$ is a natural isomorphism if and only if there is a natural transformation $\sigma : T \to S$ with $\sigma\tau = \omega_S$ and $\tau\sigma = \omega_T$.

Definition 2.1.10 (initial object)**.** An object A in a category $\mathcal{C}$ is called an initial object if, for every object X in $\mathcal{C}$, there exists a unique morphism $A \to X$. Any two initial objects in a category $\mathcal{C}$, should they exist, are isomorphic.

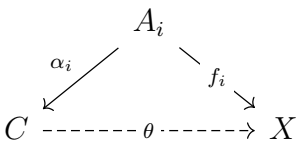
Definition 2.1.11 (terminal object)**.** An object Ω in a category $\mathcal{C}$ is called a terminal object if, for every object C in $\mathcal{C}$, there exists a unique morphism $X \to \Omega$.Any two terminal objects in a category $\mathcal{C}$, should they exist, are isomorphic.

Definition 2.1.12 (product)**.** Let $\mathcal{C}$ be a category, and let $(A_i)_{i\in I}$ be a family of objects in $\mathcal{C}$ indexed by a set I. A product is an ordered pair $\big(C, (p_i : C \to A_i)_{i\in I}\big)$, consisting of an object C and a family $(p_i : C \to A_i)_{i\in I}$ of projections, that is a solution to the following universal mapping problem: for every object X equipped with morphisms $f_i : X \to A_i$, there exists a unique morphism $\theta : X \to C$ making the diagram commute for each i.



Should it exist, a product is denoted by $\prod_{i\in I} A_i$, and it is unique to isomorphism, for it is a terminal object in a suitable category.

Definition 2.1.13 (coproduct)**.** Let $\mathcal{C}$ be a category, and let $(A_i)_{i\in I}$ be a family of objects in $\mathcal{C}$ indexed by a set I. A coproduct is an ordered pair $\big(C, (\alpha_i : A_i \to C)_{i\in I}\big)$, consisting of an object C and a family $(\alpha_i : A_i \to C)_{i\in I}$ of morphisms, called injections, that is a solution to the following universal mapping problem: for every object X equipped with morphisms $(f_i : A_i \to X)_{i\in I}$, there exists a unique morphism $\theta : C \to X$ making the diagram commute for each i.



Should it exist, a coproduct is usually denoted by $\bigsqcup_{i\in I} A_i$ (the injections are not mentioned). A coproduct is unique to isomorphism, for it is an initial object in a suitable category.

Example 2.1.14 (coproduct in category of topological space)**.** $(X_i)_{i\in I}$ be a family of topological space, $f_i : X_i \to X$ be a family of continuous map. $\bigsqcup_{i\in I} A_i = \left\{(a_i, i) \in \left(\bigcup_{i\in I} A_i\right) \times I : a_i \in A_i\right\}$ be the disjoint union of $(X_i)_{\in I}$. Define U open in $\bigsqcup_{i\in I} A_i$ if and only if $f_i^{-1}(U)$ open in X_i for all $i \in I$. Then $\bigsqcup_{i\in I} A_i$ with continous maps $\alpha_i : a_i \mapsto (a_i, i)$ is the coproduct of a family of topological space.

Example 2.1.15 (coproduct in k-aglebra)**.** If F is a commutative ring and $(A_i)_{i\in I}$ is a family of F-algebra, we can define the tensor product of all these F-algebra

$$\bigotimes_{i\in I} A_i$$

to be the quotient of the F-vector space with basis $\prod_{i\in I} A_i$ by the subspace generated by elements of the form:

(1) $(x_i) + (y_i) - (z_i)$ with $x_j + y_j = z_j$ for one $j \in I$ and $x_i = y_i = z_i$ for all $i \neq j$

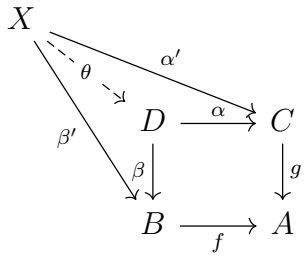
(2) $(x_j) - a\,(y_i)$ with $x_j = ay_j$ for one $j \in I$ and $x_i = y_i$ for all $i \neq j$

It can be made into a commutative F-algebra in an obvious fashion, and there are canonical homomorphisms

$$A_i \to \bigotimes_{i\in I} A_i$$

of F-algebras. Then by universal property of tensor product, the tensor product of all these F-algebra is the coproduct of A_i.

Definition 2.1.16 (pushback/fibered product)**.** Given two morphisms $f : B \to A$ and $g : C \to A$ in a category $\mathcal{C}$, a pullback (or fibered product) is a triple (D, α, β) with $g\alpha = f\beta$ that is a solution to the universal mapping problem: for every (X, α', β') with $g\alpha' = f\beta'$, there exists a unique morphism $\theta : X \to D$ making the diagram commute.

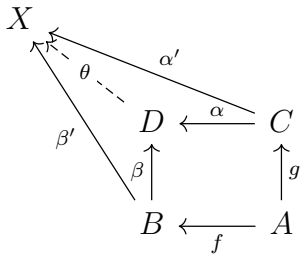


The pullback is often denoted by $B\sqcap_A C$.Pullbacks, when they exist, are unique to isomorphism, for they are terminal objects in a suitable category.

