Algebra

Erzhuo Wang

February 8, 2024

Contents

1 Commutative Algebra

1.1 Basic Definition in Ring Thoery

Notation 1.1.1. In this note, by a ring we always understand a commutative ring with unit(unless stated otherwise); ring homomorphisms $A \to B$ are assumed to take the unit element of A into the unit element of B. When we say that A is a subring of it is understood that the unit elements of A and B coincide.

Notation 1.1.2. If $f : A \to B$ is a ring homomorphism, J is an ideal of B, then $f^{-1}(J)$ is an ideal of A, and we denote it by $A \cap J$.

Notation 1.1.3. In this note, $\subset$ or $\subseteq$ are used for inclusion of a subset, including the possibility of equality;$\subsetneq$ is used for strict includsion.

Definition 1.1.4. 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 1.1.5. 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 1.1.6. If I is a proper ideal then there exists at least one maximal ideal containing I.

Definition 1.1.7. 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 1.1.8. A field F is an integral doamin such that every non-zero element in F is invertible.

Definition 1.1.9. 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 1.1.10. 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 1.1.11. A subset S of A is multiplicative if it satisfies:

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

(2) $1 \in S$.

Definition 1.1.12. 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 1.1.13. the radical $\sqrt{I}$ of I is the intersection of all prime ideals containing I.

Proof:

Lemma 1.1.14. 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 1.1.14, we can find a prime ideal which contains I disjoint from S_x.

Definition 1.1.15. 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 1.1.16. The intersection 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 1.1.17. $x \in rad(A)$ if and only if $1 + xy$ is a unit in A for all $y \in A$.

Definition 1.1.18. 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 1.1.19. 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 1.1.20. 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 $I_1 I_2 \dots I_n = I_1 \cap I_2 \dots \cap I_n$

Theorem 1.1.21 (Chinese Reminder Theorem)**.** If $I_1, \dots, I_n$ are ideals which are coprime in pairs then

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

and the isomorphism map is given by

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

Theorem 1.1.22 (Prime Avoidance)**.** (1) Let $P_1, \dots P_n$ be prime ideals and let I be an ideal contained in $\bigcup_{i=1}^n P_i$. Then $I \subset P_i$ for some $1 \le i \le n$.

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

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 1.1.23. 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 1.1.24. In an integral domain, a prime element is always irreducible.

Definition 1.1.25 (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: $r = p_1 \dots p_n$
2. the decomposition in (1) is unique up to associates.

Proposition 1.1.26. 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 1.1.27 (P.I.D)**.** A Principal Ideal Domain is an integral domain in which every ideal is principal.

Proposition 1.1.28. Every Principal Ideal Domain is a Unique Factorization Domain.

Proposition 1.1.29. If F is a field, then $F[x]$ is a Principal Ideal Domain.

Lemma 1.1.30 (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 1.1.31. 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 1.1.32. If R is a U.F.D, then $R[x]$ is a U.F.D.

Proof: By Proposition 1.1.29, Lemma 1.1.30 and Corollary 1.1.31.

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:

$$\begin{tikzcd}
A \arrow[rr, "h"] & & B \\
& R \arrow[ul, "f"] \arrow[ur, "g"'] &
\end{tikzcd}$$

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 $\{\bar{u}_1, \dots, \bar{u}_n\}$ for $\bar{M}$ over k, and choose an inverse image $u_i \in M$ of each $\bar{u}_i$, then $\{u_1, \dots, u_n\}$ 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 $\{u_1, \dots, u_n\}$ and $\{v_1, \dots, v_n\}$ 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 1.1.19

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 $\omega_1, \dots, \omega_n$ 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

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

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

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

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

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

Definition 1.2.15. 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

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

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 1.2.16 (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 $h : A \times B \to A \otimes_R B$

$$\begin{tikzcd} A \times B \arrow[d, "h"'] \arrow[dr, "f"] & \\ A \otimes_R B \arrow[r, dashed, "\tilde{f}"'] & G \end{tikzcd}$$

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 1.2.17. 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.

$$\begin{tikzcd} A \times B \arrow[d, "h"'] \arrow[dr, "g"] & \\ A \otimes_R B \arrow[r, dashed, "\tilde{g}"'] & M \end{tikzcd}$$

Proposition 1.2.18. If R is a ring, and $A_{R,R}B$ are R-modules, then there are R-module isomorphisms:

