

# Algebra

Erzhuo Wang

September 1, 2024



# Contents

<b>1</b>	<b>Abstract Algebra</b>	<b>5</b>
1.1	Linear Algebra . . . . .	5
1.2	Group Theory . . . . .	7
1.3	Field Theory . . . . .	12
1.3.1	Basic Concept . . . . .	12
1.3.2	Separable . . . . .	14
1.3.3	Normal . . . . .	17
1.3.4	Galios . . . . .	18
<b>2</b>	<b>Commutative Algebra</b>	<b>21</b>
2.1	Basic Definition in Ring Thoery . . . . .	21
2.2	Basic Definition in Module . . . . .	25
2.3	Specturm . . . . .	36
2.4	Chain conditions . . . . .	40
2.5	Localization . . . . .	42
2.6	Intergral Extension and Dedekind Domain . . . . .	48
2.7	Flatness . . . . .	51
2.8	Dimension Theory and Hilbert's Nullstellensatz . . . . .	52
2.9	Completion . . . . .	57
<b>3</b>	<b>Homological Algerba</b>	<b>59</b>
3.1	Basic Definition in Category . . . . .	59
3.2	Abelian Category . . . . .	66
3.3	Derived Functor . . . . .	70
3.4	Ext and Tor . . . . .	73
3.5	Group Cohomology . . . . .	75
<b>4</b>	<b>Representation Theory</b>	<b>81</b>
4.1	Definition . . . . .	81
4.2	Character . . . . .	87
4.3	Induced representation . . . . .	90



# Chapter 1

## Abstract Algebra

### 1.1 Linear Algebra

**Theorem 1.1.1** (Newton's Formulas). Let  $f(x)$  be a monic polynomial of degree  $n$  with roots  $\alpha_1, \dots, \alpha_n$ . Let  $s_i$  be the elementary symmetric function of degree  $i$  in the roots and define  $s_i = 0$  for  $i > n$ . Let  $p_i = \alpha_1^i + \dots + \alpha_n^i, i \geq 0$ , be the sum of the  $i^{\text{th}}$  powers of the roots of  $f(x)$ . Prove Newton's Formulas:

$$p_1 - s_1 = 0$$

$$p_2 - s_1 p_1 + 2s_2 = 0$$

$$p_3 - s_1 p_2 + s_2 p_1 - 3s_3 = 0$$

$$\vdots$$

$$p_i - s_1 p_{i-1} + s_2 p_{i-2} - \dots + (-1)^{i-1} s_{i-1} p_1 + (-1)^i i s_i = 0$$

**Definition 1.1.2** (resultant ). Let  $F$  be a field and let  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$  and  $g(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0$  be two polynomials in  $F[x]$ . It's easy to say that a necessary and sufficient condition for  $f(x)$  and  $g(x)$  to have a common root (or, equivalently, a common divisor in  $F[x]$  ) is the existence of a polynomial  $a(x) \in F[x]$  of degree at most  $m - 1$  and a polynomial  $b(x) \in F[x]$  of degree at most  $n - 1$  with  $a(x)f(x) = b(x)g(x)$ .

Write  $a(x)$  and  $b(x)$  explicitly as polynomials, then equating coefficients in the equation  $a(x)f(x) = b(x)g(x)$  gives a system of  $n + m$  linear equations for the coefficients of  $a(x)$  and  $b(x)$ . Then this system has a nontrivial solution (hence  $f(x)$  and  $g(x)$  have a common zero) if

and only if the determinant

$$R(f, g) = \begin{vmatrix} a_n & a_{n-1} & \dots & a_0 & & & & \\ & a_n & a_{n-1} & \dots & a_0 & & & \\ & & a_n & a_{n-1} & \dots & a_0 & & \\ & & & \ddots & & & & \\ & & & & a_n & a_{n-1} & \dots & a_0 \\ b_m & b_{m-1} & \dots & b_0 & & & & \\ & b_m & b_{m-1} & \dots & b_0 & & & \\ & & b_m & b_{m-1} & \dots & b_0 & & \\ & & & \ddots & & & & \\ & & & & b_m & b_{m-1} & \dots & b_0 \end{vmatrix}$$

is zero. Here  $R(f, g)$ , called the resultant of the two polynomials, is the determinant of an  $(n+m) \times (n+m)$  matrix  $R$  with  $m$  rows involving the coefficients of  $f(x)$  and  $n$  rows involving the coefficients of  $g(x)$ .

**Definition 1.1.3** (discriminant of polynomial).  $f(x) \in F[x]$ ,  $\alpha_1, \dots, \alpha_n \in \bar{F}$  are roots of  $f(x)$ . Then

$$D(f) = \prod_{i < j} (\alpha_i - \alpha_j)^2$$

**Proposition 1.1.4.**

$$D = (-1)^{n(n-1)/2} R(f, f')$$

where  $D$  is the discriminant of  $f(x)$ .

**Theorem 1.1.5.** Let  $R$  be a Principal Ideal Domain, let  $M$  be a free  $R$ -module of finite rank  $n$  and let  $N$  be a submodule of  $M$ . Then

- (1)  $N$  is free of rank  $m$ ,  $m \leq n$  and
- (2) there exists a basis  $y_1, y_2, \dots, y_n$  of  $M$  so that  $a_1 y_1, a_2 y_2, \dots, a_m y_m$  is a basis of  $N$  where  $a_1, a_2, \dots, a_m$  are nonzero elements of  $R$  with the divisibility relations

$$a_1 \mid a_2 \mid \dots \mid a_m$$

**Theorem 1.1.6** (Fundamental Theorem, Existence: Invariant Factor Form). Let  $R$  be a P.I.D. and let  $M$  be a finitely generated  $R$ -module.

- (1) Then  $M$  is isomorphic to the direct sum of finitely many cyclic modules. More precisely,

$$M \cong R^r \oplus R/(a_1) \oplus R/(a_2) \oplus \dots \oplus R/(a_m)$$

for some integer  $r \geq 0$  and nonzero elements  $a_1, a_2, \dots, a_m$  of  $R$  which are not units in  $R$  and which satisfy the divisibility relations

$$a_1 \mid a_2 \mid \dots \mid a_m$$

(2)  $M$  is torsion free if and only if  $M$  is free.

(3) In the decomposition in (1),

$$\text{Tor}(M) \cong R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m).$$

**Theorem 1.1.7** (Fundamental Theorem, Existence: Elementary Divisor Form)). Let  $R$  be a P.I.D. and let  $M$  be a finitely generated  $R$ -module. Then  $M$  is the direct sum of a finite number of cyclic modules whose annihilators are either  $(0)$  or generated by powers of primes in  $R$ , i.e.,

$$M \cong R^r \oplus R/(p_1^{\alpha_1}) \oplus R/(p_2^{\alpha_2}) \oplus \cdots \oplus R/(p_t^{\alpha_t})$$

where  $r \geq 0$  is an integer and  $p_1^{\alpha_1}, \dots, p_t^{\alpha_t}$  are positive powers of (not necessarily distinct) primes in  $R$ .

**Theorem 1.1.8.** Let  $R$  be a P.I.D.

- (1) Two finitely generated  $R$ -modules  $M_1$  and  $M_2$  are isomorphic if and only if they have the same free rank and the same list of invariant factors.
- (2) Two finitely generated  $R$ -modules  $M_1$  and  $M_2$  are isomorphic if and only if they have the same free rank and the same list of elementary divisors.

**Corollary 1.1.9.** Finite subgroup of a multiplication group of a field is cyclic.

## 1.2 Group Theory

**Definition 1.2.1.** Let  $G$  be a group. If  $\{G_\alpha\}_{\alpha \in J}$  is a family of subgroups of  $G$ , we say (as before) that these groups generate  $G$  if every element  $x$  of  $G$  can be written as a finite product of elements of the groups  $G_\alpha$ . This means that there is a finite sequence  $(x_1, \dots, x_n)$  of elements of the groups  $G_\alpha$  such that  $x = x_1 \cdots x_n$ . Such a sequence is called a word (of length  $n$ ) in the groups  $G_\alpha$ ; it is said to represent the element  $x$  of  $G$ .

**Definition 1.2.2.** A word representing  $x$  of the form  $(y_1, \dots, y_m)$ , where no group  $G_\alpha$  contains both  $y_i$  and  $y_{i+1}$ , and where  $y_i \neq 1$  for all  $i$  is called a reduced word.

**Definition 1.2.3** (free product). Let  $G$  be a group, let  $\{G_\alpha\}_{\alpha \in J}$  be a family of subgroups of  $G$  that generates  $G$ . Suppose that  $G_\alpha \cap G_\beta$  consists of the identity element alone whenever  $\alpha \neq \beta$ . We say that  $G$  is the free product of the groups  $G_\alpha$  if for each  $x \in G$ , there is only one reduced word in the groups  $G_\alpha$  that represents  $x$ . In this case, we write

$$G = \prod_{\alpha \in J}^* G_\alpha,$$

or in the finite case,  $G = G_1 * \cdots * G_n$ .

**Proposition 1.2.4.** Suppose the groups  $G_\alpha$  generate  $G$ , where  $G_\alpha \cap G_\beta = \{1\}$  for  $\alpha \neq \beta$ . In order for  $G$  to be the free product of these groups, it suffices to know that the representation of 1 by the empty word is unique.

**Proposition 1.2.5.** Let  $G$  be a group; let  $\{G_\alpha\}$  be a family of subgroups of  $G$ . If  $G$  is the free product of the groups  $G_\alpha$ , then  $G$  satisfies the following condition: Given any group  $H$  and any family of homomorphisms  $h_\alpha : G_\alpha \rightarrow H$ , there exists a homomorphism  $h : G \rightarrow H$  whose restriction to  $G_\alpha$  equals  $h_\alpha$ , for each  $\alpha$ . Furthermore,  $h$  is unique.

**Definition 1.2.6** (external free product). Let  $\{G_\alpha\}_{\alpha \in J}$  be an indexed family of groups. Suppose that  $G$  is a group, and that  $i_\alpha : G_\alpha \rightarrow G$  is a family of monomorphisms, such that  $G$  is the free product of the groups  $i_\alpha(G_\alpha)$ . Then we say that  $G$  is the external free product of the groups  $G_\alpha$ , relative to the monomorphisms  $i_\alpha$ .

**Proposition 1.2.7** (existence of free product/coproduct in category of Group). Given a family  $\{G_\alpha\}_{\alpha \in J}$  of groups, there exists a group  $G$  and a family of monomorphisms  $i_\alpha : G_\alpha \rightarrow G$  such that  $G$  is the free product of the groups  $i_\alpha(G_\alpha)$ .

*Proof:* We define a word (of length  $n$ ) in the elements of the groups  $G_\alpha$  to be an  $n$ -tuple  $w = (x_1, \dots, x_n)$  of elements of  $\bigcup G_\alpha$ . It is called a reduced word if  $\alpha_i \neq \alpha_{i+1}$  for all  $i$ , where  $\alpha_i$  is the index such that  $x_i \in G_{\alpha_i}$ , and if for each  $i$ ,  $x_i$  is not the identity element of  $G_{\alpha_i}$ . We define the empty set to be the unique reduced word of length zero.

Let  $W$  denote the set of all reduced words in the elements of the groups  $G_\alpha$ . Let  $P(W)$  denote the set of all bijective functions  $\pi : W \rightarrow W$ . Then  $P(W)$  is itself a group, with composition of functions as the group operation. We shall obtain our desired group  $G$  as a subgroup of  $P(W)$ .

Step 1: For each index  $\alpha$  and each  $x \in G_\alpha$ , we define a set map  $\pi_x : W \rightarrow W$ . It will satisfy the following conditions:

(1) If  $x = 1_\alpha$ , the identity element of  $G_\alpha$ , then  $\pi_x$  is the identity map of  $W$ .

(2) If  $x, y \in G_\alpha$  and  $z = xy$ , then  $\pi_z = \pi_x \circ \pi_y$ .

We proceed as follows: Let  $x \in G_\alpha$ . For notational purposes, let  $w = (x_1, \dots, x_n)$  denote the general nonempty element of  $W$ , and let  $\alpha_1$  denote the index such that  $x_1 \in G_{\alpha_1}$ . If  $x \neq 1_\alpha$ , define  $\pi_x$  as follows:

$$\pi_x(\emptyset) = (x),$$

$$\pi_x(w) = (x, x_1, \dots, x_n), \text{ if } \alpha_1 \neq \alpha$$

$$\pi_x(w) = (xx_1, \dots, x_n), \text{ if } \alpha_1 = \alpha, x_1 \neq x^{-1},$$

$$\pi_x(w) = (x_2, \dots, x_n), \text{ if } \alpha_1 = \alpha \text{ and } x_1 = x^{-1}$$

If  $x = 1_\alpha$ , define  $\pi_x$  to be the identity map of  $W$ .

Step 2: We show that if  $x, y \in G_\alpha$  and  $z = xy$ , then  $\pi_z = \pi_x \circ \pi_y$  and  $x \mapsto \pi_x$  is injective.



Step 3: Let  $G$  be the subgroup of  $P(W)$  generated by the groups  $G'_\alpha = i_\alpha(G_\alpha)$ . We show that  $G$  is the free product of the groups  $G'_\alpha$ .

First, we show that  $G'_\alpha \cap G'_\beta$  consists of the identity alone if  $\alpha \neq \beta$ . Let  $x \in G_\alpha$  and  $y \in G_\beta$ ; we suppose that neither  $\pi_x$  nor  $\pi_y$  is the identity map of  $W$  and show that  $\pi_x \neq \pi_y$ . But this is easy, for  $\pi_x(\emptyset) = (x)$  and  $\pi_y(\emptyset) = (y)$ , and these are different words. Second, we show that no nonempty reduced word

$$w' = (\pi_{x_1}, \dots, \pi_{x_n})$$

in the groups  $G'_\alpha$  represents the identity element of  $G$ . Let  $\alpha_i$  be the index such that  $x_i \in G_{\alpha_i}$ ; then  $\alpha_i \neq \alpha_{i+1}$  and  $x_i \neq 1_{\alpha_i}$  for each  $i$ . We compute

$$\pi_{x_1}(\pi_{x_2}(\dots(\pi_{x_n}(\emptyset)))) = (x_1, \dots, x_n),$$

so the element of  $G$  represented by  $w'$  is not the identity element of  $P(W)$ .

**Proposition 1.2.8.** Let  $G = G_1 * G_2$ , where  $G_1$  is the free product of the subgroups  $\{H_\alpha\}_{\alpha \in J}$  and  $G_2$  is the free product of the subgroups  $\{H_\beta\}_{\beta \in K}$ . If the index sets  $J$  and  $K$  are disjoint, then  $G$  is the free product of the subgroups  $\{H_\gamma\}_{\gamma \in J \cup K}$ .

**Proposition 1.2.9** (extension property). Let  $\{G_\alpha\}$  be a family of groups; let  $G$  be a group, let  $i_\alpha : G_\alpha \rightarrow G$  be a family of homomorphisms. The following statements are equivalent:

- (1) If each  $i_\alpha$  is a monomorphism and  $G$  is the free product of the groups  $i_\alpha(G_\alpha)$
- (2) (coproduct) Given a group  $H$  and a family of homomorphisms  $h_\alpha : G_\alpha \rightarrow H$ , there exists a homomorphism  $h : G \rightarrow H$  such that  $h \circ i_\alpha = h_\alpha$  for each  $\alpha$ .

Furthermore,  $h$  is unique if one of above statements holds.