Example 2.1.17 (fibered product in topological space)**.** A, B, C be topological spaces, $f : B \to A, g : C \to A$ be continuous maps, $D = \{(b, c) \in B \times C : f(b) = g(c)\}$ be the fibered product of

Definition 2.1.18 (pushout/fibered coproduct)**.** Given two morphisms $f : A \to B$ and $g : A \to C$ in a category $\mathcal{C}$, a pushout (or fibered sum) is a triple (D, α, β) with $\beta g = \alpha f$ that is

a solution to the universal mapping problem: for every triple (Y, α', β') with $\beta' g = \alpha' g$, there exists a unique morphism $\theta : D \to Y$ making the diagram commute. The pushout is often denoted by $B \cup_A C$.

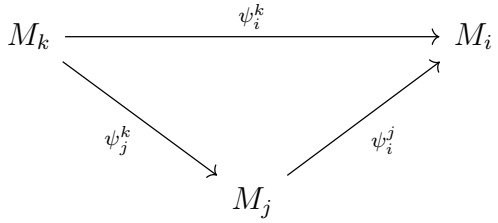


Pushouts are unique to isomorphism when they exist, for they are initial objects in a suitable category.

Example 2.1.19. In category of Commutative Rings, $f : A \to B, g : A \to B$ be ring homomorphism, then the pushout is given by tensor product of A-algebra B and A-algebra C and homorphism:

$$\begin{aligned} \beta : & B \to B \otimes_A C & \qquad \alpha : & C \to B \otimes_A C \\ & b \mapsto b \otimes 1 & & c \mapsto 1 \otimes c \end{aligned}$$

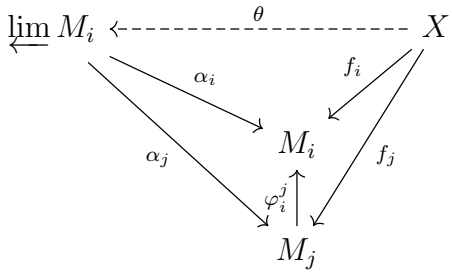
Definition 2.1.20 (inverse system)**.** Given a partially ordered set I and a category $\mathcal{C}$, an inverse system in $\mathcal{C}$ is an ordered pair $\left((M_i)_{i\in I}, \left(\psi_i^j\right)_{j\succeq i}\right)$, abbreviated $\left\{M_i, \psi_i^j\right\}$, where $(M_i)_{i\in I}$ is an indexed family of objects in $\mathcal{C}$ and $\left(\psi_i^j : M_j \to M_i\right)_{j\succeq i}$ is an indexed family of morphisms for which $\psi_i^i = 1_{M_i}$ for all i, and such that the following diagram commutes whenever $k \succeq j \succeq i$.



Definition 2.1.21 (inverse limit)**.** Let I be a partially ordered set, let $\mathcal{C}$ be a category, and let $\left\{M_i, \psi_i^j\right\}$ be an inverse system in $\mathcal{C}$ over I. The inverse limit (also called projective limit or limit) is an object $\varprojlim M_i$ and a family of projections $\left(\alpha_i : \varprojlim M_i \to M_i\right)_{i\in I}$ such that:

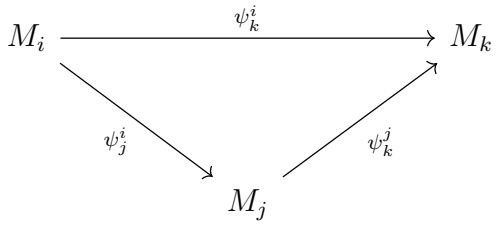
(1) $\psi_i^j \alpha_j = \alpha_i$ whenever $i \preceq j$,

(2) for every $X \in \mathrm{obj}(\mathcal{C})$ and all morphisms $f_i : X \to M_i$ satisfying $\psi_i^j f_j = f_i$ for all $i \preceq j$, there exists a unique morphism $\theta : X \to \varprojlim M_i$ making the diagram commute.



Example 2.1.22. In the category of topological group, inverse limit exists. Inverse limit of Finite discrete group is called pro-finite group. A topological group is pro-finite group if and only if it is totally disconnected and compact.

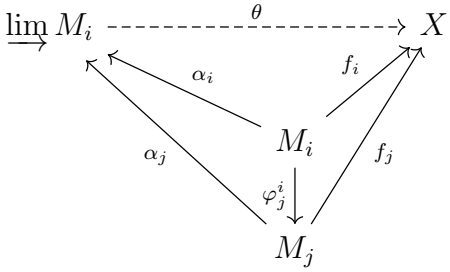
Definition 2.1.23 (direct system)**.** Given a partially ordered set I and a category $\mathcal{C}$, a direct system in $\mathcal{C}$ is an ordered pair $\left((M_i)_{i\in I}, \left(\varphi^i_j\right)_{i\preceq j}\right)$, abbreviated $\left\{M_i, \varphi^i_j\right\}$, where $(M_i)_{i\in I}$ is an indexed family of objects in $\mathcal{C}$ and $\left(\varphi^i_j : M_j \to M_i\right)_{i\preceq j}$ is an indexed family of morphisms for which $\varphi^i_i = 1_{M_i}$ for all i, and such that the following diagram commutes whenever $i \preceq j \preceq k$.