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

Theorem 1.2.19. 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 1.2.20 (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:

$$\begin{tikzcd}
M \otimes_R N \arrow[r, "\tau"] \arrow[d, "f\otimes g"'] & N \otimes_R M \arrow[d, "g\otimes f"] \\
M' \otimes_R N' \arrow[r, dashed, "\tau'"'] & N' \otimes_R M'
\end{tikzcd}$$

Theorem 1.2.21. 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 1.2.22 (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 1.2.23. '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 1.2.24. (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 1.2.25. If M is a left R-module, then there's left R-module isomorphism

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

Theorem 1.2.26. 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 1.2.27. 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 1.2.28 (The Short Five Lemma)**.** Let R be a ring and

$$\begin{tikzcd} 0 \arrow[r] & M' \arrow[r, "u"] \arrow[d, "\alpha"] & M \arrow[r, "v"] \arrow[d, "\beta"] & M'' \arrow[r] \arrow[d, "\gamma"] & 0 \\ 0 \arrow[r] & N' \arrow[r, "u'"] & N \arrow[r, "v'"] & N'' \arrow[r] & 0 \end{tikzcd}$$

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 1.2.29 (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)

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

is a spilt exact sequence of abelian groups for all R-module D.

(5)

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

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 1.2.30 (Snake lemma)**.** Let

$$
\begin{tikzcd}
0 \arrow[r] & M' \arrow[r, "u"] \arrow[d, "f'"] & M \arrow[r, "v"] \arrow[d, "f"] & M'' \arrow[r] \arrow[d, "f''"] & 0 \\
0 \arrow[r] & N' \arrow[r, "u'"] & N \arrow[r, "v'"] & N'' \arrow[r] & 0
\end{tikzcd}
$$

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

$$
\begin{tikzcd}
0 \arrow[r] & \operatorname{Ker}(f') \arrow[r, "\bar{u}"] & \operatorname{Ker}(f) \arrow[r, "\bar{v}"] & \operatorname{Ker}(f'') \arrow[dll, "d"] & \\
& \operatorname{Coker}(f') \arrow[r, "\bar{u}'"'] & \operatorname{Coker}(f) \arrow[r, "\bar{v}'"'] & \operatorname{Coker}(f'') \arrow[r] & 0
\end{tikzcd}
$$

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 $x'' \in \operatorname{Ker}(f'')$, we have $x'' = v(x)$ for some $x \in M$, and $v'(f(x)) = f''(v(x)) = 0$, hence $f(x) \in \operatorname{Ker}(v') = \operatorname{Im}(u')$, 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 1.2.31.

(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

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

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

$$\operatorname{Hom}_R(A, D) \xleftarrow{\bar{f}} \operatorname{Hom}_R(B, D) \xleftarrow{\bar{g}} \operatorname{Hom}_R(C, D) \to 0$$

is an exact sequence of abelian groups.

Definition 1.2.32 (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.

$$
\begin{tikzcd}
& P \arrow[d, "f"] \arrow[dl, dotted, "h"'] & \\
A \arrow[r, "g"] & B \arrow[r] & 0
\end{tikzcd}
$$

(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 1.2.33. Every free module F over a ring R is projective.

Proposition 1.2.34. 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 1.2.35. 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 1.2.36 (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.

$$\begin{tikzcd}
& J & \\
A \arrow[ur, dotted, bend left, "h"] & B \arrow[l, "g"'] \arrow[u, "f"'] & 0 \arrow[l]
\end{tikzcd}$$

(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 1.2.37. 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 1.2.38. 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 1.2.39. 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 1.2.40. Let R be a ring and let M be an R-module. Then M is contained in an injective R-module.

Proposition 1.2.41. Any modules over a PID, it is a projective module if and only if it is a free module.

Definition 1.2.42 (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 1.2.43. Projective modules are flat.

Example 1.2.44. $\mathbb{Q}/\mathbb{Z}$ 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 1.2.45. $\sum_{i\in I} A_i$ flat if and only if each $A_i, i \in I$ flat.

Proof: Since tensor product commute with direct sum.

Example 1.2.46.