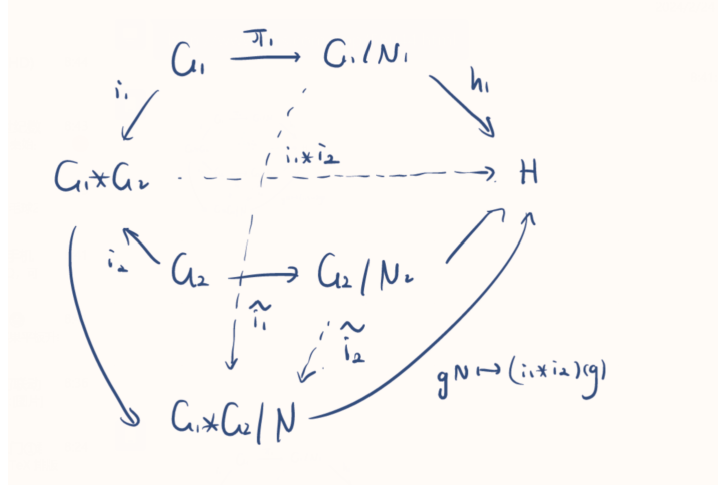
**Proposition 1.2.10** (Uniqueness of free products). Let  $\{G_\alpha\}_{\alpha \in J}$  be a family of groups. Suppose  $G$  and  $G'$  are groups and  $i_\alpha : G_\alpha \rightarrow G$  and  $i'_\alpha : G_\alpha \rightarrow G'$  are families of monomorphisms, such that the families  $\{i_\alpha(G_\alpha)\}$  and  $\{i'_\alpha(G_\alpha)\}$  generate  $G$  and  $G'$ , respectively. If both  $G$  and  $G'$  have the extension property, then there is a unique isomorphism  $\phi : G \rightarrow G'$  such that  $\phi \circ i_\alpha = i'_\alpha$  for all  $\alpha$ .

**Proposition 1.2.11.** If  $S$  is a subset of  $G$ , one can consider the intersection  $N$  of all normal subgroups of  $G$  that contain  $S$ . It is easy to see that  $N$  is itself a normal subgroup of  $G$ ; it is called the least normal subgroup of  $G$  that contains  $S$ . It can also be shown that the subgroup generated by  $\cup_{g \in G} g^{-1}Sg$  is the least normal subgroup of  $G$  that contains  $S$ .

Let  $G = G_1 * G_2$ . Let  $N_i$  be a normal subgroup of  $G_i$ , for  $i = 1, 2$ . If  $N$  is the least normal subgroup of  $G$  that contains  $N_1$  and  $N_2$ , then

$$G/N \cong (G_1/N_1) * (G_2/N_2).$$

*Proof:* By Proposition 1.2.10 and Proposition 1.2.9, it suffice to show  $G_1/N_1 \rightarrow G/N, G_2/N_2 \rightarrow G/N$  satisfies extension property.



**Definition 1.2.12** (free group). Let  $\{a_\alpha\}$  be a family of elements of a group  $G$ . Suppose each  $a_\alpha$  generates an infinite cyclic subgroup  $G_\alpha$  of  $G$ . If  $G$  is the free product of the groups  $\{G_\alpha\}$ , then  $G$  is said to be a free group, and the family  $\{a_\alpha\}$  is called a system of free generators for  $G$ .

In this case, for each element  $x$  of  $G$ , there is a unique reduced word in the elements of the groups  $G_\alpha$  that represents  $x$ . This says that if  $x \neq 1$ , then  $x$  can be written uniquely in the form

$$x = (a_{\alpha_1})^{n_1} \cdots (a_{\alpha_k})^{n_k},$$

**Definition 1.2.13.** Let  $\{a_\alpha\}_{\alpha \in J}$  be an arbitrary indexed family. Let  $G_\alpha$  denote the set of all symbols of the form  $a_\alpha^n$  for  $n \in \mathbb{Z}$ . We make  $G_\alpha$  into a group by defining

$$a_\alpha^n \cdot a_\alpha^m = a_\alpha^{n+m}.$$

Then  $a_\alpha^0$  is the identity element of  $G_\alpha$ , and  $a_\alpha^{-n}$  is the inverse of  $a_\alpha^n$ . We denote  $a_\alpha^1$  simply by  $a_\alpha$ . The external free product of the groups  $\{G_\alpha\}$  is called the free group on the elements  $a_\alpha$ .

**Theorem 1.2.14.** Given  $G$ , suppose we are given a family  $\{a_\alpha\}_{\alpha \in J}$  of generators for  $G$ . Let  $F$  be the free group on the elements  $\{a_\alpha\}$ . Then the obvious map  $h(a_\alpha) = a_\alpha$  of these elements into  $G$  extends to a homomorphism  $h : F \rightarrow G$  that is surjective. If  $N$  equals the kernel of  $h$ , then  $F/N \cong G$ . Each element of  $N$  is called a relation on  $F$ , and  $N$  is called the relations subgroup. We can specify  $N$  by giving a set of generators for  $N$ . But since  $N$  is normal in  $F$ , we can also specify  $N$  by a smaller set. Specifically, we can specify  $N$  by giving a family  $\{r_\beta\}$  of elements of  $F$  such that these elements and their conjugates generate  $N$ , that is, such that  $N$  is the least normal subgroup of  $F$  that contains the elements  $r_\beta$ . In this case, we call the family  $\{r_\beta\}$  a complete set of relations for  $G$ .

**Definition 1.2.15.** The abelianization  $G_{ab}$  of  $G$  is the group defined by

$$G_{ab} = G/[G, G],$$

where  $[G, G]$  is the (normal) subgroup generated by commutators.

**Proposition 1.2.16.**  $f : G \rightarrow H$  is a surjective group homomorphism,  $\tilde{f} : G_{ab} \rightarrow H_{ab}$  is the natural homomorphism induced by  $f$ . Let  $i : G \rightarrow G_{ab}$  be the natural projection. Then  $\text{Ker } \tilde{f} = i(\text{Ker } f)$

**Example 1.2.17.** Consider

$$(1) \ G = \langle a_1, a_2, \dots, a_n \mid a_1^2 \dots a_n^2 = e \rangle$$

$$(2) \ H = \langle a_1, b_1, a_2, b_2, \dots, a_n, b_n \mid [a_1, b_1] \dots [a_n, b_n] = e \rangle$$

Show that  $G_{ab} \simeq \mathbb{Z}^{n-1} \times \mathbb{Z}/2\mathbb{Z}$ , and  $H_{ab} \simeq \mathbb{Z}^{2n}$

*Proof:* For (1), consider the surjective homomorphism  $F = F(a_1, \dots, a_n) \rightarrow G$ , which induces a surjective homomorphism  $\tilde{f} : F_{ab} \rightarrow G_{ab}$ . Then by Proposition 1.2.16,  $G_{ab}$  is isomorphic to  $\mathbb{Z}a_1 \oplus \dots \mathbb{Z}a_n / (2(a_1 + \dots + a_n))$ .

## 1.3 Field Theory

### 1.3.1 Basic Concept

**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

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

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

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

consists of all polynomials of degree  $< n$  in  $\theta$ .

**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  $\alpha$  over  $F$ ,  $K = F(\alpha)$ , then  $K$  is said to be a simple extension of  $F$  and the element  $\alpha$  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  $\alpha$  of  $p(x) : p(\alpha) = 0$ . Let  $F(\alpha)$  denote the subfield of  $K$  generated over  $F$  by  $\alpha$ . Then

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

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

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

**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  $\varphi$  to the coefficients of  $p(x)$ . Let  $\alpha$  be a root of  $p(x)$  (in some extension of  $F$ ) and let  $\beta$  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  $\alpha$  to  $\beta$  and extending  $\varphi$ , i.e., such that  $\sigma$  restricted to  $F$  is the isomorphism  $\varphi$ .

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  $\alpha$  is a root of some nonzero polynomial  $f(x) \in F[x]$ . If  $\alpha$  is not algebraic over  $F$ , then  $\alpha$  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  $\alpha$  be algebraic over  $F$ . Then there is a unique monic irreducible polynomial  $m_{\alpha,F}(x) \in F[x]$  which has  $\alpha$  as a root. A polynomial  $f(x) \in F[x]$  has  $\alpha$  as a root if and only if  $m_{\alpha,F}(x)$  divides  $f(x)$  in  $F[x]$ .

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

$$F(\alpha) \cong F[x]/(m_{\alpha}(x))$$

so that in particular

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

i.e., the degree of  $\alpha$  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  $\alpha$  is an element of an extension of degree  $n$  over  $F$  then  $\alpha$  satisfies a polynomial of degree at most  $n$  over  $F$  and if  $\alpha$  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  $\alpha$  and  $\beta$  is the field generated by  $\beta$  over the field  $F(\alpha)$  generated by  $\alpha$ . In general, if  $a_1, \dots, a_n$  be elements of  $K$ , then  $F(a_1, \dots, a_n) = ((F(a_1)(a_2)) \dots)(a_n)$

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

**Definition 1.3.11** (splitting 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  $\alpha$  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  $f(x)$ .

**Definition 1.3.13.** 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 algebraically closed if every polynomial with coefficients in  $K$  has a root in  $K$ .

**Theorem 1.3.14.** Let  $\bar{F}$  be an algebraic closure of  $F$ . Then  $F$  is algebraically closed.

*Proof:* By Corollary 1.3.10.

**Lemma 1.3.15** (extension of  $F$ -homomorphism for algebraic extension). Let  $\varphi : F \xrightarrow{\sim} F'$  be an isomorphism of fields,  $\bar{F}'$  be the algebraic closure of  $F'$ ,  $E/F$  is a algebraic extension, then there's  $\sigma : E \rightarrow \bar{F}'$  ring homomorphism satisfying  $\sigma|_F = \varphi$ .

*Proof:* By Zorn's Lemma and Theorem 1.3.4.

**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  $\Omega$  is a  $F$ -algebra and  $E_f$  can be embedded into  $\Omega$ . Since  $f$  splits in  $E_f$ , it must also split in the larger field  $\Omega$ . Then all the algebraic elements in  $\Omega$  is therefore an algebraic closure of  $F$ .

Uniqueness: By Lemma 1.3.15.

### 1.3.2 Separable

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

**Definition 1.3.17** (separable). A polynomial  $f(x) \in F[x]$  is separable if  $f(x)$  has no multiple root in  $\bar{F}$ .

**Proposition 1.3.18.** A polynomial  $f(x)$  has a multiple root  $\alpha \in \bar{F}$  if and only if  $\alpha$  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 1.3.19.** 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 1.3.20.**  $\alpha \in \bar{F}$  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  $\alpha \in E$ ,  $\alpha$  is separable.

**Definition 1.3.21** (perfect field). A field  $F \subset \bar{F}$  is perfect if and only if every finite extension of  $F$  is separable.

**Lemma 1.3.22.** 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

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

Hence  $p(x) = \deg p_{\text{sep}} p^k$  and  $\deg p_{\text{sep}}$  is called the separable degree,  $p^k$  is called the inseparable degree of  $P$ .

**Proposition 1.3.23.** 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:* ' $\Leftarrow$ ': case 1: If  $\text{ch} F = 0$ , then by Proposition 1.3.18,  $F$  is perfect.

case 2: If  $\text{ch} F = p$ ,  $\alpha \in \bar{F}$ , and  $p(x) = m_\alpha(x) \in F[x]$  is inseparable, by Lemma 1.3.22, there's irreducible polynomial  $q(x)$  such that  $p(x) = q(x^p)$ . Hence

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

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

' $\Rightarrow$ ': if  $\text{ch} F = p$  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  $\alpha$  is not a  $p$ -th root. Hence  $p(x)$  is irreducible inseparable polynomial, and contradict to the fact  $F$  is perfect!

**Corollary 1.3.24.** In the proof of above Proposition, we can obtain if  $\text{ch} F \neq 0$  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 1.3.25.**  $\mathbb{Q}, \mathbb{F}_q$  are perfect fields and  $\mathbb{F}_p(t)$  is not perfect field.

**Definition 1.3.26.** Given field extensions  $F \subset E \subset \bar{F}$ ,  $E$  is called purely inseparable if for each  $\alpha \in E$  the minimal polynomial of  $\alpha$  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  $\alpha$ ), and  $m_{\alpha, F}(x) = x^{p^n} - \alpha^{p^n}$ .

**Proposition 1.3.27.** Given a field extension  $K/F$ ,  $u \in K$  is separable over  $F$  iff  $F(u) = F(u^p)$ .

*Proof:* We assume  $u$  is separable first. Then  $F_1 = F(u^p) \subseteq F(u)$ . Consider the polynomial  $X^p - u^p \in F_1[X]$  and  $u$  is a root of it. Let  $P$  be the minimal polynomial of  $u$  over  $F_1 \Rightarrow P \mid X^p - u^p$ . But  $X^p - u^p = (X - u)^p$ . Thus  $P = (X - u)^k$  for some integer  $k$ . Since  $P$  is separable and all roots of it are different,  $P = X - u$ . Hence  $u \in F_1$ . Then  $F(u) = F(u^p)$ .

On the other hand, we assume  $F(u) = F(u^p)$ . Let  $P$  be the minimal polynomial of  $u$  over  $F$ . If  $P$  is not separable, then  $P(X) = P_1(X^p)$ . Since  $P_1$  is irreducible and  $P(u^p) = 0$ ,  $P_1$  is the minimal polynomial of  $u^p$ . Then  $[F(u) : F] = [F(u^p) : F] = \deg P = \deg P_1 = p \cdot \deg P_1$ . A contradiction! Hence  $P$  is separable and  $u$  is separable.

**Proposition 1.3.28.** Assume  $[K : F] = d < \infty$ . The following statements are equivalent.

- (1)  $F \subseteq K$  is separable.
- (2)  $K = F \cdot K^p$ , where  $K^p = \{k^p \mid k \in K\}$  a subfield of  $K$  since  $\text{char}(F) = \text{char}(K) = p > 0$ ;
- (3) There is a basis  $\{e_1, \dots, e_d\}$  of  $K$  over  $F$  such that  $\{e_1^p, \dots, e_d^p\}$  is still a basis.

**Proposition 1.3.29.** A simple algebraic extension  $F(u)/F$  is separable iff  $u$  is separable over  $F$ .

*Proof:* If  $P(X) \in F[X]$  is the minimal polynomial of  $u$  over  $F$ ,  $P(X) = \sum_k a_k X^k$  with  $\deg(P) = n$ , then  $\{1, u, \dots, u^{n-1}\}$  form a basis of  $F(u)$  over  $F$ . We prove  $\{1, u^p, \dots, u^{p(n-1)}\}$  is a basis as well.

If this is true, from the Lemma 1.3.28,  $F(u)/F$  is separable.

If this is not true, there will exist  $\{b_k\}$  which are not all zero such that  $\sum_k b_k u^{kp} = 0$ . Let  $P_1(X) = \sum_k b_k X^k$ , with  $\deg(P_1) \leq n - 1$ .  $P_1(u^p) = 0$ . Then  $[F(u^p) : F] \leq \deg(P_1) \leq n - 1$ . But since  $u$  is separable,  $F(u) = F(u^p)$ ,  $[F(u) : F] = [F(u^p) : F] = n$ , a contradiction!

**Proposition 1.3.30.**  $F \subseteq E \subseteq K$  are field extensions.  $K/F$  is separable iff  $E/F$  and  $K/E$  are separable.

*Proof:* We only prove the part of  $\Leftarrow$ . If  $[K : F] < \infty$ ,  $K = E \cdot K^p = (F \cdot E^p) \cdot K^p = F \cdot (E^p \cdot K^p) = F \cdot K^p$ . Hence  $K/F$  is separable.

If  $[K : F] = \infty$ ,  $u \in K$  and  $P_u \in E[X]$  is the minimal polynomial of  $u$  over  $E$ .  $P_u(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0$ . Consider  $F \subseteq F(a_0, \dots, a_{n-1}) \subseteq E \subseteq E(u) \subseteq K$ . Since  $E/F$  is separable, according to the part of  $\Rightarrow$  of 1., we know  $F(a_0, \dots, a_{n-1})/F$  is separable. And since the minimal polynomial of  $u$  over  $F(a_0, \dots, a_{n-1})$  is just  $P_u$ , which is separable. Then  $F(a_0, \dots, a_{n-1}, u)/F(a_0, \dots, a_{n-1})$  is separable. Since  $[F(a_0, \dots, a_{n-1}, u) : F] < \infty$ ,  $F(a_0, \dots, a_{n-1}, u)/F$  is separable and especially  $u$  is separable.