Definition 2.1.24 (direct limit)**.** Let I be a partially ordered set, let $\mathcal{C}$ be a category, and let $\left\{M_i, \varphi^i_j\right\}$ be a direct system in $\mathcal{C}$ over I. The direct limit (also called inductive limit or colimit) is an object $\varinjlim M_i$ and insertion morphisms $\left(\alpha_i : M_i \to \varinjlim M_i\right)_{i\in I}$.

(1) $\alpha_j\varphi^i_j = \alpha_i$ whenever $i \preceq j$,

(2) Let $X \in \mathrm{obj}(\mathcal{C})$, and let there be given morphisms $f_i : M_i \to X$ satisfying $f_j\varphi^i_j = f_i$ for all $i \preceq j$. There exists a unique morphism $\theta : \varinjlim M_i \to X$ making the diagram commute.



Example 2.1.25. M is a smooth manifold, $p \in M$, $C^\infty_p(M)$ be the germ of smooth function at p, then $C^\infty_p(M)$ is the direct limit of the direct system $\left\{(C^\infty(U))_{p\in U \text{ open in } M}, (\mathrm{res}^U_V)_{V\subset U}\right\}$ where res be the restriction map from the bigger open subset to the smaller one.

Definition 2.1.26. Recall that a direct system $\left\{A_i, \alpha^i_j\right\}$ in a category $\mathcal{C}$ over a partially ordered index set I can be construed as a covariant functor $A : I \to \mathcal{C}$, where $A(i) = A_i$ and $A\left(\kappa^i_j\right) = \alpha^i_j$.

Let $A = \left\{A_i, \alpha^i_j\right\}$ and $B = \left\{B_i, \beta^i_j\right\}$ be direct systems over the same (not necessarily directed) index set I. A morphism of direct systems is a natural transformation $r : A \to B$.

if the direct limit of these two direct system exist, by universal property of direct limit, r induce a morphism between $\varinjlim A_i$ and $\varinjlim B_i$

Proposition 2.1.27. Let I be a directed set, and let $\left\{A_i, \alpha^i_j\right\}, \left\{B_i, \beta^i_j\right\}$, and $\left\{C_i, \gamma^i_j\right\}$ be direct systems of left R-modules over I. If : $\left\{A_i, \alpha^i_j\right\} \to \left\{B_i, \beta^i_j\right\}$ and $s : \left\{B_i, \beta^i_j\right\} \to \left\{C_i, \gamma^i_j\right\}$ are morphisms of direct systems, and if

$$0 \to A_i \xrightarrow{r_i} B_i \xrightarrow{s_i} C_i \to 0$$

is exact for each $i \in I$, then there is an exact sequence

$$0 \to \varinjlim A_i \xrightarrow{\vec{r}} \varinjlim B_i \xrightarrow{\vec{s}} \varinjlim C_i \to 0$$

Definition 2.1.28. A inverse system can by viewed as a functor from opposite category of partially ordered set to category $\mathcal{C}$. A morphism between inverse system is a natrual transformation between inverse system.

Let $A = \left\{A_i, \alpha_j^i\right\}$ and $B = \left\{B_i, \beta_j^i\right\}$ be inverse systems over the same index set I, assume the direct limit of these two direct system exist, a natural transformation $r : A \to B$ induce a morphism by between $\varprojlim A_i$ and $\varprojlim B_i$

Proposition 2.1.29. In ${}_R\,\mathrm{Mod}$, let $r : \left\{A_i, \alpha_j^i\right\} \to \left\{B_i, \beta_j^i\right\}$ and $s : \left\{B_i, \beta_j^i\right\} \to \left\{C_i, \gamma_j^i\right\}$ be morphisms of inverse systems over any (not necessarily directed) index set I. If

$$0 \to A_i \xrightarrow{r_i} B_i \xrightarrow{s_i} C_i$$

is exact for each $i \in I$, prove that there are homomorphisms $\overleftarrow{r}, \overleftarrow{s}$ given by the universal property of inverse limits, and an exact sequence

$$0 \to \varprojlim A_i \xrightarrow{\vec{r}} \varprojlim B_i \xrightarrow{\vec{s}} \varprojlim C_i \to 0$$

Definition 2.1.30. A covariant functor $F : \mathcal{A} \to \mathcal{C}$ preserves direct limits if, whenever $\left(\varinjlim A_i, \left(\alpha_i : A_i \to \varinjlim A_i\right)\right)$ is a direct limit of a direct system $\left\{A_i, \varphi_j^i\right\}$ in $\mathcal{A}$, then $\left(F\left(\varinjlim A_i\right), \left(F\alpha_i : FA_i \to F\left(\varinjlim A_i\right)\right)\right)$ is a direct limit of the direct system $\left\{FA_i, F\varphi_j^i\right\}$ in $\mathcal{C}$.