	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{Q}/\mathbb{Z}$	$\mathbb{Z} \oplus \mathbb{Q}$
flat	✓	✓(By 1.8.2)	×(1.2.44)	✓(1.2.45)
projective	✓	×(By 1.2.41)	×	×(1.2.34)
injective	×(By 1.2.38)	✓(By 1.2.38)	✓(By 1.2.38)	×(1.2.37)

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 intersection 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 :

$$\begin{tikzcd}
\sigma : E \arrow[r, "\sim"] & E' \\
\varphi : F \arrow[r, "\sim"] \arrow[u] & F' \arrow[u]
\end{tikzcd}$$

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. $\square$

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 $1 \le i \le r$. 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:

$$\begin{tikzcd}
\{F\text{-algebra homomorphism between } E \text{ and } \bar{F}\} \arrow[dr, "\text{Extended by 1.3.16 and 1.3.31}"] & \\
\{\text{left cosets of } H \text{ in } G\} \arrow[u, "\sigma H \mapsto \sigma|_E"'] \arrow[r, "\sigma H \mapsto \sigma|_E"] & \{\sigma|_E : \sigma \in G\}
\end{tikzcd}$$

(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 intersection $E_1 \cap E_2$ 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 intersection $H_1 \cap H_2$.

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

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

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 intersection $K_1 \cap K_2$ 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 $\mathrm{Gal}\left(K_1/F\right) \times \mathrm{Gal}\left(K_2/F\right)$ consisting of elements whose restrictions to the intersection $K_1 \cap K_2$ 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 intersection 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.

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

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 1.1.22

Proposition 1.4.2. X=Spec$A$, $X_f = X - V(f)$.

(1) X_f form a basis of X.

(2) $X_{fg} = X_f \cap X_g$.

(3) X is compact.

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

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

(6) An open subset of X is open if and only if it is finite union of sets X_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) $\overline{\{x\}} = V(P_x)$

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 specture 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

$$I \longrightarrow V(I)$$

$$\bigcap_{P \in E} P \longleftarrow V(E)$$

Proposition 1.4.7. Let $\varphi : A \to B$ be a ring homomorphism. Let $X =$Spec$A$ and $Y =$Spec$B$. Let ϕ to be the map:

$$\text{Spec}B \to \text{Spec}A$$

$$P \mapsto \varphi^{-1}(P)$$

(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, $\overline{\phi(V(J))} = V(\phi(J))$

Definition 1.4.8. 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 1.4.9. R is a Noetherian ring, then $X = \text{Spec}(R)$ is a Notherian space.

Proof: By Theorem 1.4.6

Theorem 1.4.10 (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 1.4.11. A Notherian ring has only finite many minimal prime ideals.

Proof: By Example 1.4.11 and Theorem 1.4.10.

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:

$$P_1 \supset P_1 P_2 \cdots \supset P_1 \ldots P_n \supset \ldots$$

By Theorem 1.1.22, 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.

Theorem 1.5.14 (Cohen)**.** If all the prime ideals of a ring A are finitely generated then A is Noetherian.

Definition 1.5.15 (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 1.5.16. 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 1.2.26, and Nakayama's lemma, define $M_k = M \otimes_A k$, it suffice to show $M_k \otimes_k N_k = (M \otimes N)_k$. Notice that

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

□

(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:

$$\begin{tikzcd} A \arrow[r, "a \mapsto a/1"] \arrow[dr, "a \mapsto a/1"'] & S^{-1}A \arrow[d, "a/s \mapsto a/s"] \\ & T^{-1}A \end{tikzcd}$$

1.7 Intergral Extension

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 1.2.18.

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 1.2.18.

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 $\bar{S} \cap Y = S$. Indeed, if $\bar{S} = V \cup W$ with V and W closed in X then

$$S = \bigcap_{W \supset S, W \text{ closed in X}} W \cap Y = \bar{S} \cap Y = (V \cap Y) \cup (W \cap Y)$$

, 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 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 coht p. It follows from the definitions that

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

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 1.1.22 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. The polynomial ring $k[X_1, \ldots, X_n]$ over a field k is an integral domain, and since

$$k[X_1, \ldots, X_n] / (X_1, \ldots, X_i) \simeq k[X_{i+1}, \ldots, X_n],$$

$(X_1, \ldots, X_i)$ is a prime ideal of $k[X_1, \ldots, X_n]$. Thus

$$(0) \subset (X_1) \subset (X_1, X_2) \subset \cdots \subset (X_1, \ldots, X_n)$$

is a chain of prime ideals of length n, and $\dim k[X_1, \ldots, X_n] \geqslant n$.

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 :

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

Here also we have the inequality

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

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 $\operatorname{Supp}(M) = V(\operatorname{ann}(M))$ of $\operatorname{Spec} A$.