**Definition 1.3.31.** Given an algebraic extension  $K/F$ , all separable elements in  $K$  form a subfield containing  $F$ , which is denoted by  $K_s$ . Especially if  $K = \bar{F}$ ,  $\bar{F}_s$  is denoted by  $F_{sep}$  and called the separable closure. This motivates us to study  $K_s/F$  and  $K/K_s$  respectively, which is the task in the next subsection.

**Proposition 1.3.32.** If  $E/F$  and  $E'/F$  are separable, then  $E \cdot E'/F$  is separable.

**Proposition 1.3.33.** Given a finite algebraic extension  $K/F$ , we have the following equation

$$[K : F]_s = |\text{Hom}_F(K, \bar{F})|$$

More generally, we have

**Corollary 1.3.34.** Let  $\varphi : F \xrightarrow{\sim} F'$  be an isomorphism of fields,  $\bar{F}'$  be the algebraic closure of  $F'$ ,  $E/F$  is a finite separable extension, then there are exactly  $[E : F]$  ways to give an extension  $\sigma : E \rightarrow \bar{F}'$  ring homomorphism satisfying  $\sigma|_F = \varphi$ .

### 1.3.3 Normal

**Definition 1.3.35.** 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 1.3.36.** Let  $F \subset E \subset \bar{F}$  be field extensions. Let  $\text{Aut}(E/F)$  be the collection of automorphisms of  $E$  which fix  $F$ .

**Theorem 1.3.37.** 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  $[E : F] < \infty$ , then the above statements are equivalent to that  $E$  is a splitting field of some  $p(x) \in F[x]$ .

*Proof:* (1) $\implies$ (2) is clear.

(2) $\implies$ (1): By Lemma 1.3.15

Now suppose  $[E : F] < \infty$ . First we assume  $F \subset E$  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  $E = F(u_1, \dots, u_n)$ . 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  $\{u_1, \dots, u_n\}$ . Then  $E = F(u_1, \dots, u_n)$ . Consider an  $F$ -algebra homomorphism  $\iota : F(u_1, \dots, u_n) \rightarrow \bar{F}$ , since  $\iota(u_i)$  is a root of  $P$  as well,  $\iota(u_i) \in E$ . Hence  $\iota(E) \subseteq E$ .

**Proposition 1.3.38.** Given field extensions  $F \subset E \subset \bar{F}$ , then all  $F$ -algebra homomorphisms from  $E$  to  $E$  are in  $\text{Aut}(E/F)$  i.e.  $\text{Aut}(E/F) = \{F\text{-algebra homomorphism between } E \text{ and } E\}$

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

**Proposition 1.3.39.** For field extensions  $F \subseteq E \subseteq K \subseteq \bar{F}$ , if  $K/F$  is normal then  $K/E$  is normal.

**Proposition 1.3.40.** If  $E/F$  and  $E'/F$  are normal, then  $E \cdot E'/F$  is normal.

### 1.3.4 Galios

**Definition 1.3.41.** Let  $E/F$  be a finite extension. Then  $E$  is said to be Galois over  $F$  and  $E/F$  is a Galois extension if it is separable and normal.

**Theorem 1.3.42** (Fundamental Theorem of Galois Theory).  $F \subset K \subset \bar{F}$  be field extensions.  $K/F$  be a Galois extension and set  $G = \text{Gal}(K/F)$ . 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)  $K/E$  is always Galois.
- (2) there's a one-to-one correspondence:

$$\begin{array}{ccc}
 \{F\text{-algebra homomorphism between } E \text{ and } \bar{F}\} & & \\
 \uparrow \sigma H \mapsto \sigma|_E & \searrow \text{Extended by 1.3.15 and 1.3.38} & \\
 \{\text{left cosets of } H \text{ in } G\} & \xrightarrow{\sigma H \mapsto \sigma|_E} & \{\sigma|_E : \sigma \in G\}
 \end{array}$$

- (3) (inclusion reversing) If  $E_1, E_2$  correspond to  $H_1, H_2$ , respectively, then  $E_1 \subseteq E_2$  if and only if  $H_2 \leq H_1$
- (4)  $[K : E] = |H|$  and  $[E : F] = [G : H]$

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

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

In particular, by Theorem 1.3.37,  $E$  is normal(hence Galois) 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

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

(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  $E_1 E_2$  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 1.3.43.** Suppose  $K/F$  is a Galois extension and  $F'/F$  is any extension. Then  $KF'/F'$  is a Galois extension, with Galois group

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

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

**Corollary 1.3.44.** 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 1.3.45.** 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  $K_1 K_2$  is Galois over  $F$ . The Galois group is isomorphic to the subgroup

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

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

**Corollary 1.3.46.**  $F \subseteq E \subseteq F_{sep} \subseteq \bar{F}$  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 Galois extension of  $F$  which contains  $E$ , then

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

is actually finite many intersection of Galois extension of  $F$  which contains  $E$  by Fundamental Theorem of Galois Theory.

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

**Corollary 1.3.47.** If  $K/F$  is finite and separable, then  $K/F$  is simple. In particular, any finite extension of fields of characteristic 0 is simple.

**Proposition 1.3.48.**  $\bar{F}/F_{sep}$  is purely inseparable extension and  $F_{sep}$  is separable and normal extension.

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

**Definition 1.3.49.**

A subset  $\{a_1, a_2, \dots, a_n\}$  of  $E$  is called algebraically independent over  $F$  if there is no nonzero polynomial

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

such that  $f(a_1, a_2, \dots, a_n) = 0$ . 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  $F$ .

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

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

**Definition 1.3.50.** The cardinality of a transcendence base for  $E/F$  is called the transcendence degree of  $E/F$ .

**Proposition 1.3.51.**  $E/F$  be a field extension,  $\alpha_1, \dots, \alpha_n \in E$ ,  $F_i = F(\alpha_1, \dots, \alpha_i)$ , then  $\{\alpha_1, \dots, \alpha_n\}$  is algebraically independent over  $F$ , if and only if  $\alpha_i$  is transcendental over  $F_{i-1}$  for all  $i = 1, \dots, n$ .

# Chapter 2

## Commutative Algebra

### 2.1 Basic Definition in Ring Thoery

**Definition 2.1.1.** 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 2.1.2.** 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 2.1.3.** If  $I$  is a proper ideal then there exists at least one maximal ideal containing  $I$ .

**Definition 2.1.4.** 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 2.1.5.** A field  $F$  is an integral doamin such that every non-zero element in  $F$  is invertible.

**Definition 2.1.6.** 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 2.1.7.** 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

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

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

given by the correspondences

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

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

where  $\pi$  be the natural homomorphism from  $A$  to  $A/I$ .

**Definition 2.1.8.** A subset  $S$  of  $A$  is multiplicative if it satisfies:

- (1)  $x, y \in S \Rightarrow xy \in S$ .
- (2)  $1 \in S$ .

**Definition 2.1.9.** 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 2.1.10.** the radical  $\sqrt{I}$  of  $I$  is the intersection of all prime ideals containing  $I$ .

*Proof:*

**Lemma 2.1.11.** 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!  $\square$

If  $x \notin \sqrt{I}$ ,  $S_x = x^n : n \geq 0$  be a multiplicative subset. By lemma 2.1.11, we can find a prime ideal which contains  $I$  disjoint from  $S_x$ .

**Definition 2.1.12.** 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  $\text{nil}(A)$  for this. When  $\text{nil}(A) = 0$  we say that  $A$  is reduced, For any ring  $A$  we write  $A_{\text{red}}$  for  $A/\text{nil}(A)$  is of course reduced.

**Definition 2.1.13.** 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  $\text{rad}(A)$ .

**Proposition 2.1.14.**  $x \in \text{rad}(A)$  if and only if  $1 + xy$  is a unit in  $A$  for all  $y \in A$ .

**Definition 2.1.15.** 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,  $m = \text{rad}(A)$  and  $k = A/m$ .

**Proposition 2.1.16.** 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 2.1.17.** If  $I_1, I_2, \dots, I_n$  are ideals which are coprime (i.e.  $I_i + I_j = A$  for all  $i \neq j$ ) in pairs then  $I_1 I_2 \dots I_n = I_1 \cap I_2 \cap \dots \cap I_n$

**Theorem 2.1.18** (Chinese Remainder Theorem). If  $I_1, \dots, I_n$  are ideals which are coprime in pairs then

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

and the isomorphism map is given by

$$a + I_1 \cdots I_n \rightarrow (a + I_1, \dots, a + I_n)$$

**Theorem 2.1.19** (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  $1 \leq i \leq n$ .

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

*Proof:* (2): If  $P \supset IJ$  and  $P \not\supset I$ , 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 2.1.20.** 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 2.1.21.** In an integral domain, a prime element is always irreducible.

**Definition 2.1.22** (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  $R$ :  $r = p_1 \cdots p_n$
- (2) the decomposition in (1) is unique up to associates.

**Proposition 2.1.23.** An integral 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 2.1.24** (P.I.D). A Principal Ideal Domain is an integral domain in which every ideal is principal.

**Proposition 2.1.25.** Every Principal Ideal Domain is a Unique Factorization Domain.

**Proposition 2.1.26.** If  $F$  is a field, then  $F[x]$  is a Principal Ideal Domain.

**Lemma 2.1.27** (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 2.1.28.** 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 2.1.29.** If  $R$  is a U.F.D, then  $R[x]$  is a U.F.D.

*Proof:* By Proposition 2.1.26, Lemma 2.1.27 and Corollary 2.1.28.

**Corollary 2.1.30** (Eisenstein's criterion).  $R$  is a U.F.D.,  $p(x) = a_n x^n + \cdots + a_1 x^1 + a_0 \in R[x]$  is a irreducible polynomial if there's some  $p \in R$  such that  $p \nmid a_n, p \mid a_{n-1} \dots, a_0, p^2 \nmid a_0$



## 2.2 Basic Definition in Module

**Proposition 2.2.1.** 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:

$$\begin{aligned} R &\rightarrow \text{End}(M) \\ r &\rightarrow (x \rightarrow rx) \end{aligned}$$

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

$$\begin{aligned} R \times M &\rightarrow M \\ (r, m) &\rightarrow f(r)m \end{aligned}$$

is a  $R$ -module structure.

**Remark 2.2.2.** By Proposition 2.2.1, if we have a  $B$ -mdule  $M$  and a ring homomorphism  $f : A \rightarrow B$ ,  $M$  has naturally a  $A$ -module structure.

**Definition 2.2.3.**  $f : R \rightarrow B$  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  $R$ -algebra category between object  $(A, f : R \rightarrow A)$  and  $(B, g : R \rightarrow B)$ , is the ring homomorphism  $h : A \rightarrow B$  making the following diagram commute:

$$\begin{array}{ccc} A & \xrightarrow{h} & B \\ & \swarrow f \quad \searrow g & \\ & R & \end{array}$$

**Definition 2.2.4.** 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  $\text{Ann}(M)$ . We can consider  $M$  as a module over  $A/\text{Ann}(M)$ . If  $\text{Ann}(M) = 0$ , we say that  $M$  is a faithful  $A$ -module. For  $x \in M$ , we write  $\text{Ann}(x) = \{a \in A : ax = 0\}$ .

**Definition 2.2.5.** 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 2.2.6** (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  $a \equiv 1 \pmod{I}$ . If in addition  $I \subset \text{rad}(A)$ , then  $M = 0$ .

**Corollary 2.2.7.**  $(A, m)$  be a Notherian local ring. If  $A = mA$ , then  $A = 0$ .

**Corollary 2.2.8.** Let  $A$  be a ring and  $I$  an ideal contained in  $\text{rad}(A)$ . 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 2.2.6.

**Definition 2.2.9.** 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 2.2.10.** Let  $(A, m, k)$  be a local ring and  $M$  a finite  $A$ -module; set  $\bar{M} = M/mM$ . Now  $\bar{M}$  is a finite-dimensional vector space over  $k$ , and we write  $n$  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 2.2.8

(3): By Proposition 2.1.16

**Theorem 2.2.11** (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  $\varphi : F \rightarrow M$  from the free module  $F = Ae_1 \oplus \dots \oplus Ae_n$  to  $M$  by  $\varphi(\sum a_i e_i) = \sum a_i \omega_i$ ; if we set  $K = \text{Ker}(\varphi)$  then, from the minimal basis property(1),

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

Thus  $K \subset mF$ . Because  $M$  is projective, there exists  $\psi : M \rightarrow F$  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 2.2.12.** Let  $A$  be a ring  $\neq 0$ . Show that if  $A^m \simeq A^n$ , then  $m = n$ .

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

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

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

$$A^p \rightarrow A^q \rightarrow M \rightarrow 0.$$

**Proposition 2.2.14.** Let  $A$  be a ring, and suppose that  $M$  is an  $A$ -module of finite presentation. If

$$0 \rightarrow K \rightarrow N \rightarrow M \rightarrow 0$$

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

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

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

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  $0 = \varphi\alpha\left(\sum a_i v_i\right) = f\left(\sum a_i v_i\right)$ , 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 2.2.15.** Let  $A$  be a ring and let  $A[x]$  be the ring of polynomials with coefficients in  $A$ .  $A[[x]]$  be the ring of formal power series. Let  $f = a_0 + a_1x + \cdots + a_nx^n \in A[x]$ ,  $g = \sum_{n=0}^{\infty} b_nx^n$ . Prove that

- (1)  $f$  is a unit in  $A[x] \Leftrightarrow a_0$  is a unit in  $A$  and  $a_1, \dots, a_n$  are nilpotent.
- (2)  $f$  is nilpotent  $\Leftrightarrow a_0, a_1, \dots, a_n$  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)  $g$  is a unit in  $A[[x]] \Leftrightarrow b_0$  is a unit in  $A$ .
- (5)  $g$  is nilpotent, then  $b_n$  are all nilpotent.

**Definition 2.2.16** (The Ring of Formal Laurent Series). The ring of formal Laurent series in  $x$  with coefficients in  $R$  is denoted by  $R((x))$ , and is defined as follows. The elements of  $R((x))$  are infinite expressions of the form

$$f(x) = a_rx^r + a_{r+1}x^{r+1} + a_{r+2}x^{r+2} + \cdots$$

in which  $r \in \mathbb{Z}$  and  $a_n \in R$  for all  $n \geq r$ .

**Proposition 2.2.17.** If  $R$  is a field then  $R((x))$  is a field.

*Proof:* Consider a nonzero  $f(x) = \sum_{n=I(f)}^{\infty} a_n x^n$  in  $R((x))$ . Then  $a_{I(f)} \neq 0$  so that it is invertible in  $R$ , since  $R$  is a field. We may write  $f(x) = x^{I(f)} g(x)$  with  $g(x) = \sum_{n=0}^{\infty} a_{n+I(f)} x^n$ , so that  $g(x)$  is a formal power series in  $R[[x]]$ . The coefficient of  $x^0$  in  $g(x)$  is  $a_{I(f)}$  and, it follows that  $g(x)$  is invertible in  $R[[x]]$ , and hence in  $R((x))$ . Let  $h(x) := x^{-I(f)} g^{-1}(x)$ . Then

$$f(x)h(x) = x^{I(f)} g(x) x^{-I(f)} g^{-1}(x) = 1$$

so that  $h(x) = f^{-1}(x)$  and  $f(x)$  is invertible in  $R((x))$ . Therefore,  $R((x))$  is a field.