A covariant functor $F : \mathcal{A} \to \mathcal{C}$ preserves inverse limits if, whenever $\left(\varprojlim A_i, (\alpha_i : \lim A_i \to A_i)\right)$ is an inverse limit of an inverse system $\left\{A_i, \psi_i^j\right\}$ in $\mathcal{A}$, then $\left(F\left(\varprojlim A_i\right), \left(F\alpha_i : F\left(\varprojlim A_i\right) \to FA_i\right)\right)$ is an inverse limit of the inverse system $\left\{FA_i, F\psi_i^j\right\}$ in $\mathcal{C}$.

Definition 2.1.31. Let $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{D} \to \mathcal{C}$ be covariant functors. The ordered pair (F, G) is an adjoint pair if, for each $C \in \mathrm{obj}(\mathcal{C})$ and $D \in \mathrm{obj}(\mathcal{D})$, there are bijections

$$\tau_{C,D} : \mathrm{Hom}_{\mathcal{D}}(FC, D) \to \mathrm{Hom}_{\mathcal{C}}(C, GD)$$

such that the following diagram commute:

$$\begin{array}{ccc}
\mathrm{Hom}_{\mathcal{D}}(FC, D) & \xrightarrow{(Ff)^*} & \mathrm{Hom}_{\mathcal{D}}\left(FC', D\right) \\
\Big\downarrow{\scriptstyle \tau_{C,D}} & & \Big\downarrow{\scriptstyle \tau_{C',D}} \\
\mathrm{Hom}_{\mathcal{C}}(C, GD) & \xrightarrow[f^*]{} & \mathrm{Hom}_{\mathcal{C}}\left(C', GD\right)
\end{array}$$

$$\begin{array}{ccc}
\mathrm{Hom}_{\mathcal{D}}(FC, D) & \xrightarrow{(g)^*} & \mathrm{Hom}_{\mathcal{D}}\left(FC, D'\right) \\
\Big\downarrow{\scriptstyle \tau_{C,D}} & & \Big\downarrow{\scriptstyle \tau_{C,D'}} \\
\mathrm{Hom}_{\mathcal{C}}(C, GD) & \xrightarrow[(Gg)_*]{} & \mathrm{Hom}_{\mathcal{C}}\left(C, GD'\right)
\end{array}$$

Example 2.1.32 (Hom and Tensor)**.** If $B = {}_RB_S$ is a bimodule, $\square \otimes_R B : \mathrm{Mod}_R \to \mathrm{Mod}_S$ and $\mathrm{Hom}_S(B, \square) : \mathrm{Mod}_S \to \mathrm{Mod}_R$ be two functors. then $(\square \otimes_R B, \mathrm{Hom}_S(B, \square))$ is an adjoint pair. Similarly, if $B = {}_SB_R$ is a bimodule, $B \otimes_R \square :_R \mathrm{Mod} \to_S \mathrm{Mod}$ and $\mathrm{Hom}_S(B, \square) :_S \mathrm{Mod} \to_R \mathrm{Mod}$ be two functors. then $(B \otimes_R \square, \mathrm{Hom}_S(B, \square))$ is an adjoint pair.

Example 2.1.33 (Free and Forget)**.**

Example 2.1.34 (Induced Representation)**.** G is a finite group, H be a subgroup of G, then $\mathbb{C}[G]$ be a $(\mathbb{C}[G], \mathbb{C}[H])$ bi-module, funcotr $\mathbb{C}[G] \otimes_{\mathbb{C}[H]} \square :_{\mathbb{C}[H]} \mathrm{Mod} \to_{\mathbb{C}[G]} \mathrm{Mod}$ and funcotr $\mathrm{Hom}_{\mathbb{C}[G]}(\mathbb{C}[G], \square)$ be an adjoint pair, since $\mathrm{Hom}_{\mathbb{C}[G]}(\mathbb{C}[G], \square) \simeq \mathrm{Res}^{\mathbb{C}[G]}_{\mathbb{C}[H]}$(Restriction from $\mathbb{C}[G]$-module to $\mathbb{C}[H]$-module), we have $(\mathbb{C}[G] \otimes_{\mathbb{C}[H]} \square, \mathrm{Res}^{\mathbb{C}[G]}_{\mathbb{C}[H]})$ is an adjoint pair.

Proposition 2.1.35. Let (F, G) be an adjoint pair offunctors, where $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{D} \to \mathcal{C}$. Then F preserves direct limits and G preserves inverse limits.

2.2 Abelian Category

Definition 2.2.1 (additive category)**.** A category $\mathcal{C}$ is additive if

(1) $\mathrm{Hom}(A, B)$ is an (additive) abelian group for every $A, B \in \mathrm{obj}(\mathcal{C})$,

(2) composition map
$$\mathrm{Hom}(A, B) \times \mathrm{Hom}(B, C) \to \mathrm{Hom}(A, C)$$
is $\mathbb{Z}$-bilinear.

(3) $\mathcal{C}$ has a zero object (a zero object is an object that is both initial and terminal),

(4) $\mathcal{C}$ has finite products and finite coproducts: for all objects A, B in $\mathcal{C}$, both $A \sqcap B$ and $A \sqcup B$ exist in $\mathrm{obj}(\mathcal{C})$.