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 $\mathrm{Hom}_{\mathcal{S}}(A, B) = \mathrm{Hom}_{\mathcal{C}}(A, B)$.

Definition 2.1.3 (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 $A \in \mathrm{obj}(\mathcal{C})$, then $T(A) \in \mathrm{obj}(\mathcal{D})$,

(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 $A \in \mathrm{obj}(\mathcal{C})$.

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

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

(2) if $f : C \to C'$ in $\mathcal{C}$, then $T(f) : T(C') \to T(C)$ in $\mathcal{D}$ (note the reversal of arrows),

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

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

Definition 2.1.5 (faithful functor)**.** A functor $T : \mathcal{C} \to \mathcal{D}$ is faithful if, for all $A, B \in \operatorname{obj}(\mathcal{C})$, the functions $\operatorname{Hom}_{\mathcal{C}}(A, B) \to \operatorname{Hom}_{\mathcal{D}}(TA, TB)$ given by $f \mapsto Tf$ are injections.

Definition 2.1.6 (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 2.1.7 (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 $\mathcal{B}$,

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

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

Natural transformations between contravariant functors are defined similarly. A natural isomorphism is a natural transformation τ for which each τ_A is an isomorphism.

Definition 2.1.8 (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 2.1.9 (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 2.1.10 (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 $\left(C, (p_i : C \to A_i)_{i \in I}\right)$, 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.

$$\begin{tikzcd}
& A_i & \\
C \arrow[ur, "\alpha_i"] & & X \arrow[ul, "f_i"'] \arrow[ll, dashed, "\theta"]
\end{tikzcd}$$

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 2.1.11 (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.

$$\begin{tikzcd} & A_i \arrow[dl, "\alpha_i"'] \arrow[dr, "f_i"] & \\ C \arrow[rr, dashed, "\theta"] & & X \end{tikzcd}$$

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 2.1.12 (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. $\bigsqcup_{i\in I} A_i = \big\{(a_i, i) \in \big(\bigcup_{i\in I} A_i\big) \times I : a_i \in A_i\big\}$ 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 2.1.13 (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 2.1.14 (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.

$$\begin{tikzcd} X \arrow[dr, dashed, "\theta"] \arrow[drr, "\alpha'"] \arrow[ddr, "\beta'"'] & & \\ & D \arrow[r, "\alpha"] \arrow[d, "\beta"'] & C \arrow[d, "g"] \\ & B \arrow[r, "f"'] & A \end{tikzcd}$$

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 2.1.15 (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 2.1.16 (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 $B \cup_A C$.

$$\begin{tikzcd}
X & & \\
& D \arrow[ul, dashed, "\theta"'] & C \arrow[l, "\alpha"'] \arrow[ull, "\alpha'"'] \\
& B \arrow[u, "\beta"] \arrow[uul, "\beta'"] & A \arrow[l, "f"] \arrow[u, "g"']
\end{tikzcd}$$

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

Example 2.1.17. 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:

$$\beta : B \to B \otimes_A C \qquad\qquad \alpha : C \to B \otimes_A C$$
$$b \mapsto b \otimes 1 \qquad\qquad c \mapsto 1 \otimes c$$

Definition 2.1.18 (inverse system)**.** Given a partially ordered set I and a category $\mathcal{C}$, an inverse system in $\mathcal{C}$ is an ordered pair $\left((M_i)_{i \in I}, (\psi_i^j)_{j \succeq i}\right)$, abbreviated $\{M_i, \psi_i^j\}$, 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 $k \succeq j \succeq i$.

$$\begin{tikzcd}
M_k \arrow[rr, "\psi_i^k"] \arrow[dr, "\psi_j^k"'] & & M_i \\
& M_j \arrow[ur, "\psi_i^j"'] &
\end{tikzcd}$$

Definition 2.1.19 (inverse limit)**.** Let I be a partially ordered set, let $\mathcal{C}$ be a category, and let $\{M_i, \psi_i^j\}$ 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 $X \in \text{obj}(\mathcal{C})$ 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.

$$
\begin{tikzcd}
\varprojlim M_i \arrow[dr, "\alpha_i"] \arrow[ddr, "\alpha_j"'] & & X \arrow[ll, dashed, "\theta"'] \arrow[dl, "f_i"'] \arrow[ddl, "f_j"] \\
& M_i & \\
& M_j \arrow[u, "\varphi_i^j"] &
\end{tikzcd}
$$