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

**Definition 2.2.18.** Let  $R$  be a ring, let  $A_R$  be a right  $R$ -module, let  ${}_R B$  be a left  $R$  module, and let  $G$  be an (additive) abelian group. A function  $f : A \times B \rightarrow G$  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  $f : A \times B \rightarrow M$  is called  $R$ -bilinear if  $f$  is  $R$ -biadditive and also

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

**Definition 2.2.19** (Tensor product). Given a ring  $R$  and modules  $A_R$  and  ${}_R B$ , then their tensor product is an abelian group  $A \otimes_R B$  and an  $R$ -biadditive function  $h : A \times B \rightarrow A \otimes_R B$

$$\begin{array}{ccc} A \times B & & \\ \downarrow h & \searrow f & \\ A \otimes_R B & \xrightarrow{\tilde{f}} & G \end{array}$$

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

**Proposition 2.2.20.** 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  $h : A \times B \rightarrow A \otimes_R B$  is  $R$ -bilinear, and, for every  $R$ -module  $M$  and every  $R$ -bilinear function  $g : A \times B \rightarrow M$ , there exists a unique  $R$ -homomorphism  $\tilde{g} : A \otimes_R B \rightarrow M$  making the following diagram commute.

$$\begin{array}{ccc} A \times B & & \\ \downarrow h & \searrow g & \\ A \otimes_R B & \xrightarrow{\tilde{g}} & M \end{array}$$

**Proposition 2.2.21.**  $A$  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 2.2.22.** If  $R$  is a ring, and  $A, B$  are  $R$ -modules, then there are  $R$ -module isomorphisms:

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

**Theorem 2.2.23.** If  $R$  and  $S$  are rings and  $A_R, {}_R B_S, S_C$  are (bi)modules, then there is an isomorphism:

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

**Theorem 2.2.24** (Commutativity). If  $R$  is a commutative ring and  $M_R, {}_R N$  are modules, then there is a  $R$ -isomorphism

$$\tau : M \otimes_R N \rightarrow N \otimes_R M$$

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

$$\begin{array}{ccc} M \otimes_R N & \xrightarrow{\tau} & N \otimes_R M \\ f \otimes g \downarrow & & \downarrow g \otimes f \\ M' \otimes_R N' & \xrightarrow{\tau'} & N' \otimes_R M' \end{array}$$

**Theorem 2.2.25.** 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:

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

**Theorem 2.2.26** (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 a natural bijection (actually a isomorphism of abelian groups):

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

given by

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

and

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

**Remark 2.2.27.** 'natrual' in above theorem means:  ${}_R B_S$  is a bi-module, then  $(\_\otimes_R B, \text{Hom}_S(B, \_))$  is a adjoint pair between right  $R$ -module category and right  $S$ -module category.

**Remark 2.2.28.** (1) If  ${}_R B_S$  is a bi-module,  $C$  is a right  $R$ -module,  $\text{Hom}_S(B, C)$  has a natrual right  $R$ -module sturct. Notice that we can define  $fr(b) = f(rb)$ , then  $fr(bs) = f(r(bs)) = f((rb)s) = f(rb)s = (fr(b))s, f(r_1 r_2)(b) = (fr_1)r_2(b)$ . It makes  $\text{Hom}_S(B, C)$  to be a right  $R$ -module.

- (2) If  ${}_S B_R$  is a bi-module,  $C$  is a left  $S$ -module, then  $\text{Hom}_S(B, C)$  has a natural left  $R$ -module structure.
- (3) If  ${}_S B_R$  is a bi-module,  $C$  is a left  $S$ -module, then  $B \otimes_R A$  has a natural left  $S$ -module structure.

**Proposition 2.2.29.** If  $M$  is a left  $R$ -module, then there's left  $R$ -module isomorphism

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

**Theorem 2.2.30.** Let  $R$  be a ring with. If  $A$  is a right  $R$ -module and  $F$  is a free left  $R$ -module with basis  $Y$ , then every element  $u$  of  $A \otimes_R F$  may be written uniquely in the form  $u = \sum_{i=1}^n a_i \otimes y_i$ , where  $a_i \in A$  and the  $y_i$  are distinct elements of  $Y$ .

**Theorem 2.2.31.** If  $R$  is a ring with identity and  $A_R$  and  ${}_R B$  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 2.2.32.** 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 2.2.33** (The Short Five Lemma). Let  $R$  be a ring and

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

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

- (1)  $\alpha, \gamma$  monomorphisms  $\Rightarrow \beta$  is a monomorphism (injective);
- (2)  $\alpha, \gamma$  epimorphisms  $\Rightarrow \beta$  is an epimorphism (surjective);
- (3)  $\alpha, \gamma$  isomorphisms  $\Rightarrow \beta$  is an isomorphism.

**Definition 2.2.34** (Split exact sequence). Let  $R$  be a ring and  $0 \rightarrow A_1 \xrightarrow{f} B \xrightarrow{g} A_2 \rightarrow 0$  a short exact sequence of  $R$ -module homomorphisms. Then the following conditions are equivalent:

- (1) There is an  $R$ -module homomorphism  $h : A_2 \rightarrow B$  with  $gh = 1_{A_2}$ ;
- (2) There is an  $R$ -module homomorphism  $k : B \rightarrow A_1$  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  $0 \rightarrow A_1 \xrightarrow{l_1} A_1 \oplus A_2 \xrightarrow{\pi_2} A_2 \rightarrow 0$ ; in particular  $B \simeq A_1 \oplus A_2$ .

(4)

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

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

(5)

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

is a split 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 2.2.35** (Snake lemma). Let

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

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

$$\begin{array}{ccccccc} 0 & \longrightarrow & \operatorname{Ker}(f') & \xrightarrow{\bar{u}} & \operatorname{Ker}(f) & \xrightarrow{\bar{v}} & \operatorname{Ker}(f'') \\ & & & & & \swarrow d & \\ & & \operatorname{Coker}(f') & \xleftarrow{\bar{u}'} & \operatorname{Coker}(f) & \xrightarrow{\bar{v}'} & \operatorname{Coker}(f'') \longrightarrow 0 \end{array}$$

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  $x'' \in \operatorname{Ker}(f'')$ , 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  $\operatorname{Coker}(f')$ .

**Proposition 2.2.36.**

(1)

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

is any short exact sequence of  $R$ -modules, if and only if for all  $R$ -module  $D$

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

is an exact sequence of abelian groups. ( $\operatorname{Hom}(D, \square)$  is left exact in  $\{R\text{-module}\}$ )

(2)

$$0 \leftarrow C \xleftarrow{g} B \xleftarrow{f} A$$

is any short exact sequence of  $R$ -modules, is any short exact sequence of  $R$ -modules, if and only if for all  $R$ -module  $D$

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

is an exact sequence of abelian groups. ( $\operatorname{Hom}(\square, D)$  is left exact in  $(\{R\text{-module}\})^{opp}$ .)



**Definition 2.2.37** (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.

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

- (2) every short exact sequence  $0 \rightarrow A \xrightarrow{f} B \xrightarrow{g} P \rightarrow 0$  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  $f : B \rightarrow C$  is any  $R$ -module epimorphism then  $\bar{f} : \text{Hom}_R(P, B) \rightarrow \text{Hom}_R(P, C)$  is an epimorphism of abelian groups;
- (5) if

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

is any short exact sequence of  $R$ -modules, then

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

is an exact sequence of abelian groups. ( $\text{Hom}(P, \square)$  is exact in  $\{R\text{-module}\}$ )

**Proposition 2.2.38.** Every free module  $F$  over a ring  $R$  is projective.

**Proposition 2.2.39.** 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 2.2.40.** 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 2.2.41** (Injective module). Let  $R$  be a ring, the following conditions on a  $R$ -module  $J$  are equivalent:

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

$$\begin{array}{ccccc} & & J & & \\ & \nwarrow h & \uparrow f & & \\ A & \xleftarrow{g} & B & \longleftarrow & 0 \end{array}$$

- (2) every short exact sequence  $0 \rightarrow J \xrightarrow{f} B \xrightarrow{g} C \rightarrow 0$  is split exact.
- (3) If  $J$  is a submodule of  $B$ , then there's submodule  $K$  such that  $B = J \oplus K$ .

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

(5) if

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

is any short exact sequence of  $R$ -modules, then

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

is an exact sequence of abelian groups.

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

**Proposition 2.2.42.** A direct product of  $R$ -modules  $\prod_{i \in I} J_i$  is injective if and only if  $J_i$  is injective for every  $J_i, i \in I$ .

**Proposition 2.2.43.** 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 2.2.44.** 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 2.2.45.** Let  $R$  be a ring and let  $M$  be an  $R$ -module. Then  $M$  is contained in an injective  $R$ -module.

**Proposition 2.2.46.** Any modules over a PID, it is a projective module if and only if it is a free module.

**Definition 2.2.47** (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  $0 \rightarrow L \xrightarrow{\psi} M$  is an exact sequence of left  $R$ -modules (i.e.,  $\psi : L \rightarrow M$  is injective) then  $0 \rightarrow A \otimes_R L \xrightarrow{1 \otimes \psi} A \otimes_R M$  is an exact sequence of abelian groups (i.e.,  $1 \otimes \psi : A \otimes_R L \rightarrow A \otimes_R M$  is injective).

Similarly, we can define left flat  $R$ -module.

**Proposition 2.2.48.** Projective modules are flat.

**Example 2.2.49.**  $\mathbb{Q}/\mathbb{Z}$  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

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

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

*Proof:* Since tensor product commute with direct sum.

**Example 2.2.51.**

	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{Q}/\mathbb{Z}$	$\mathbb{Z} \oplus \mathbb{Q}$
flat	✓	✓ (By 2.7.2)	× (2.2.49)	✓ (2.2.50)
projective	✓	× (By 2.2.46)	×	× (2.2.39)
injective	× (By 2.2.43)	✓ (By 2.2.43)	✓ (By 2.2.43)	× (2.2.42)

## 2.3 Specturm

**Proposition 2.3.1.** 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)  $V(\emptyset) = X, V((1)) = \emptyset$
- (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  $\text{Spec}(A)$ .

*Proof:* By Theorem 2.1.19

**Proposition 2.3.2.**  $X = \text{Spec}(A)$ ,  $D(f) = X - V(f)$ .

- (1)  $D(f)$  form a basis of  $X$ .
- (2)  $D(fg) = D(f) \cap D(g)$ .
- (3)  $D(f)$  is compact.
- (4)  $D(f) = \emptyset \Leftrightarrow f$  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  $X = \text{Spec} A$

**Proposition 2.3.3.** 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  $X = \text{Spec} A$ . 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  $\text{Spec}(A)$  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 2.3.4.** A topological space  $X$  is said to be irreducible if  $X \neq \emptyset$  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 2.3.5.** Let  $X$  be a topological space.

- (1) If  $Y$  is an irreducible subspace of  $X$ , then the closure  $\overline{Y}$  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 2.3.6.**  $A$  is a ring,  $\text{Spec}A$  is the spectrum of  $A$ .

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

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

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

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

given by the correspondences

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

**Corollary 2.3.7.**  $X = \text{Spec}(A)$  is irreducible if and only if the nilradical of  $A$  is a prime ideal.

**Proposition 2.3.8.** Let  $\varphi : A \rightarrow B$  be a ring homomorphism. Let  $X = \text{Spec}A$  and  $Y = \text{Spec}B$ . Let  $\phi$  to be the map:

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

- (1) If  $f \in A$ , then  $\phi^{-1}(X_f) = Y_{\varphi(f)}$ , and hence  $\phi$  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  $\varphi$  is surjective, then  $\phi$  is a homeomorphism of  $Y$  onto the closed subset  $V(\text{Ker}(\phi))$  of  $X$ .

**Definition 2.3.9.** 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 2.3.10.** If  $X = \text{Spec } A$  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 2.3.11.** A topological space is called Noetherian if it satisfies one of the following equivalent conditions

- (1) descending chain of closed subsets becomes stationary.
- (2) ascending chain of open subsets becomes stationary.
- (3) every non-empty set of open subsets of  $X$  has a maximal element.
- (4) every non-empty set of closed subsets of  $X$  has a minimal element.

**Example 2.3.12.**  $R$  is a Noetherian ring, then  $X = \text{Spec}(R)$  is a Noetherian space.

*Proof:* By Theorem 2.3.6

**Theorem 2.3.13** (Decomposition into irreducibles). Let  $X$  be a Noetherian topological space.

- (1) There exist a nonnegative integer  $n$  and closed, irreducible subsets  $Z_1, \dots, Z_n \subset X$  such that  $X = Z_1 \cup \dots \cup Z_n$  and  $Z_i \not\subseteq Z_j$  for  $i \neq j$ .
- (2) If  $Z_1, \dots, Z_n$  are closed, irreducible subsets satisfying (1), then every irreducible subset  $Z \subset X$  is contained in some  $Z_i$ .
- (3) If  $Z_1, \dots, Z_n \subset X$  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.

**Proposition 2.3.14.** Let  $X$  be a Noetherian topological space.

- (1) Every subspace of  $X$  is noetherian.
- (2) Every subset of  $X$  is quasi-compact (in particular,  $X$  is quasi-compact).

*Proof:* (1): Let  $(Z_i)_i$  be a descending chain of closed subsets of a subspace  $Y$ . Then the closures  $\bar{Z}_i$  of  $Z_i$  in  $X$  form a descending chain of closed subsets of  $X$  which becomes stationary by hypothesis. As we have  $Z_i = Y \cap \bar{Z}_i$ , this shows that the chain  $(Z_i)_i$  becomes stationary as well. This proves (1).

(2): By (1) it suffices to show that  $X$  is quasi-compact. Let  $(U_i)_i$  be an open covering of  $X$  and let  $\mathcal{U}$  be the set of those open subsets of  $X$  that are finite unions of the subsets  $U_i$ . As  $X$  is noetherian,  $\mathcal{U}$  has a maximal element  $V$ . Clearly  $V = X$ , otherwise there would exist an  $U_i$  such that  $V \subsetneq V \cup U_i \in \mathcal{U}$ . This shows that  $(U_i)_i$  has a finite subcovering.

**Corollary 2.3.15.** A Noetherian ring has only finite many minimal prime ideals.

*Proof:* By Example 2.3.15 and Theorem 2.3.13.

**Proposition 2.3.16.** Let  $X$  be a topological space that has a finite covering  $X = \bigcup_{i=1}^r X_i$  by noetherian subspaces. Then  $X$  itself is noetherian.

**Proposition 2.3.17.** Let  $X$  be a topological space and let  $X = \bigcup_{i \in I} U_i$  be an open covering of  $X$  by connected open subsets  $U_i$ .

- (1) If  $X$  is not connected, then there exists a subset  $\emptyset \neq J \subsetneq I$  such that for all  $j \in J$ ,  $i \in I \setminus J, U_j \cap U_i = \emptyset$ .
- (2) If  $X$  is connected,  $I$  is finite, and all the  $U_i$  are irreducible, then  $X$  is irreducible.

## 2.4 Chain conditions

**Definition 2.4.1** (Noetherian). 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 2.4.2** (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 2.4.3.** Let  $0 \rightarrow M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \rightarrow 0$  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 2.4.4.** If  $M_i (1 \leq i \leq n)$  are Noetherian (resp. Artinian)  $A$ -modules, so is  $\bigoplus_{i=1}^n M_i$ .

*Proof:* Apply Theorem 2.4.3 to the exact sequence

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

**Corollary 2.4.5.** Let  $A$  be a Noetherian (resp. Artinian) ring,  $M$  a finitely generated  $A$ -module. Then  $M$  is Noetherian (resp. Artinian).

**Definition 2.4.6.** A chain of submodules of a module  $M$  is a sequence  $(M_i) (0 \leq i \leq n)$  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  $M_{i-1}/M_i (1 \leq i \leq n)$  is simple (that is, has no submodules except 0 and itself).

**Proposition 2.4.7.** 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 2.4.8.**  $M$  has a composition series  $\Leftrightarrow M$  satisfies both chain conditions.