Definition 2.2.2 (Additive Functor)**.** If $\mathcal{C}$ and $\mathcal{D}$ are additive categories, a functor $T : \mathcal{C} \to \mathcal{D}$ (of either variance) is additive if, for all A, B and all $f, g \in \mathrm{Hom}(A, B)$, we have

$$T(f + g) = Tf + Tg;$$

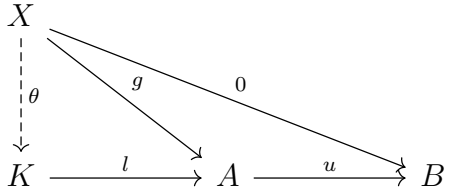
that is, the function $\mathrm{Hom}_{\mathcal{C}}(A, B) \to \mathrm{Hom}_{\mathcal{D}}(TA, TB)$, given by $f \mapsto Tf$, is a homomorphism of abelian groups.

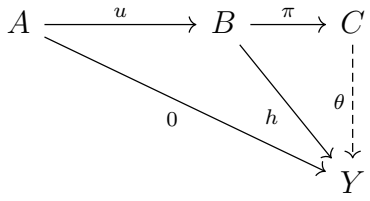
Proposition 2.2.3. If $\mathcal{C}$ and $\mathcal{D}$ are additive categories and $T : \mathcal{C} \to \mathcal{D}$ is an additive functor of either variance, then $T(A \oplus B) \cong T(A) \oplus T(B)$ for all $A, B \in \mathrm{obj}(\mathcal{C})$.

Definition 2.2.4. A morphism $u : B \to C$ in a category $\mathcal{C}$ is a monomorphism (or is monic) if u can be canceled from the left; that is, for all objects A and all morphisms $f, g : A \to B$, we have that $uf = ug$ implies $f = g$.
$$A \underset{g}{\overset{f}{\rightrightarrows}} B \xrightarrow{u} C$$

Definition 2.2.5. A morphism $v : B \to C$ in a category $\mathcal{C}$ is an epimorphism (or is epic) if v can be canceled from the right; that is, for all objects D and all morphisms $h, k : C \to D$, we have that $hv = kv$ implies $h = k$.
$$B \xrightarrow{v} C \underset{k}{\overset{h}{\rightrightarrows}} D$$

Definition 2.2.6 (kernel,cokernel)**.** Definition. If $u : A \to B$ is a morphism in an additive category $\mathcal{A}$, then its kernel $\ker u$ is a morphism $i : K \to A$ that satisfies the following universal mapping property: $ui = 0$ and, for every $g : X \to A$ with $ug = 0$, there exists a unique $\theta : X \to K$ with $i\theta = g$.





There is a dual definition for cokernel (the morphism π in the diagram).

Proposition 2.2.7. Let $u : A \to B$ be a morphism in an additive category $\mathcal{A}$.

(1) If $\ker u$ exists, then u is monic if and only if $\ker u = 0$.

(2) Dually, if $\operatorname{coker} u$ exists, then u is epic if and only if $\operatorname{coker} u = 0$.

Proof: We refer to the diagrams in the definitions of kernel and cokernel. Let $\ker u$ be $\iota : K \to A$, and assume that $\iota = 0$. If $g : X \to A$ satisfies $ug = 0$, then the universal property of kernel provides a morphism $\theta : X \to K$ with $g = \iota\theta = 0$ (because $\iota = 0$). Hence, u is monic. Conversely, if u is monic, consider

$$K \underset{0}{\overset{\iota}{\rightrightarrows}} A \xrightarrow{u} B.$$

Since $u\iota = 0 = u0$, we have $\iota = 0$. The proof for epimorphisms and cokers is dual.

Proposition 2.2.8. Every kernel is monomorphism, every cokernel is epimorphism.

Proof: By uniqueness of θ.

Proposition 2.2.9. If B is an object in an additive category $\mathcal{A}$, consider all ordered pairs (A, f), where $f : A \to B$ is a monomorphism. Call two such pairs (A, f) and (A', f') equivalent if there exists an isomorphism $g : A' \to A$ with $f' = fg$.

A subgadget of B is an equivalence class $[(A, f)]$, and we call A a subobject of B. Note that if (A', f') is equivalent to (A, f), then $A' \cong A$.

Proposition 2.2.10. If B is an object in an additive category $\mathcal{A}$, consider all ordered pairs (f, C), where $f : B \to C$ is an epimorphism. Call two such pairs (f, C) and (f', C') equivalent if there exists an isomorphism $g : C \to C'$ with $f' = gf$. A quotient of B is an equivalence class $[(f, C)]$, and we call C a quotient object of B. Note that if (f', C') is equivalent to (f, C), then $C' \cong C$.

Definition 2.2.11. A category $\mathcal{C}$ is an abelian category if it is an additive category such that

(1) every morphism has a kernel and a cokernel,

(2) every monomorphism is a kernel and every epimorphism is a cokernel.