Example 2.1.20. 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 2.1.21 (direct system)**.** Given a partially ordered set I and a category $\mathcal{C}$, a direct system in $\mathcal{C}$ is an ordered pair $\left((M_i)_{i\in I}, \left(\varphi_j^i\right)_{i\preceq j}\right)$, abbreviated $\left\{M_i, \varphi_j^i\right\}$, where $(M_i)_{i\in I}$ is an indexed family of objects in $\mathcal{C}$ and $\left(\varphi_j^i : M_j \to M_i\right)_{i\preceq j}$ 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 $i \preceq j \preceq k$.

$$
\begin{tikzcd}
M_i \arrow[rr, "\psi_k^i"] \arrow[dr, "\psi_j^i"'] & & M_k \\
& M_j \arrow[ur, "\psi_k^j"'] &
\end{tikzcd}
$$

Definition 2.1.22 (direct limit)**.** Let I be a partially ordered set, let $\mathcal{C}$ be a category, and let $\left\{M_i, \varphi_j^i\right\}$ 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) $\alpha_j \varphi_j^i = \alpha_i$ whenever $i \preceq j$,

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

$$
\begin{tikzcd}
\varinjlim M_i \arrow[rr, dashed, "\theta"] & & X \\
& M_i \arrow[ul, "\alpha_i"'] \arrow[ur, "f_i"] \arrow[d, "\varphi_j^i"'] & \\
& M_j \arrow[uul, "\alpha_j"] \arrow[uur, "f_j"'] &
\end{tikzcd}
$$

Example 2.1.23. M is a smooth manifold, $p \in M$, $C_p^\infty(M)$ be the germ of smooth function at p, then $C_p^\infty(M)$ is the direct limit of the direct system $\left\{(C^\infty(U))_{p\in U \text{ open in } M}, (\text{res}_V^U)_{V\subset U}\right\}$ where res be the restriction map from the bigger open subset to the smaller one.

Definition 2.1.24. 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 $\mathcal{C}$.

Similarly, we can define co(contra)variant functor perserve(convert) limit(limit to colimit/colimit to limit)

Definition 2.1.25. 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:

$$\begin{tikzcd}
\mathrm{Hom}_{\mathcal{D}}(FC, D) \arrow[r, "(Ff)^*"] \arrow[d, "\tau_{C,D}"'] & \mathrm{Hom}_{\mathcal{D}}\left(FC', D\right) \arrow[d, "\tau_{C',D}"] \\
\mathrm{Hom}_{\mathcal{C}}(C, GD) \arrow[r, "f^*"'] & \mathrm{Hom}_{\mathcal{C}}\left(C', GD\right)
\end{tikzcd}$$

$$\begin{tikzcd}
\mathrm{Hom}_{\mathcal{D}}(FC, D) \arrow[r, "(g)^*"] \arrow[d, "\tau_{C,D}"'] & \mathrm{Hom}_{\mathcal{D}}\left(FC, D'\right) \arrow[d, "\tau_{C,D'}"] \\
\mathrm{Hom}_{\mathcal{C}}(C, GD) \arrow[r, "(Gg)_*"'] & \mathrm{Hom}_{\mathcal{C}}\left(C, GD'\right)
\end{tikzcd}$$

Example 2.1.26 (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 2.1.27 (Free and Forget)**.**

Example 2.1.28 (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 $\mathrm{Hom}_{\mathbb{C}[G]}(\mathbb{C}[G], \square) \simeq \mathrm{Res}_{\mathbb{C}[H]}^{\mathbb{C}[G]}$(Restriction from $\mathbb{C}[G]$-module to $\mathbb{C}[H]$-module), we have $(\mathbb{C}[G] \otimes_{\mathbb{C}[H]} \square, \mathrm{Res}_{\mathbb{C}[H]}^{\mathbb{C}[G]})$ is an adjoint pair.

Proposition 2.1.29. 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) the distributive laws hold: given morphisms

$$X \xrightarrow{a} A \underset{g}{\overset{f}{\rightrightarrows}} B \xrightarrow{b} Y,$$

where X and $Y \in \mathrm{obj}(\mathcal{C})$, then

$$b(f+g) = bf + bg \quad \text{and} \quad (f+g)a = fa + ga,$$

(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)**.**

2.3 Derived Functor

3 Theory of Scheme