**Proposition 2.4.9.** If  $A$  is a Artinian ring,  $A$  has only finitely many maximal ideals.

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

$$P_1 \supset P_1 P_2 \cdots \supset P_1 \cdots P_n \supset \dots$$

By Theorem 2.1.19, each ' $\supset$ ' is strict. A contradiction!

**Proposition 2.4.10.** A ring  $A$  is Artinian, then the product of all its maximal ideals is nilpotent.

*Proof:*

**Proposition 2.4.11.** A ring  $A$  is Artinian, then  $A$  is Notherian.

**Proposition 2.4.12.** Let  $A$  be a ring and  $M$  an  $A$ -module. Then if  $M$  is a Noetherian module,  $A/\text{Ann}(M)$  is a Noetherian ring.

*Proof:* If we set  $\bar{A} = A/\text{Ann}(M)$  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  $\text{Ann}(M) = (0)$ . Now letting  $M = A\omega_1 + \cdots + A\omega_n$ , we can embed  $A$  in  $M^n$  by means of the map  $a \mapsto (a\omega_1, \dots, a\omega_n)$ . By Theorem 1,  $M^n$  is a Noetherian module, so that its submodule  $A$  is also Noetherian.

**Theorem 2.4.13** (Hilbert basis theorem).  $R$  is Notherian, then  $R[x]$  and  $R[[x]]$  are Notherian.

**Corollary 2.4.14.** Let  $B$  be a finitely-generated  $A$ -algebra. If  $A$  is Noetherian, then so is  $B$ .

*Proof:* By Hilbert basis theorem and Theorem 2.4.3.

**Theorem 2.4.15** (Cohen). If all the prime ideals of a ring  $A$  are finitely generated then  $A$  is Noetherian.

**Definition 2.4.16** (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 2.4.17.** An invertible fractional ideal of  $A$  is finitely generated as an  $A$ -module. Conversely, if  $A$  is Noetherian, every fractional ideal is finitely generated.

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

## 2.5 Localization

**Definition 2.5.1** (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  $\varphi_S : R \rightarrow S^{-1}R$  be the map given by  $\varphi_S(x) = x/1$ . Then  $\varphi_S$  is a ring homomorphism between  $R$  and  $S^{-1}R$

**Example 2.5.2** (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 2.5.3** (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 2.5.4.** Let  $f : A \rightarrow B$  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 2.5.5.** 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 2.5.6.**  $A$  is Notherian, then  $S^{-1}A$  is Notherian.

**Proposition 2.5.7.** 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)  $I \cap S \neq \emptyset$
- (3)  $\varphi_S^{-1}(S^{-1}I) = R$

*Proof:* Obviously,  $S^{-1}I$  is the ideal generated by  $\varphi_S(I)$ .

(1) $\Rightarrow$ (2): Consider  $1/1 \in S^{-1}I$ .

(2) $\Rightarrow$ (3): Take  $a \in I \cap S$ , notice that  $a/a = 1/1$ .

(3) $\Rightarrow$ (1): Consider  $1/1 \in S^{-1}I$ .

**Proposition 2.5.8.** Let  $R$  be a ring,  $S$  be a multiplicative subset of  $R$ , there's a one-to-one order-preserving bijection:

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

given by the following maps:

$$\begin{aligned} P &\longrightarrow S^{-1}P \\ \varphi_S^{-1}(\bar{P}) &\longrightarrow \bar{P} \in \text{Spec}(S^{-1}R) \end{aligned}$$

*Proof:* Step 1 (well-defined): If  $P \in \text{Spec}(R)$  and  $P \cap S = \emptyset$ , 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 2.5.9** (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 2.5.10.**  $S^{-1}M$  has both  $A$ -module structure and  $S^{-1}A$ -module structure by the natural way:

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

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

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

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

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

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

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

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 2.5.11.** It follows from Proposition 2.5.10 that if  $N$  is a submodule of  $M$ , the map  $S^{-1}M \xrightarrow{S^{-1}f} S^{-1}M$  is injective, where  $f : N \rightarrow M$  be the embedding. Therefore  $S^{-1}N$  can be regarded as a submodule of  $S^{-1}M$ .

**Remark 2.5.12.** If  $P$  is a prime ideal of  $A$ ,  $S = A - P$ ,  $f : M \rightarrow N$  be a  $A$ -module homomorphism, we usually denote  $S^{-1}f$  by  $f_P$ .

**Proposition 2.5.13.** 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  $S^{-1}f : S^{-1}M \rightarrow S^{-1}(M/N)$  given by the natural homomorphism  $f : M \rightarrow M/N$  is surjective. In particular,  $S^{-1}M/S^{-1}N \simeq S^{-1}(M/N)$  as  $S^{-1}A$ -module and  $A$ -module.

**Theorem 2.5.14.** 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 isomorphism map is given by the bi-linear map:

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

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

and the universal property of tensor product.

**Remark 2.5.15.** ‘naturally’ in above theorem means: given two covariant functors:  $S^{-1}A \otimes \_$  and  $S^{-1}\_$ , then the isomorphism map induced by  $\varphi$  induce a natural transformation between these two functors.

**Proposition 2.5.16** (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:*

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

**Proposition 2.5.17** ( $M=0$  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 2.5.18** (injective homomorphism is a local property). Let  $f : M \rightarrow N$  be  $A$ -module homomorphism,  $f_P : M_P \rightarrow N_P$  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 2.5.19** (flat is a local property). Let  $f : M \rightarrow N$  be  $A$ -module homomorphism,  $f_P : M_P \rightarrow N_P$  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 2.5.20.** Let  $M$  be a finitely generated  $A$ -module,  $S$  a multiplicatively closed subset of  $A$ . Then  $S^{-1}(\text{Ann}(M)) = \text{Ann}(S^{-1}M)$ .

**Definition 2.5.21** (support of a module). Let  $A$  be a ring,  $M$  an  $A$ -module. The support of  $M$  is defined to be the set  $\text{Supp}(M) = \{P \in \text{Spec}(A) : M_P \neq 0\}$ .

**Proposition 2.5.22.**  $M$  is a  $R$ -module,  $A$  is a ring,  $I$  is an ideal of  $A$ .

- (1)  $M \neq 0 \Leftrightarrow \text{Supp}(M) \neq \emptyset$
- (2)  $V(I) = \text{Supp}(A/I)$
- (3) If  $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$  is an exact sequence, then  $\text{Supp}(M) = \text{Supp}(M') \cup \text{Supp}(M'')$ .
- (4) If  $M$  is finitely generated, then  $\text{Supp}(M) = V(\text{Ann}(M))$
- (5) If  $M, N$  are finitely generated, then  $\text{Supp}(M \otimes_A N) = \text{Supp}(M) \cap \text{Supp}(N)$ .
- (6) If  $M = \sum_{i \in I} M_i$ , then  $\text{Supp}(M) = \bigcap_{i \in I} \text{Supp}(M_i)$

*Proof:*

- (1):By Theorem 2.5.17
- (2):By Proposition 2.5.13 and Proposition 2.5.7.
- (3):By Theorem 2.5.10.
- (4):Notice that  $M_P \neq 0 \Leftrightarrow \text{Ann}(M_P) \neq R$ . Then Proposition 2.5.20.
- (5):Since localization commute with tensor product, it suffice to show:

**Lemma 2.5.23.**  $M, N$  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 2.2.31, 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 2.5.24** (universal property of localization). Let  $g : A \rightarrow B$  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  $h : S^{-1}A \rightarrow B$  such that  $g = h \circ f$ .

**Theorem 2.5.25.** 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

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

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  $A_{\mathfrak{p}}$ , 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 2.5.13 and universal property of localization.

**Theorem 2.5.26.** Let  $A$  be a ring,  $S \subset A$  a multiplicative set, and  $f : A \rightarrow S^{-1}A$  the canonical map. If  $B$  is a ring, with ring homomorphisms  $g : A \rightarrow B$  and  $h : B \rightarrow S^{-1}A$  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:

$$\begin{aligned} S^{-1}A &\rightarrow g(S)^{-1}B \\ \varphi : a/s &\mapsto g(a)/g(s) \end{aligned}$$

$$\begin{aligned} g(S)^{-1}B &\rightarrow S^{-1}A \\ \psi : b/g(s) &\mapsto h(b) \cdot (1/s) \end{aligned}$$

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

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

$$\begin{aligned} S^{-1}A &\rightarrow T^{-1}B \\ \varphi : a/s &\mapsto g(a)/g(s) \end{aligned}$$

$$\begin{aligned} T^{-1}B &\rightarrow S^{-1}A \\ \psi : b/t &\mapsto h(b)h(t)^{-1} \end{aligned}$$

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 check 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 2.5.27.** 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  $A_{\mathfrak{p}} \simeq B_P$ .

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

**Corollary 2.5.28.** 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:

$$\begin{array}{ccc}
 A & \xrightarrow{a \mapsto a/1} & S^{-1}A \\
 & \searrow a \mapsto a/1 & \downarrow a/s \mapsto a/s \\
 & & T^{-1}A
 \end{array}$$

## 2.6 Integral Extension and Dedekind Domain

**Definition 2.6.1.** 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

$$x^n + a_1x^{n-1} + \cdots + a_n = 0$$

where the  $a_i$  are elements of  $A$ .

**Proposition 2.6.2.** 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.

*Proof:* (4) implies (1): Assume  $M = Am_1 + \cdots + Am_k$ . Let  $[xm_1, \dots, xm_k] = [m_1, \dots, m_k]R$ . Then  $(xI - R)m = 0$ . Since  $A[x]$ -module is faithful, then the statement follows from the following lemma

**Lemma 2.6.3.** Let  $A = (a_{ij})$  be an  $(r \times r)$  matrix with entries in an arbitrary ring, and let  $A^* = (a_{ij}^*)$  be the adjoint matrix, i.e.,  $a_{ij}^* = (-1)^{i+j} \det(A_{ij})$ , where the matrix  $A_{ij}$  is obtained from  $A$  by deleting the  $i$ -th column and the  $j$ -th row. Then one has

$$AA^* = A^*A = \det(A)E,$$

where  $E$  denotes the unit matrix of rank  $r$ . For any vector  $x = (x_1, \dots, x_r)$ , this yields the implication

$$Ax = 0 \implies (\det A)x = 0$$

**Proposition 2.6.4.** Let  $x_i (1 \leq i \leq n)$  be elements of  $B$ , each integral over  $A$ . Then the ring  $A[x_1, \dots, x_n]$  is a finitely-generated  $A$ -module.

**Corollary 2.6.5.** The set  $C$  of elements of  $B$  which are integral over  $A$  is a subring of  $B$  containing  $A$ .

**Corollary 2.6.6.** Let  $A \subseteq B \subseteq C$  be two ring extensions. If  $C$  is integral over  $B$  and  $B$  is integral over  $A$ , then  $C$  is integral over  $A$ .

*Proof:* For all  $x \in C$ , there's  $f(y) = b_ny^n + \cdots + b_1y_1 + b_0 \in B[y]$  such that  $x$  is a root of  $f(y)$ . Since  $x$  integral over  $B$ ,  $x$  integral over  $A[b_n, \dots, b_0]$ . By Proposition 2.6.2,  $A[b_n, \dots, b_0, x]$  is finitely generated  $A[b_n, \dots, b_0]$ -module. By Proposition 2.6.4,  $A[b_n, \dots, b_0]$  is finite  $A$ -module, then  $A[b_n, \dots, b_0, x]$  is finite  $A$ -module. Hence by Proposition 2.6.2 again,  $x$  is integral over  $A$ .



**Definition 2.6.7.** 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  $A$ .

**Definition 2.6.8.** If  $A$  is an integral domain with field of fractions  $K$ , then the integral closure  $\bar{A}$  of  $A$  in  $K$  is called the normalization of  $A$ , and  $A$  is simply called integrally closed if  $A = \bar{A}$ .

**Proposition 2.6.9.** 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.

**Example 2.6.10.** A U.F.D. is an integrally closed domain.

**Definition 2.6.11** (going-up and going down). For a ring  $A$  and an  $A$ -algebra  $B$ , the following statement is called the going-up theorem: given two prime ideals  $\mathfrak{p} \subset \mathfrak{p}'$  of  $A$  and a prime ideal  $P$  of  $B$  lying over  $\mathfrak{p}$ , there exists  $P' \in \text{Spec } B$  such that  $P \subset P'$  and  $P' \cap A = \mathfrak{p}'$ . Similarly, the going-down theorem is the following statement: given  $\mathfrak{p} \subset \mathfrak{p}'$  and  $P' \in \text{Spec } B$  lying over  $\mathfrak{p}'$ , there exists  $P \in \text{Spec } B$  such that  $P \subset P'$  and  $P \cap A = \mathfrak{p}$ .

**Theorem 2.6.12.** If  $B \supset A$  is an extension ring which is integral over  $A$  then the going-up theorem holds.

If in addition  $B$  is an integral domain and  $A$  is integrally closed, the going-down theorem also holds.

**Definition 2.6.13.** A Noetherian, integrally closed integral domain in which every nonzero prime ideal is maximal ( $\dim = 1$ ) is called a Dedekind domain.

**Proposition 2.6.14.** Every non-zero ideal  $\mathfrak{a}$  of a Dedekind domain  $\mathcal{O}$  admits a factorization

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$$

into nonzero prime ideals  $\mathfrak{p}_i$  of  $\mathcal{O}$  which is unique up to the order of the factors.

Moreover,  $I_1 \mid I_2$  iff  $I_1 \supset I_2$ ,  $I_1 + I_2 = \gcd(I_1, I_2)$ .

**Proposition 2.6.15.** In Dedekind Domain, every fractional ideal is invertible.

**Proposition 2.6.16.** The fractional ideals form an abelian group, the ideal group  $J_K$  of  $K$ . The identity element is  $(1) = \mathcal{O}$ , and the inverse of  $\mathfrak{a}$  is

$$\mathfrak{a}^{-1} = \{x \in K \mid x\mathfrak{a} \subseteq \mathcal{O}\}$$

**Proposition 2.6.17.** Every fractional ideal  $\mathfrak{a}$  admits a unique representation as a product

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_p}$$

with  $\nu_p \in \mathbb{Z}$  and  $\nu_p = 0$  for almost all  $p$ . In other words,  $J_K$  is the free abelian group on the set of nonzero prime ideals  $\mathfrak{p}$  of  $\mathcal{O}$ .

**Definition 2.6.18** (ideal class group). The fractional principal ideals  $(a) = a\mathcal{O}$ ,  $a \in K^*$ , form a subgroup of the group of ideals  $J_K$ , which will be denoted  $P_K$ . The quotient group

$$Cl_K = J_K/P_K$$

is called the ideal class group, or class group for short, of  $K$ . Along with the group of units  $\mathcal{O}^*$  of  $\mathcal{O}$ , it fits into the exact sequence

$$1 \longrightarrow \mathcal{O}^* \longrightarrow K^* \longrightarrow J_K \longrightarrow Cl_K \longrightarrow 1,$$

## 2.7 Flatness

**Theorem 2.7.1** (Base Change). If  $f : A \rightarrow B$  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 2.2.22.

**Theorem 2.7.2** (Localization).  $S^{-1}A$  is a flat  $A$ -module.

*Proof:* By Theorem 2.5.14.

**Theorem 2.7.3** (Transitivity).  $f : A \rightarrow B$  is a ring homomorphism,  $B$  is flat  $A$ -module,  $N$  is flat  $B$ -module, then  $N$  is flat over  $A$ .

*Proof:* By Theorem 2.2.22.

**Definition 2.7.4** (faithfully flat).

**Proposition 2.7.5.** Let  $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$  be an exact sequence, with  $C$  flat. Then  $A$  is flat if and only if  $B$  is flat.

*Proof:* By Long exact homology sequence, for any  $R$ -module  $D$ , there's exact sequence

$$0 \rightarrow \operatorname{Tor}_R^1(D, A) \rightarrow \operatorname{Tor}_R^1(D, B) \rightarrow 0$$

## 2.8 Dimension Theory and Hilbert's Nullstellensatz

**Definition 2.8.1.** Let  $X$  be a topological space; we consider strictly decreasing (or strictly increasing) chains  $Z_0, Z_1, \dots, Z_r$  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  $\dim Y \leq \dim X$ .