Definition 2.2.12. Let $f : A \to B$ be a morphism in an abelian category, and let $\operatorname{coker} f$ be $\tau : B \to C$ for some object C. Then its image is

$$\operatorname{im} f = \ker(\operatorname{coker} f) = \ker \tau.$$

A sequence $A \xrightarrow{f} B \xrightarrow{g} C$ in $\mathcal{A}$ is exact if there is equality of subobjects

$$\ker g = \operatorname{im} f.$$

Definition 2.2.13. Let $\mathcal{C}$ and $\mathcal{D}$ be abelian categories. An additive functor $F : \mathcal{C} \to \mathcal{D}$ is left exact (resp. right exact) if for any exact sequence $0 \to X' \to X \to X''$ (resp. $X' \to X \to X'' \to 0$) the sequence $0 \to F(X') \to F(X) \to F(X'')$ (resp. $F(X') \to F(X) \to F(X'') \to 0$) is exact. The functor F is exact if it is right exact and left exact. A functor F is exact if and only if for all exact sequences $X \xrightarrow{u} Y \xrightarrow{v} Z$ the sequence

$$F(X) \xrightarrow{F(u)} F(Y) \xrightarrow{F(v)} F(Z)$$

is exact.

Definition 2.2.14. An object P in an abelian category $\mathcal{A}$ is projective if, for every epic $g : B \to C$ and every $f : P \to C$, there exists $h : P \to B$ with $f = gh$.

An object E in an abelian category $\mathcal{A}$ is injective if, for every monic $g : A \to B$ and every $f : A \to E$, there exists $h : B \to E$ with $f = hg$.

An abelian category $\mathcal{A}$ has enough injectives if, for every $A \in \mathrm{obj}(\mathcal{A})$, there exist an injective E and a monic $A \to E$. Dually, $\mathcal{A}$ has enough projectives if, for every $A \in \mathrm{obj}(\mathcal{A})$, there exist a projective P and an epic $P \to A$.

2.3 Derived Functor

2.4 Ext and Tor

2.5 Group Cohomology

Chapter 3

Theory of Scheme

3.1 Sheaf Theory

Definition 3.1.1. Let X be a topological space. *A* presheaf $\mathscr{F}$ on X consists of the following data,

(1) for every open set U of X a set $\mathscr{F}(U)$,

(2) for each pair of open sets $U \subseteq V$ a map $\mathrm{res}_U^V : \mathscr{F}(V) \to \mathscr{F}(U)$, called restriction map,

such that the following conditions hold (1) $\mathrm{res}_U^U = \mathrm{id}_{\mathscr{F}(U)}$ for every open set $U \subseteq X$, (2) for $U \subseteq V \subseteq W$ open sets of X, $\mathrm{res}_U^W = \mathrm{res}_U^V \circ \mathrm{res}_V^W$. Let $\mathscr{F}_1$ and $\mathscr{F}_2$ be presheaves on X. A morphism of presheaves $\varphi : \mathscr{F}_1 \to \mathscr{F}_2$ is a family of maps $\varphi_U : \mathscr{F}_1(U) \to \mathscr{F}_2(U)$ (for all $U \subseteq X$ open), such that for all pairs of open sets $U \subseteq V$ in X the following diagram commutes If $U \subseteq V$ are open sets of X and $s \in \mathscr{F}(V)$ we will often write $s_{|U}$ instead of $\mathrm{res}_U^V(s)$. The elements of $\mathscr{F}(U)$ are called sections of $\mathscr{F}$ over U. Very often we will also write $\Gamma(U, \mathscr{F})$ instead of $\mathscr{F}(U)$.

Remark 3.1.2. We can also describe presheaves as follows. Let (Ouv_X) be the category whose objects are the open sets of X and, for two open sets $U, V \subseteq X, \mathrm{Hom}(U, V)$ is empty if $U \nsubseteq V$, and consists of the inclusion map $U \to V$ if $U \subseteq V$ (composition of morphisms being the composition of the inclusion maps). Then a presheaf is the same as a contravariant functor $\mathscr{F}$ from the category (Ouv_X) to the category (Sets) of sets.

By replacing (Sets) in this definition by some other category $\mathcal{C}$ (e.g. the category of abelian groups, the category of rings, the category of R-modules, or the category of R-algebras, R a fixed ring) we obtain the notion of a presheaf $\mathscr{F}$ with values in $\mathcal{C}$ (e.g. a presheaf of abelian groups, a presheaf of rings, a presheaf of R-modules, or a presheaf of R-algebras). This signifies that $\mathscr{F}(U)$ is an object in $\mathcal{C}$ for every open subset U of X and that the restriction maps are morphisms in $\mathcal{C}$. A morphism $\mathscr{F}_1 \to \mathscr{F}_2$ of presheaves with values in $\mathcal{C}$ is then simply a morphism of functors.

Definition 3.1.3. Let $\mathscr{F}$ be a presheaf on a topological space X, let U be an open set in X

and let $\mathscr{U} = (U_i)_{i\in I}$ be an open covering of U. We define maps (depending on $\mathscr{U}$)

$$\rho : \mathscr{F}(U) \to \prod_{i\in I} \mathscr{F}(U_i), \quad s \mapsto \left(s_{|U_i}\right)_i$$
$$\sigma : \prod_{i\in I} \mathscr{F}(U_i) \to \prod_{(i,j)\in I\times I} \mathscr{F}(U_i \cap U_j), \quad (s_i)_i \mapsto \left(s_{i|U_i\cap U_j}\right)_{(i,j)},$$
$$\sigma' : \prod_{i\in I} \mathscr{F}(U_i) \to \prod_{(i,j)\in I\times I} \mathscr{F}(U_i \cap U_j), \quad (s_i)_i \mapsto \left(s_{j|U_i\cap U_j}\right)_{(i,j)}.$$