Let  $A$  be a ring. The supremum of the lengths  $r$ , taken over all strictly decreasing chains  $\mathfrak{p}_0 \supset \mathfrak{p}_1 \supset \dots \supset \mathfrak{p}_r$  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  $\text{Spec } A$ . For a prime ideal  $\mathfrak{p}$  of  $A$ , the supremum of the lengths, taken over all strictly decreasing chains of prime ideals  $\mathfrak{p} = \mathfrak{p}_0 \supset \mathfrak{p}_1 \supset \dots \supset \mathfrak{p}_r$  starting from  $\mathfrak{p}$ , is called the height of  $\mathfrak{p}$ , and denoted  $\text{ht } \mathfrak{p}$ . Moreover, the supremum of the lengths, taken over all strictly increasing chain of prime ideals  $\mathfrak{p} = \mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \dots \subset \mathfrak{p}_r$  starting from  $\mathfrak{p}$ , is called the coheight of  $\mathfrak{p}$ , and written  $\text{coht } \mathfrak{p}$ . It follows from the definitions that

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

**Example 2.8.2.**  $A$  is a Artinian ring, then  $\dim A = 0$ .

*Proof:* Since there's only a finite number of maximal ideals  $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ , and that the product of all of these is nilpotent. If then  $\mathfrak{p}$  is a prime ideal,  $\mathfrak{p} \supset (0) = (\mathfrak{p}_1 \dots \mathfrak{p}_r)^v$ , by Theorem 2.1.19 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 2.8.3.**  $A$  is Artinian if and only if  $A$  is Noetherian and  $\dim A = 0$

**Definition 2.8.4.** 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  $I$  :

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

Here also we have the inequality

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

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

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

**Proposition 2.8.5.** If  $M$  is finitely generated then  $\dim M$  is the combinatorial dimension of the closed subspace  $\text{Supp}(M) = V(\text{ann}(M))$  of  $\text{Spec } A$ .

*Proof:* By Proposition 2.3.8,

$$\dim M = \dim(A/\text{ann}(M)) = \dim V(\text{ann}(M))$$

**Theorem 2.8.6** (Ratliff, 1972). A strictly increasing (or decreasing) chain  $\mathfrak{p}_0, \mathfrak{p}_1, \dots$  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  $\mathfrak{p}$  we have  $\text{ht } \mathfrak{p} + \text{coht } \mathfrak{p} = \dim A$ . Conversely, if  $A$  is a Noetherian local domain and this equality holds for all  $\mathfrak{p}$  then  $A$  is catenary.

**Theorem 2.8.7.** Let  $k$  be a field,  $L$  an algebraic extension of  $k$  and  $\alpha_1, \dots, \alpha_n \in L$ ; then

- (1)  $k[\alpha_1, \dots, \alpha_n] = k(\alpha_1, \dots, \alpha_n)$ .
- (2) Write  $\varphi : k[X_1, \dots, X_n] \longrightarrow k(\alpha_1, \dots, \alpha_n)$  for the homomorphism over  $k$  which maps  $X_i$  to  $\alpha_i$ ; then  $\text{Ker } \varphi$  is the maximal ideal generated by  $n$  elements of the form

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

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

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

**Theorem 2.8.8.** 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  $E = k[x_1, \dots, x_n]$ . If  $E$  is not algebraic over  $k$ , by Proposition 1.3.51, we can renumber the  $x_i$  so that  $x_1, \dots, x_r$  are algebraically independent over  $k$ , where  $r \geq 1$ , and each of  $x_{r+1}, \dots, x_n$  is algebraic over the field  $F = k(x_1, \dots, x_r)$ . Hence  $E$  is a finite algebraic extension of  $F$  and therefore finitely generated as an  $F$ -module. Applying Proposition 2.6.9 to  $k \subseteq F \subseteq E$ , it follows that  $F$  is a finitely generated  $k$ -algebra, say  $F = k[y_1, \dots, y_r]$ . Each  $y_j$  is of the form  $f_j/g_j$ , where  $f_j$  and  $g_j$  are polynomials in  $x_1, \dots, x_r$ . It contradicts to the fact that there are infinitely many irreducible polynomials in the ring  $k[x_1, \dots, x_r]$  (adapt Euclid's proof of the existence of infinitely many prime numbers).

**Theorem 2.8.9.** Let  $k$  be a field, and let  $\mathfrak{m}$  be any maximal ideal of the polynomial ring  $k[X_1, \dots, X_n]$ ; then the residue class field  $k[X_1, \dots, X_n]/\mathfrak{m}$  is algebraic over  $k$ . Hence  $\mathfrak{m}$  can be generated by  $n$  elements, and in particular if  $k$  is algebraically closed then  $\mathfrak{m}$  is of the form  $\mathfrak{m} = (X_1 - \alpha_1, \dots, X_n - \alpha_n)$  for  $\alpha_i \in k$ .

*Proof:* Set  $k[X_1, \dots, X_n]/m = K$ , and write  $\alpha_i$  for the image of  $X_i$  in  $K$ ; then  $K = k[\alpha_1, \dots, \alpha_n]$ . By the previous theorem, since  $K$  is a field it is algebraic over  $k$ , and then by Theorem 2.8.7,  $m$  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  $(X_1 - \alpha_1, \dots, X_n - \alpha_n) \subset m$ . On the other hand  $(X_1 - \alpha_1, \dots, X_n - \alpha_n)$  is obviously a maximal ideal, so that equality must hold.

**Theorem 2.8.10** (Hilbert's Nullstellensatz). If  $k$  is algebraically 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  $A = (f_1, \dots, f_m)$ . If  $g \in k[X_1, \dots, X_n]$  satisfies:

$$\{f_1(a_1, \dots, a_n) = \dots = f_m(a_1, \dots, a_n) = 0\} \implies g(a_1, \dots, a_n) = 0$$

then there is an integer  $\ell$  and polynomials  $h_1, \dots, h_m$  such that

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

To prove this, introduce the ideal

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

in  $k[X_1, \dots, X_{n+1}]$  where  $A \cdot k[X_1, \dots, X_n, X_{n+1}]$  be the ideal generated by  $A$ . There are 2 possibilities: either  $B$  is a proper ideal, or  $B = k[X_1, \dots, X_{n+1}]$ . In the first case, let  $M$  be a maximal ideal in  $k[X_1, \dots, X_{n+1}]$  containing  $B$ . By Theorem 2.8.9,

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

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

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

$B \subset M$  means that:

$$f_1(a_1, \dots, a_n) = \dots = f_m(a_1, \dots, a_n) = 0 \tag{2.1}$$

and

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

But by our assumption on  $g$ , (2.1) implies that  $g(a_1, \dots, a_n) = 0$ . 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  $h_1, \dots, h_m, h_{m+1} \in k[X_1, \dots, X_{n+1}]$  such that:

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

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

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

Clearing denominators, this gives:

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

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

**Theorem 2.8.11.** 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 ?? and Hilbert's Nullstellensatz.

**Theorem 2.8.12.** 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  $\text{Frac}(A)/k$ . For convenience, we denote it by  $\deg_k A$ .

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

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

$$\text{tr} \cdot \deg_k k[X]/Q < \text{tr} \cdot \deg_k k[X]/P.$$

The  $k$ -algebra homomorphism  $k[X]/P \rightarrow k[X]/Q$  is onto, so that  $\text{tr} \cdot \deg_k k[X]/Q \leq \text{tr} \cdot \deg_k k[X]/P$  is obvious. Suppose that equality holds. Let  $k[X]/P = k[\alpha_1, \dots, \alpha_n]$  and  $k[X]/Q = k[\beta_1, \dots, \beta_n]$ .

By Proposition 1.3.51, we may assume that  $\beta_1, \dots, \beta_r$  is a transcendence basis for  $k(\beta_1, \dots, \beta_n)/k$ . Then  $\alpha_1, \dots, \alpha_r$  are also algebraically independent over  $k$ , so that they form a transcendence basis for  $k(\alpha_1, \dots, \alpha_n)$  over  $k$ . Now set  $S = k[X_1, \dots, X_r] - \{0\}$ ;  $S$  is a multiplicative set in  $k[X_1, \dots, X_n]$  with  $P \cap S = \emptyset$  and  $Q \cap S = \emptyset$ . Setting  $R = k[X_1, \dots, X_n]$  and  $K = k(X_1, \dots, X_r)$ , we have  $R_S \simeq K[X_{r+1}, \dots, X_n]$ , and

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

so that  $R_S/PR_S$  is algebraic over  $K = k(X_1, \dots, X_r) \simeq k(\alpha_1, \dots, \alpha_r)$ , 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 2.5.8.

Now let us prove that  $r \leq \dim A$  by induction on  $r$ . If  $r = 0$  then, by Theorem 2.8.8,  $A$  is a field, so  $\dim A = 0$  and the assertion holds. Now let  $r > 0$ , and suppose that  $A = k[\alpha_1, \dots, \alpha_n]$  with  $\alpha_1$  transcendental over  $k$ ; setting  $S = k[X_1] - \{0\}$  and  $R = k[X_1, \dots, X_n]$  we get

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

Hence  $R_S/PR_S$  has transcendence degree  $r-1$  over  $k(X_1)$ , so that by induction  $\dim R_S/PR_S \geq r-1$ . 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  $\text{tr.deg}_k R/P_{r-1} > 0$ . Then  $P_{r-1}$  is not a maximal ideal of  $R$  by Theorem 2.8.8, and therefore  $R$  has a maximal ideal  $P_r$  strictly bigger than  $P_{r-1}$ . Hence  $\dim A = \text{coht } P \geq r$ .



## 2.9 Completion

**Definition 2.9.1.** Let  $A$  be a ring and  $M$  an  $A$ -module; for a directed set  $\Lambda$ , suppose that  $\mathcal{F} = \{M_\lambda\}_{\lambda \in \Lambda}$  is a family of submodules of  $M$  indexed by  $\Lambda$  and such that  $\lambda < \mu \Rightarrow M_\lambda \supset M_\mu$ . Then  $\mathcal{F}$  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  $M_\lambda$  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  $M_\lambda$  is a union of cosets, so is also open. Hence  $M_\lambda$  is an open and closed subset; the quotient module  $M/M_\lambda$  is then discrete in the quotient topology.

**Definition 2.9.2.** Since for  $\lambda < \mu$  there is a natural linear map  $\varphi_\lambda^\mu : M/M_\mu \rightarrow M/M_\lambda$ , 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  $M/M_\lambda$  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  $\psi : M \rightarrow \hat{M}$  be the natural  $A$ -linear map;

**Proposition 2.9.3.**  $\psi$  is continuous, and  $\psi(M)$  is dense in  $\hat{M}$ . If  $\psi$  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 2.9.4.**  $\psi$  is injective if and only if  $M$  is Hausdorff if and only if  $\bigcap_\lambda M_\lambda = 0$ .

**Theorem 2.9.5.** Write  $p_\lambda : \hat{M} \rightarrow M/M_\lambda$  for the projection, and set  $\text{Ker } p_\lambda = M_\lambda^*$ , then the topology of  $\hat{M}$  coincides with the linear topology defined by  $\mathcal{F} = \{M_\lambda^*\}_{\lambda \in \Lambda}$ .

*Proof:* Notice that

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

.

**Lemma 2.9.6** (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 3

## Homological Algebra

### 3.1 Basic Definition in Category

**Definition 3.1.1** (Category). A category  $\mathcal{C}$  consists of three ingredients: a class  $\text{obj}(\mathcal{C})$  of objects, a set of morphisms  $\text{Hom}(A, B)$  for every ordered pair  $(A, B)$  of objects, and composition  $\text{Hom}(A, B) \times \text{Hom}(B, C) \rightarrow \text{Hom}(A, C)$ , denoted by

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

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

- (1) the  $\text{Hom}$  sets are pairwise disjoint; that is, each  $f \in \text{Hom}(A, B)$  has a unique domain  $A$  and a unique target  $B$ ;
- (2) for each object  $A$ , there is an identity morphism  $1_A \in \text{Hom}(A, A)$  such that  $f1_A = f$  and  $1_B f = f$  for all  $f : A \rightarrow B$ ;
- (3) composition is associative: given morphisms  $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$ , then

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

**Definition 3.1.2** (Subcategory). A category  $\mathcal{S}$  is a subcategory of a category  $\mathcal{C}$  if

- (1)  $\text{obj}(\mathcal{S}) \subseteq \text{obj}(\mathcal{C})$
- (2)  $\text{Hom}_{\mathcal{S}}(A, B) \subseteq \text{Hom}_{\mathcal{C}}(A, B)$  for all  $A, B \in \text{obj}(\mathcal{S})$ , where we denote  $\text{Hom}$  sets in  $\mathcal{S}$  by  $\text{Hom}_{\mathcal{S}}(\square, \square)$ ,
- (3) if  $f \in \text{Hom}_{\mathcal{S}}(A, B)$  and  $g \in \text{Hom}_{\mathcal{S}}(B, C)$ , then the composite  $gf \in \text{Hom}_{\mathcal{S}}(A, C)$  is equal to the composite  $gf \in \text{Hom}_{\mathcal{C}}(A, C)$ ,
- (4) if  $A \in \text{obj}(\mathcal{S})$ , then the identity  $1_A \in \text{Hom}_{\mathcal{S}}(A, A)$  is equal to the identity  $1_A \in \text{Hom}_{\mathcal{C}}(A, A)$ . A subcategory  $\mathcal{S}$  of  $\mathcal{C}$  is a full subcategory if, for all  $A, B \in \text{obj}(\mathcal{S})$ , we have  $\text{Hom}_{\mathcal{S}}(A, B) = \text{Hom}_{\mathcal{C}}(A, B)$ .

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 3.1.3.** 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 3.1.4** (covariant functor). If  $\mathcal{C}$  and  $\mathcal{D}$  are categories, then a covariant functor  $T : \mathcal{C} \rightarrow \mathcal{D}$  is a function such that

- (1) if  $A \in \text{obj}(\mathcal{C})$ , then  $T(A) \in \text{obj}(\mathcal{D})$ ,
- (2) if  $f : A \rightarrow A'$  in  $\mathcal{C}$ , then  $T(f) : T(A) \rightarrow T(A')$  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 3.1.5** (contravariant functor). A contravariant functor from  $\mathcal{C}$  to  $\mathcal{D}$  is by definition a covariant functor  $F : \mathcal{C}^{\text{opp}} \rightarrow \mathcal{D}$ , where  $\mathcal{C}^{\text{opp}}$  is the opposite category of  $\mathcal{C}$ . Sometimes we use the notation  $F : \mathcal{C} \rightarrow \mathcal{D}$  for a contravariant functor, in which case we explicitly state that  $F$  is contravariant.

**Definition 3.1.6** (faithful functor). A functor  $F : \mathcal{C} \rightarrow \mathcal{D}$  is faithful (resp. full, resp. fully faithful) if the map  $\text{Hom}_{\mathcal{C}}(X, Y) \rightarrow \text{Hom}_{\mathcal{D}}(FX, FY)$  is an injection (resp. surjection, resp. bijection) for all  $X, Y \in \text{Ob}(\mathcal{C})$ .

**Proposition 3.1.7.** Let  $F : \mathcal{C} \rightarrow \mathcal{D}$  is fully faithful functor.

- (1) Let  $f : X \rightarrow Y$  be a morphism of  $\mathcal{C}$  such that  $Ff$  is an isomorphism. Then  $f$  is an isomorphism.
- (2) Let  $X$  and  $Y$  be objects of  $\mathcal{C}$  such that  $FX \simeq FY$ . Then  $X \simeq Y$ .

**Definition 3.1.8** (isomorphism). A morphism  $f : A \rightarrow B$  in a category  $\mathcal{C}$  is an isomorphism if there exists a morphism  $g : B \rightarrow A$  in  $\mathcal{C}$  with

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

The morphism  $g$  is called the inverse of  $f$ .

**Definition 3.1.9** (natural transformation). Let  $S, T : \mathcal{A} \rightarrow \mathcal{B}$  be covariant functors. A natural transformation  $\tau : S \rightarrow T$  is a one-parameter family of morphisms in  $\mathcal{B}$ ,

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

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

$$\begin{array}{ccc} SA & \xrightarrow{\tau_A} & TA \\ sf \downarrow & & \downarrow Tf \\ SA' & \xrightarrow{\tau_{A'}} & TA' \end{array}$$

A natural isomorphism is a natural transformation  $\tau$  for which each  $\tau_A$  is an isomorphism.

**Proposition 3.1.10.** Given functors  $F, G, H : \mathcal{C} \rightarrow \mathcal{D}$  and natural transformations  $\alpha : F \rightarrow G$  and  $\beta : G \rightarrow H$ , we have the (vertically) composite natural transformation  $\beta\alpha : F \rightarrow H$ . Functors  $\mathcal{C} \rightarrow \mathcal{D}$  and natural transformations form a category  $\text{Fun}(\mathcal{C}, \mathcal{D})$ . Isomorphisms in this category are called natural isomorphisms. A natural transformation  $\alpha$  is a natural isomorphism if and only if  $\alpha_X$  is an isomorphism for every object  $X$  of  $\mathcal{C}$ .

**Definition 3.1.11** (equivalence of categories). An equivalence of categories is a functor  $F : \mathcal{C} \rightarrow \mathcal{D}$  such that there exist a functor  $G : \mathcal{D} \rightarrow \mathcal{C}$  and natural isomorphisms  $\text{id}_{\mathcal{C}} \simeq GF$  and  $FG \simeq \text{id}_{\mathcal{D}}$ . The functors  $F$  and  $G$  are then called quasi-inverses of each other.

**Definition 3.1.12** (essentially surjective). A functor  $F : \mathcal{C} \rightarrow \mathcal{D}$  is essentially surjective if for every object  $Y$  of  $\mathcal{D}$ , there exists an object  $X$  of  $\mathcal{C}$  and an isomorphism  $FX \simeq Y$ .

**Proposition 3.1.13.** A functor  $F : \mathcal{C} \rightarrow \mathcal{D}$  is an equivalence of categories if and only if it is fully faithful and essentially surjective.

**Definition 3.1.14** (groupoid). A category of which where every morphism is an isomorphism is called a groupoid.

**Definition 3.1.15** (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  $A \rightarrow X$ . Any two initial objects in a category  $\mathcal{C}$ , should they exist, are isomorphic.

**Definition 3.1.16** (terminal object). An object  $\Omega$  in a category  $\mathcal{C}$  is called a terminal object if, for every object  $C$  in  $\mathcal{C}$ , there exists a unique morphism  $C \rightarrow \Omega$ . Any two terminal objects in a category  $\mathcal{C}$ , should they exist, are isomorphic.

**Definition 3.1.17** (product, direct product in module). 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  $(C, (p_i : C \rightarrow A_i)_{i \in I})$ , consisting of an object  $C$  and a family  $(p_i : C \rightarrow A_i)_{i \in I}$  of projections, that is a solution to the following universal mapping problem: for every object  $X$  equipped with morphisms  $f_i : X \rightarrow A_i$ , there exists a unique morphism  $\theta : X \rightarrow C$  making the diagram commute for each  $i$ .

$$\begin{array}{ccc} & A_i & \\ \alpha_i \nearrow & & \nwarrow f_i \\ C & \xleftarrow{\theta} & X \end{array}$$

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 3.1.18** (coproduct, direct sum in module). 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  $(C, (\alpha_i : A_i \rightarrow C)_{i \in I})$ , consisting of an object  $C$  and a family  $(\alpha_i : A_i \rightarrow C)_{i \in I}$  of morphisms, called injections, that is a solution to the following universal mapping problem: for every object  $X$  equipped with morphisms  $(f_i : A_i \rightarrow X)_{i \in I}$ , there exists a unique morphism  $\theta : C \rightarrow X$  making the diagram commute for each  $i$ .

$$\begin{array}{ccc} & A_i & \\ \alpha_i \swarrow & & \searrow f_i \\ C & \xrightarrow{\quad \theta \quad} & X \end{array}$$

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 3.1.19** (coproduct in category of topological space).  $(X_i)_{i \in I}$  be a family of topological space,  $f_i : X_i \rightarrow X$  be a family of continuous map.  $\bigsqcup_{i \in I} A_i = \{(a_i, i) \in (\bigcup_{i \in I} A_i) \times I : a_i \in A_i\}$  be the disjoint union of  $(X_i)_{i \in I}$ . 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 3.1.20** (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

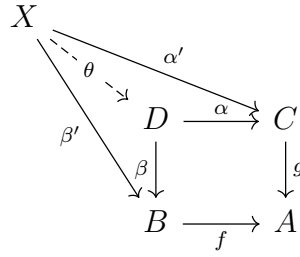
$$A_i \rightarrow \bigotimes_{i \in I} A_i$$

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

**Example 3.1.21.** Coproduct in the category of Group is the free product of groups.

**Definition 3.1.22** (pushback/fibered product). Given two morphisms  $f : B \rightarrow A$  and  $g : C \rightarrow A$  in a category  $\mathcal{C}$ , a **pullback** (or **fibered product**) is a triple  $(D, \alpha, \beta)$  with  $g\alpha = f\beta$  that is a solution to the universal mapping problem: for every  $(X, \alpha', \beta')$  with  $g\alpha' = f\beta'$ , there exists a

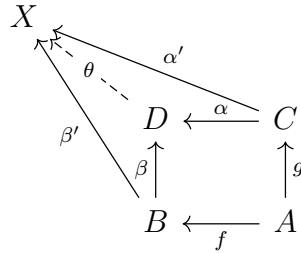
unique morphism  $\theta : X \rightarrow D$  making the diagram commute.



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

**Definition 3.1.24** (pushout/fibered coproduct). Given two morphisms  $f : A \rightarrow B$  and  $g : A \rightarrow C$  in a category  $\mathcal{C}$ , a pushout (or fibered sum) is a triple  $(D, \alpha, \beta)$  with  $\beta g = \alpha f$  that is a solution to the universal mapping problem: for every triple  $(Y, \alpha', \beta')$  with  $\beta' g = \alpha' f$ , there exists a unique morphism  $\theta : D \rightarrow Y$  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 3.1.25.** In category of Commutative Rings,  $f : A \rightarrow B, g : A \rightarrow C$  be ring homomorphism, then the pushout is given by tensor product of  $A$ -algebra  $B$  and  $A$ -algebra  $C$  and homomorphism:

$$\begin{array}{ll} \beta : B \rightarrow B \otimes_A C & \alpha : C \rightarrow B \otimes_A C \\ b \mapsto b \otimes 1 & c \mapsto 1 \otimes c \end{array}$$

**Definition 3.1.26.** A inverse system is a functor from opposite category of the category induced by a given directed partially ordered set to a category  $\mathcal{C}$ . A morphism between inverse system is a natural transformation between inverse system.

Conversely, a inverse system is a functor from the category induced by a given directed partially ordered set to a category  $\mathcal{C}$ . A morphism between inverse system is the natural transformation between direct system.

**Definition 3.1.27** (inverse limit). Let  $(M_i, \varphi_{ij} : M_i \leftarrow M_j), i \leq j$  be an inverse system, The inverse limit (also called projective limit or limit) is an object  $\varprojlim M_i$  and a family of projections  $(\alpha_i : \varprojlim M_i \rightarrow M_i)_{i \in I}$  such that:

- (1)  $\varphi_{ij}\alpha_j = \alpha_i$  whenever  $i \preceq j$ ,
- (2) for every  $X \in \text{obj}(\mathcal{C})$  and all morphisms  $f_i : X \rightarrow M_i$  satisfying  $\varphi_i^j f_j = f_i$  for all  $i \preceq j$ , there exists a unique morphism  $\theta : X \rightarrow \varprojlim M_i$  making the diagram commute.

$$\begin{array}{ccc}
 \varprojlim M_i & \xleftarrow{\quad \theta \quad} & X \\
 \alpha_i \searrow & & \swarrow f_i \\
 & M_i & \\
 \alpha_j \searrow & \uparrow \varphi_{ij} & \swarrow f_j \\
 & M_j &
 \end{array}$$

**Definition 3.1.28** (direct limit). Let  $\{M_i, \varphi_{ij} : M_i \rightarrow M_j\}, i \leq j$  be a direct system. The direct limit (also called inductive limit or colimit) is an object  $\varinjlim M_i$  and insertion morphisms  $(\alpha_i : M_i \rightarrow \varinjlim M_i)_{i \in I}$ .

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

$$\begin{array}{ccc}
 \varinjlim M_i & \xrightarrow{\quad \theta \quad} & X \\
 \alpha_i \searrow & & \swarrow f_i \\
 & M_i & \\
 \alpha_j \searrow & \downarrow \varphi_{ij} & \swarrow f_j \\
 & M_j &
 \end{array}$$

**Remark 3.1.29.** If  $A, B$  are direct systems whose direct limit exist, and  $F : A \rightarrow B$  is a natural transformation. We have a natural morphism between direct limit induced by  $F$ .

**Proposition 3.1.30** (direct limit is exact functor). Let  $\{A_i, \alpha_j^i\}, \{B_i, \beta_j^i\}$ , and  $\{C_i, \gamma_j^i\}$  be direct systems of left  $R$ -modules over  $I$ . If  $r : \{A_i, \alpha_j^i\} \rightarrow \{B_i, \beta_j^i\}$  and  $s : \{B_i, \beta_j^i\} \rightarrow \{C_i, \gamma_j^i\}$  are morphisms of direct systems, and if

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

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

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

**Proposition 3.1.31** (inverse limit is left exact functor). In  ${}_R \text{Mod}$ , let  $r : \{A_i, \alpha_j^i\} \rightarrow \{B_i, \beta_j^i\}$  and  $s : \{B_i, \beta_j^i\} \rightarrow \{C_i, \gamma_j^i\}$  be morphisms of inverse systems. If

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



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

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

**Definition 3.1.32.** Let  $F : \mathcal{C} \rightarrow \mathcal{D}$  and  $G : \mathcal{D} \rightarrow \mathcal{C}$  be covariant functors. The ordered pair  $(F, G)$  is an adjoint pair if, for each  $C \in \text{obj}(\mathcal{C})$  and  $D \in \text{obj}(\mathcal{D})$ , there are bijections

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

such that the following diagram commute:

$$\begin{array}{ccc} \text{Hom}_{\mathcal{D}}(FC, D) & \xrightarrow{(Ff)^*} & \text{Hom}_{\mathcal{D}}(FC', D) \\ \tau_{C,D} \downarrow & & \downarrow \tau_{C',D} \\ \text{Hom}_{\mathcal{C}}(C, GD) & \xrightarrow{f^*} & \text{Hom}_{\mathcal{C}}(C', GD) \\ \\ \text{Hom}_{\mathcal{D}}(FC, D) & \xrightarrow{(g)^*} & \text{Hom}_{\mathcal{D}}(FC, D') \\ \tau_{C,D} \downarrow & & \downarrow \tau_{C,D'} \\ \text{Hom}_{\mathcal{C}}(C, GD) & \xrightarrow{(Gg)_*} & \text{Hom}_{\mathcal{C}}(C, GD') \end{array}$$

**Example 3.1.33** (Hom and Tensor). If  $B = {}_R B_S$  is a bimodule,  $\square \otimes_R B : \text{Mod}_R \rightarrow \text{Mod}_S$  and  $\text{Hom}_S(B, \square) : \text{Mod}_S \rightarrow \text{Mod}_R$  be two functors. then  $(\square \otimes_R B, \text{Hom}_S(B, \square))$  is an adjoint pair. Similarly, if  $B = {}_S B_R$  is a bimodule,  $B \otimes_R \square : {}_R \text{Mod} \rightarrow {}_S \text{Mod}$  and  $\text{Hom}_S(B, \square) : {}_S \text{Mod} \rightarrow {}_R \text{Mod}$  be two functors. then  $(B \otimes_R \square, \text{Hom}_S(B, \square))$  is an adjoint pair.

**Example 3.1.34** (Free and Forget).

**Example 3.1.35** (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, functor  $\mathbb{C}[G] \otimes_{\mathbb{C}[H]} \square : {}_{\mathbb{C}[H]} \text{Mod} \rightarrow {}_{\mathbb{C}[G]} \text{Mod}$  and functor  $\text{Hom}_{\mathbb{C}[G]}(\mathbb{C}[G], \square)$  be an adjoint pair, since  $\text{Hom}_{\mathbb{C}[G]}(\mathbb{C}[G], \square) \simeq \text{Res}_{\mathbb{C}[H]}^{\mathbb{C}[G]}$  (Restriction from  $\mathbb{C}[G]$ -module to  $\mathbb{C}[H]$ -module), we have  $(\mathbb{C}[G] \otimes_{\mathbb{C}[H]} \square, \text{Res}_{\mathbb{C}[H]}^{\mathbb{C}[G]})$  is an adjoint pair.

**Proposition 3.1.36.** Let  $(F, G)$  be an adjoint pair offunctors, where  $F : \mathcal{C} \rightarrow \mathcal{D}$  and  $G : \mathcal{D} \rightarrow \mathcal{C}$ . Then  $F$  preserves direct limits and  $G$  preserves inverse limits.

**Proposition 3.1.37.** If  $F$  preserve inverse limit, then  $F$  preserve kernel. If  $F$  preserve direct limit, then  $G$  preserve cokernel.

*Proof:* Trivial.

**Proposition 3.1.38.**  $F$  is additive functor between abelian categories,  $F$  preserve kernel, then  $F$  is left exact. If  $F$  preserve cokernel, then  $F$  is right exact.

## 3.2 Abelian Category

**Definition 3.2.1** (additive category). A category  $\mathcal{C}$  is additive if

- (1)  $\text{Hom}(A, B)$  is an (additive) abelian group for every  $A, B \in \text{obj}(\mathcal{C})$ ,
- (2) composition map

$$\text{Hom}(A, B) \times \text{Hom}(B, C) \rightarrow \text{Hom}(A, C)$$

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  $\text{obj}(\mathcal{C})$ .

**Definition 3.2.2** (Additive Functor). If  $\mathcal{C}$  and  $\mathcal{D}$  are additive categories, a functor  $T : \mathcal{C} \rightarrow \mathcal{D}$  (of either variance) is additive if, for all  $A, B$  and all  $f, g \in \text{Hom}(A, B)$ , we have

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

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

**Proposition 3.2.3.** Additive Functor preserve zero object.

**Proposition 3.2.4.** If  $\mathcal{C}$  and  $\mathcal{D}$  are additive categories and  $T : \mathcal{C} \rightarrow \mathcal{D}$  is an additive functor of either variance, then  $T(A \oplus B) \cong T(A) \oplus T(B)$  for all  $A, B \in \text{obj}(\mathcal{C})$ .