The presheaf $\mathscr{F}$ is called a sheaf, if it satisfies for all U and all coverings (U_i) as above the following condition:

$$\mathscr{F}(U) \xrightarrow{\rho} \prod_{i\in I} \mathscr{F}(U_i) \underset{\sigma'}{\overset{\sigma}{\rightrightarrows}} \prod_{(i,j)\in I\times I} \mathscr{F}(U_i \cap U_j)$$

is exact. This means that the map ρ is injective and that its image is the set of elements $(s_i)_{i\in I} \in \prod_{i\in I} \mathscr{F}(U_i)$ such that $\sigma((s_i)_i) = \sigma'((s_i)_i)$.

In other words, a presheaf $\mathscr{F}$ is a sheaf if and only if for all open sets U in X and every open covering $U = \bigcup_i U_i$ the following two conditions hold:

(1) (Sh1) Let $s, s' \in \mathscr{F}(U)$ with $s_{|U_i} = s'_{|U_i}$ for all i. Then $s = s'$.

(2) (Sh2) Given $s_i \in \mathscr{F}(U_i)$ for all i such that $s_{i|U_i\cap U_j} = s_{j|U_i\cap U_j}$ for all i, j. Then there exists an $s \in \mathscr{F}(U)$ such that $s_{|U_i} = s_i$ (note that s is unique by (Sh1)).

Definition 3.1.4. The inductive limit

$$\mathscr{F}_x := \varinjlim_{U\ni x} \mathscr{F}(U)$$

is called the stalk of $\mathscr{F}$ in x. In other words, $\mathscr{F}_x$ is the set of equivalence classes of pairs (U, s), where U is an open neighborhood of x and $s \in \mathscr{F}(U)$. Here two such pairs (U_1, s_1) and (U_2, s_2) are equivalent, if there exists an open neighborhood V of x with $V \subseteq U_1 \cap U_2$ such that $s_{1|V} = s_{2|V}$. For each open neighborhood U of x we have a canonical map

$$\mathscr{F}(U) \to \mathscr{F}_x, \quad s \mapsto s_x$$

which sends $s \in \mathscr{F}(U)$ to the class of (U, s) in $\mathscr{F}_x$. We call s_x the germ of s in x. If $\varphi : \mathscr{F} \to \mathscr{G}$ is a morphism of presheaves on X, we have an induced map

$$\mathscr{F}_x \to \mathscr{G}_x$$

of the stalks in x by Proposition 2.1.26. We obtain a functor $\mathscr{F} \mapsto \mathscr{F}_x$ from the category of presheaves on X to the category of sets.

If $\mathscr{F}$ is a presheaf with values in $\mathcal{C}$, where $\mathcal{C}$ is the category of abelian groups, of rings, or any category in which filtered inductive limits exist, then the stalk $\mathscr{F}_x$ is an object in $\mathcal{C}$ and we obtain a functor $\mathscr{F} \mapsto \mathscr{F}_x$ from the category of presheaves on X with values in $\mathcal{C}$ to the category $\mathcal{C}$.

Definition 3.1.5. Let X be a topological space, $\mathscr{F}$ and $\mathscr{G}$ presheaves on X, and let $\varphi, \psi : \mathscr{F} \to \mathscr{G}$ be two morphisms of presheaves.

(1) Assume that $\mathscr{F}$ is a sheaf. Then the induced maps on stalks $\varphi_x : \mathscr{F}_x \to \mathscr{G}_x$ are injective for all $x \in X$ if and only if $\varphi_U : \mathscr{F}(U) \to \mathscr{G}(U)$ is injective for all open subsets $U \subseteq X$.

(2) If $\mathscr{F}$ and $\mathscr{G}$ are both sheaves, the maps φ_x are bijective for all $x \in X$ if and only if φ_U is bijective for all open subsets $U \subseteq X$.

(3) If $\mathscr{F}$ and $\mathscr{G}$ are both sheaves, the morphisms φ and ψ are equal if and only if $\varphi_x = \psi_x$ for all $x \in X$.

Proof: For $U \subseteq X$ open consider the map

$$\mathscr{F}(U) \to \prod_{x \in U} \mathscr{F}_x, \quad s \mapsto (s_x)_{x \in U}$$

We claim that this map is injective if $\mathscr{F}$ is a sheaf. Indeed let $s, t \in \mathscr{F}(U)$ such that $s_x = t_x$ for all $x \in U$. Then for all $x \in U$ there exists an open neighborhood $V_x \subseteq U$ of x such that $s_{|V_x} = t_{|V_x}$. Clearly, $U = \bigcup_{x \in U} V_x$ and therefore $s = t$ by sheaf condition (Sh1). Using the commutative diagram

$$\begin{array}{ccc} \mathscr{F}(U) & \longrightarrow & \prod \mathscr{F}_x \\ \downarrow{\scriptstyle \varphi_U} & & \downarrow{\scriptstyle \prod \varphi_x} \\ \mathscr{G}(U) & \longrightarrow & \prod \mathscr{G}_x \end{array}$$

and Proposition 2.1.27, (1) and (3) hold.

(2): By proposition 2.1.27, it suffice to show the bijectivity of φ_x for all $x \in U$ implies the surjectivity of φ_U. Let $t \in \mathscr{G}(U)$. For all $x \in U$ we choose an open neighborhood U^x of x in U and $s^x \in \mathscr{F}(U^x)$ such that $\left(\varphi_{U^x}(s^x)\right)_x = t_x$. Then there exists an open neighborhood $V^x \subseteq U^x$ of x with $\varphi_{V^x}\left(s^x{}_{|V^x}\right) = t_{|V^x}$. Then $(V^x)_{x \in U}$ is an open covering of U and for $x, y \in U$

$$\varphi_{V^x \cap V^y}\left(s^x{}_{|V^x \cap V^y}\right) = t_{|V^x \cap V^y} = \varphi_{V^x \cap V^y}\left(s^y \mid V^x \cap V^y\right).$$

As we already know that $\varphi_{V^x \cap V^y}$ is injective, this shows $s^x \,|V^x \cap V^y = s^y| \, V^x \cap V^y$ and the sheaf condition (Sh2) ensures that we find $s \in \mathscr{F}(U)$ such that $s_{|V^x} = s^x{}_{|V^x}$ for all $x \in U$. Clearly, we have $\varphi_U(s)_x = t_x$ for all $x \in U$ and hence $\varphi_U(s) = t$.

Definition 3.1.6. A morphism $\varphi : \mathscr{F} \to \mathscr{G}$ of sheaves injective (resp. surjective, resp. bijective) if $\varphi_x : \mathscr{F}_x \to \mathscr{G}_x$ is injective (resp. surjective, resp. bijective) for all $x \in X$.

Remark 3.1.7. If $\varphi : \mathscr{F} \to \mathscr{G}$ is a morphism of sheaves, φ is surjective if and only if for all open subsets $U \subseteq X$ and every $t \in \mathscr{G}(U)$ there exist an open covering $U = \bigcup_i U_i$ (depending on t) and sections $s_i \in \mathscr{F}(U_i)$ such that $\varphi_{U_i}(s_i) = t_{|U_i}$, i.e., locally we can find a preimage of t. But the surjectivity of φ does not imply that $\varphi_U : \mathscr{F}(U) \to \mathscr{G}(U)$ is surjective for all open sets U of X

Definition 3.1.8. If $\mathscr{F}, \mathscr{G}$ are (pre-)sheaves on X such that $\mathscr{F}(U) \subseteq \mathscr{G}(U)$ for all $U \subseteq X$ open, and such that the following diagram commute

$$\begin{array}{ccc} \mathscr{F}(U) & \xrightarrow{\subset} & \mathscr{G}(U) \\ {\scriptstyle \mathrm{res}_U^V}\uparrow & & \uparrow{\scriptstyle \mathrm{res}_U^V} \\ \mathscr{F}(V) & \xrightarrow[\subset]{} & \mathscr{G}(V) \end{array}$$

we call $\varphi : \mathscr{F}$ sub(pre-)sheaf of $\varphi : \mathscr{G}$.

Definition 3.1.9 (sheafification)**.** Let $\mathscr{F}$ be a presheaf on a topological space X. Then there exists a pair $\left(\tilde{\mathscr{F}}, \iota_{\mathscr{F}}\right)$, where $\tilde{\mathscr{F}}$ is a sheaf on X and $\iota_{\mathscr{F}} : \mathscr{F} \to \tilde{\mathscr{F}}$ is a morphism of presheaves, such that the following holds: If $\mathscr{G}$ is a sheaf on X and $\varphi : \mathscr{F} \to \mathscr{G}$ is a morphism of presheaves, then there exists a unique morphism of sheaves $\tilde{\varphi} : \tilde{\mathscr{F}} \to \mathscr{G}$ with $\tilde{\varphi} \circ \iota\mathscr{F} = \varphi$. The pair $\left(\tilde{\mathscr{F}}, \iota_{\mathscr{F}}\right)$ is unique up to unique isomorphism. Moreover, the following properties hold:

(1) For all $x \in X$ the map on stalks $\iota_{\mathscr{F},x} : \mathscr{F}_x \to \tilde{\mathscr{F}}_x$ is bijective.

(2) For every presheaf $\mathscr{G}$ on X and every morphism of presheaves $\varphi : \mathscr{F} \to \mathscr{G}$ there exists a unique morphism $\tilde{\varphi} : \tilde{\mathscr{F}} \to \tilde{\mathscr{G}}$ making the diagram

$$\begin{array}{ccc} \mathscr{F} & \xrightarrow{\iota_{\mathscr{F}}} & \tilde{\mathscr{F}} \\ {\scriptstyle \varphi}\downarrow & & \downarrow{\scriptstyle \tilde{\varphi}} \\ \mathscr{G} & \xrightarrow[\iota_{\mathscr{G}}]{} & \tilde{\mathscr{G}} \end{array}$$

commutative.

In particular, $\mathscr{F} \mapsto \tilde{\mathscr{F}}$ is a functor from the category of presheaves on X to the category of sheaves on X.

Chapter 4

Representation Theory