**Definition 3.2.5.** A morphism  $u : B \rightarrow C$  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  $f, g : A \rightarrow B$ , we have that  $uf = ug$  implies  $f = g$ .

$$A \begin{array}{c} \xrightarrow{f} \\ \xrightarrow{g} \end{array} B \xrightarrow{u} C$$

**Definition 3.2.6.** A morphism  $v : B \rightarrow C$  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  $h, k : C \rightarrow D$ , we have that  $hv = kv$  implies  $h = k$ .

$$B \xrightarrow{v} C \begin{array}{c} \xrightarrow{h} \\ \xrightarrow{k} \end{array} D$$

**Definition 3.2.7** (kernel, cokernel). If  $u : A \rightarrow B$  is a morphism in an additive category  $\mathcal{A}$ , then its kernel  $\ker u$  is a morphism  $i : K \rightarrow A$  that satisfies the following universal mapping property:  $u \circ i = 0$  and, for every  $g : X \rightarrow A$  with  $ug = 0$ , there exists a unique  $\theta : X \rightarrow K$  with  $i\theta = g$ .

$$\begin{array}{ccccc} X & & & & \\ \downarrow \theta & \searrow g & \searrow 0 & & \\ K & \xrightarrow{i} & A & \xrightarrow{u} & B \end{array}$$

$$\begin{array}{ccccc}
 A & \xrightarrow{u} & B & \xrightarrow{\pi} & C \\
 & \searrow & \searrow & & \downarrow \theta \\
 & & & & Y
 \end{array}$$

$0$        $h$

There is a dual definition for cokernel (the morphism  $\pi$  in the diagram).

**Proposition 3.2.8.** Let  $u : A \rightarrow B$  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  $\iota : K \rightarrow A$ , and assume that  $\iota = 0$ . If  $g : X \rightarrow A$  satisfies  $ug = 0$ , then the universal property of kernel provides a morphism  $\theta : X \rightarrow K$  with  $g = \iota\theta = 0$  (because  $\iota = 0$ ). Hence,  $u$  is monic. Conversely, if  $u$  is monic, consider

$$K \xrightarrow[\iota]{0} A \xrightarrow{u} B.$$

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

**Proposition 3.2.9.** Every kernel is monomorphism, every cokernel is epimorphism.

**Definition 3.2.10.** Let  $\mathcal{A}$  be an additive category admitting kernels and cokernels and let  $f : A \rightarrow B$  be a morphism. We define the coimage and image of  $f$  to be  $\operatorname{coim}(f) = \operatorname{coker}(g)$ ,  $\operatorname{im}(f) = \ker(h)$ , where  $g : \operatorname{Ker}(f) \rightarrow A$  and  $h : B \rightarrow \operatorname{coker}(f)$  are the canonical morphisms.

In the above situation, every morphism  $f : A \rightarrow B$  factors uniquely into

$$A \twoheadrightarrow \operatorname{coim}(f) \rightarrow \operatorname{im}(f) \hookrightarrow B.$$

as the following diagram

$$\begin{array}{ccccccc}
 \operatorname{Ker} f & \xrightarrow{g} & A & \xrightarrow{f} & B & \xrightarrow{h} & \operatorname{coker} f \\
 & & \downarrow & & \uparrow & & \\
 & & \operatorname{coker} g & \xrightarrow{\tilde{f}} & \operatorname{Ker} h & & 
 \end{array}$$

**Definition 3.2.11.** 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 (AB1)
- (2) For each morphism  $f : A \rightarrow B$ , the morphism  $\operatorname{coim}(f) \rightarrow \operatorname{im}(f)$  is an isomorphism. (AB2)

**Proposition 3.2.12.** The following properties follow from (AB2):

- (1) If a morphism is both a monomorphism and an epimorphism, then it is an isomorphism.
- (2) Every monomorphism is the kernel of its cokernel.

- (3) Every epimorphism is the cokernel of its kernel.
- (4) Every morphism  $f : A \rightarrow B$  can be decomposed into

$$A \xrightarrow{g} \text{im}(f) \xrightarrow{h} B,$$

where  $g$  is an epimorphism and  $h$  is a monomorphism.

**Example 3.2.13.** Category of abelian topological group is not an abelian category, but it is an additive category. For example, consider the identity map between  $\mathbb{R}$  with discrete topology and euclidean topology.

**Definition 3.2.14.** We say that a sequence  $A \xrightarrow{f} B \xrightarrow{g} C$  in an abelian category is exact at  $B$  if  $gf = 0$  and the morphism  $\text{im}(f) \rightarrow \ker(g)$  is an isomorphism. We say that a sequence  $A^0 \rightarrow A^1 \rightarrow \cdots \rightarrow A^n$  is exact if it is exact at each  $A^i, 1 \leq i \leq n-1$ .

$$\begin{array}{ccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C \\ & \searrow & \nearrow & \nwarrow & \\ & \text{im} f & \xrightarrow{\theta} & \text{Ker} g & \end{array}$$

**Definition 3.2.15.** Let  $\mathcal{C}$  and  $\mathcal{D}$  be abelian categories. An additive functor  $F : \mathcal{C} \rightarrow \mathcal{D}$  is left exact (resp. right exact) if for any exact sequence  $0 \rightarrow X' \rightarrow X \rightarrow X''$  ( resp.  $X' \rightarrow X \rightarrow X'' \rightarrow 0$  ) the sequence  $0 \rightarrow F(X') \rightarrow F(X) \rightarrow F(X'')$  (resp.  $F(X') \rightarrow F(X) \rightarrow F(X'') \rightarrow 0$  ) 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.

**Proposition 3.2.16.** Let  $F : \mathcal{A} \rightarrow \mathcal{B}$  be an additive functor between abelian categories. Then the following conditions are equivalent: (1)  $F$  is left exact. (2) For every short exact sequence  $0 \rightarrow X \rightarrow Y \rightarrow Z \rightarrow 0$  in  $\mathcal{A}$ ,  $0 \rightarrow FX \rightarrow FY \rightarrow FZ$  is an exact sequence in  $\mathcal{B}$ .

**Proposition 3.2.17.** Let  $F : \mathcal{A} \rightarrow \mathcal{B}$  be an additive functor between abelian categories. Then the following conditions are equivalent:

- (1)  $F$  is exact.
- (2) For every short exact sequence  $0 \rightarrow X \rightarrow Y \rightarrow Z \rightarrow 0$  in  $\mathcal{A}$ ,  $0 \rightarrow FX \rightarrow FY \rightarrow FZ \rightarrow 0$  is a short exact sequence in  $\mathcal{B}$ .
- (3)  $F$  is left exact and preserves epimorphisms.
- (4)  $F$  is right exact and preserves monomorphisms.

**Definition 3.2.18.** An object  $P$  in an abelian category  $\mathcal{A}$  is projective if, for every epic  $g : B \rightarrow C$  and every  $f : P \rightarrow C$ , there exists  $h : P \rightarrow B$  with  $f = gh$ .

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

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

**Theorem 3.2.19** (snake lemma). In an abelian category, consider a commutative diagram:

$$\begin{array}{ccccccc}
 \ker a & \longrightarrow & \ker b & \longrightarrow & \ker c & & \\
 \downarrow & & \downarrow & & \downarrow & & \\
 A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\
 \downarrow a & & \downarrow b & & \downarrow c & & \\
 0 \longrightarrow & A' & \xrightarrow{f'} & A' & \xrightarrow{g'} & A' & \\
 \downarrow & & \downarrow & & \downarrow & & \\
 \text{coker } a & \longrightarrow & \text{coker } b & \longrightarrow & \text{coker } c & & 
 \end{array}$$

(Note: Dashed arrows in the original diagram connect  $\ker c$  to  $\text{coker } a$  and  $\text{coker } b$  to  $A'$ .)

where the rows are exact sequences and  $0$  is the zero object. Then there is an exact sequence relating the kernels and cokernels of  $a$ ,  $b$ , and  $c$ .

$$\ker a \longrightarrow \ker b \longrightarrow \ker c \xrightarrow{d} \text{coker } a \longrightarrow \text{coker } b \longrightarrow \text{coker } c$$

where  $d$  is a homomorphism, known as the connecting homomorphism. Furthermore, if the morphism  $f$  is a monomorphism, then so is the morphism  $\ker a \rightarrow \ker b$ , and if  $g'$  is an epimorphism, then so is  $\text{coker } b \rightarrow \text{coker } c$ .

### 3.3 Derived Functor

**Definition 3.3.1** (cochain complex). A (cochain) complex in  $\mathcal{A}$  consists of  $X = (X^n, d_X^n)_{n \in \mathbb{Z}}$ , where  $X^n$  is an object of  $\mathcal{A}$ ,  $d_X^n : X^n \rightarrow X^{n+1}$  is a morphism of  $\mathcal{A}$  (called differential) such that for any  $n$ ,  $d_X^{n+1}d_X^n = 0$ . The index  $n$  in  $X^n$  is called the degree. A (cochain) morphism of complexes  $X \rightarrow Y$  is a collection of morphisms  $(f^n)_{n \in \mathbb{Z}}$  of morphisms  $f^n : X^n \rightarrow Y^n$  in  $\mathcal{A}$  such that  $d_Y^n f^n = f^{n+1} d_X^n$ . We let  $C(\mathcal{A})$  denote the category of complexes in  $\mathcal{A}$ .

**Definition 3.3.2.** Let  $X$  be a complex in  $\mathcal{A}$ . We define

$$\begin{aligned} Z^n X &= \ker(d_X^n : X^n \rightarrow X^{n+1}), \\ B^n X &= \operatorname{im}(d_X^{n-1} : X^{n-1} \rightarrow X^n), \\ H^n X &= \operatorname{coker}(B^n X \hookrightarrow Z^n X), \end{aligned}$$

and call them the cocycle, coboundary, cohomology objects, of degree  $n$ .

$$\begin{array}{ccccc} & \operatorname{im} d^{n-1} & \xhookrightarrow{\quad} & \operatorname{Ker} d^n & \\ & \nearrow & & \nwarrow & \\ X^{n-1} & \xrightarrow{d^{n-1}} & X^n & \xrightarrow{d^n} & X^{n+1} \end{array}$$

**Definition 3.3.3.** Let  $X$  and  $Y$  be cochain complexes in  $\mathcal{A}$  and  $f : X \rightarrow Y$  be a morphism, we can induce a morphism  $H^n(f) : H^n(X) \rightarrow H^n(Y)$  by the following diagram:

$$\begin{array}{ccccccc} & \operatorname{im} d^{n-1} & \xrightarrow{\quad} & \operatorname{Ker} d^n & \xrightarrow{\quad} & H^n(X) & \\ & \nearrow & & \nwarrow & & \downarrow & \\ X^{n-1} & \xrightarrow{d^{n-1}} & X^n & \xrightarrow{d^n} & X^{n+1} & & \\ \downarrow f^{n-1} & & \downarrow f^n & & \downarrow f^{n+1} & & \\ Y^{n-1} & \xrightarrow{e^{n-1}} & Y^n & \xrightarrow{e^n} & Y^{n+1} & & \\ & \searrow & \nearrow & & \nwarrow & & \\ & \operatorname{im} e^{n-1} & \xrightarrow{\quad} & \operatorname{Ker} e^n & \xrightarrow{\quad} & H^n(Y) & \\ & \downarrow & & \downarrow & & \downarrow H^n(f) & \end{array}$$

**Definition 3.3.4.** A complex  $X$  is said to be acyclic if  $H^n X = 0$  for all  $n$ . A morphism of complexes  $X \rightarrow Y$  is called a quasi-isomorphism if  $H^n f : H^n X \rightarrow H^n Y$  is an isomorphism for all  $n$ .

**Theorem 3.3.5** (long exact sequence cohomology). Let  $0 \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow 0$  be a short

exact sequence of complexes. Then we have a long exact sequence

$$\begin{array}{ccccccc}
 H^n(A) & \xrightarrow{H^n(f)} & H^n(B) & \xrightarrow{H^n(g)} & H^n(C) & & \\
 & & & \searrow \delta_n & & & \\
 H^{n+1}(A) & \xleftarrow{H^{n+1}(f)} & H^{n+1}(B) & \xrightarrow{H^{n+1}(g)} & H^{n+1}(C) & & \\
 & & & \searrow \delta_{n+1} & & & \\
 & & H^{n+2}(A) & & & & 
 \end{array}$$

where  $\delta_n$  are called connecting morphisms.

**Theorem 3.3.6.** Given a commutative diagram in category of cochain complex with exact rows

$$\begin{array}{ccccccccc}
 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0
 \end{array}$$

then for every  $n \in \mathbb{Z}$ , there is a commutative diagram

$$\begin{array}{ccccccccccccccc}
 H^n(A) & \xrightarrow{H^n(f)} & H^n(B) & \xrightarrow{H^n(g)} & H^n(C) & \xrightarrow{\delta_n} & H^{n+1}(A) & \xrightarrow{H^{n+1}(f)} & H^{n+1}(B) & \xrightarrow{H^{n+1}(g)} & H^{n+1}(C) \\
 \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
 H^n(A') & \longrightarrow & H^n(B') & \longrightarrow & H^n(C') & \xrightarrow{\delta'_n} & H^{n+1}(A') & \longrightarrow & H^{n+1}(B') & \longrightarrow & H^{n+1}(C')
 \end{array}$$

**Definition 3.3.7.** Let  $X$  be an object of  $\mathcal{A}$ . A left resolution of  $X$  is an exact sequence

$$\dots \rightarrow P^{-n} \rightarrow \dots \rightarrow P^0 \rightarrow X \rightarrow 0$$

in  $\mathcal{A}$ . It is called a projective resolution if each  $P^i$  is projective.

Dually, a right resolution of  $X$  is an exact sequence

$$0 \rightarrow X \rightarrow I^0 \rightarrow \dots \rightarrow I^n \rightarrow \dots$$

in  $\mathcal{A}$ . It is called an injective resolution if each  $I^i$  is injective.

**Proposition 3.3.8.** Consider the following diagram:

$$\begin{array}{ccccc}
 0 & \longrightarrow & X & \xrightarrow{u} & I^0 & \longrightarrow & I^1 \\
 & & & & \searrow & & \nearrow \\
 & & & & \text{coker}(u) & & 
 \end{array}$$

in which  $I^1$  is an injective object such that  $\text{coker}(u) \rightarrow I^1$  is monomorphism. Then it's easy to check  $0 \rightarrow X \rightarrow I^0 \rightarrow I^1$  is an exact sequence.

**Definition 3.3.9.** Let  $\mathcal{A}$  be an additive category. Let  $X$  and  $Y$  be complexes in  $\mathcal{A}$ . We let

$$\text{Ht}(X, Y) = \prod_n \text{Hom}_{\mathcal{A}}(X^n, Y^{n-1})$$

denote the abelian group of families of morphisms  $h = (h^n : X^n \rightarrow Y^{n-1})_{n \in \mathbb{Z}}$ . Given  $h$ , consider  $f^n = d_Y^{n-1}h^n + h^{n+1}d_X^n : X^n \rightarrow Y^n$ . We have

$$d_Y^n f^n = d_Y^n d_Y^{n-1} h^n + d_Y^n h^{n+1} d_X^n = d_Y^n h^{n+1} d_X^n = d_Y^n h^{n+1} d_X^n + h^{n+2} d_X^{n+1} d_X^n = f^{n+1} d_X^n.$$

Thus we get a morphism of complexes  $f : X \rightarrow Y$ . We get a homomorphism of abelian groups

$$\text{Ht}(X, Y) \rightarrow \text{Hom}_{C(\mathcal{A})}(X, Y).$$

We say that a morphism of complexes  $f : X \rightarrow Y$  is nullhomotopic if there exists  $h \in \text{Ht}(X, Y)$  such that  $f^n = d_Y^{n-1}h^n + h^{n+1}d_X^n$ . We say that two morphisms of complexes  $f, g : X \rightarrow Y$  are homotopic if  $f - g$  is null-homotopic.

Let  $f : X \rightarrow Y, g : Y \rightarrow Z$  be morphisms of complexes in  $\mathcal{A}$ . If  $f$  or  $g$  is null-homotopic, then  $gf$  is null-homotopic.

**Proposition 3.3.10.** If  $f, g : X \rightarrow Y$  are homotopic, then  $H^n f = H^n g : H^n X \rightarrow H^n Y$ .

**Proposition 3.3.11.** Suppose we are given injective resolutions of objects  $A, B$  in  $\mathcal{A}$  and a morphism  $f : A \rightarrow B$ ,

$$\begin{aligned} I : 0 &\longrightarrow A \longrightarrow I^0 \longrightarrow I^1 \longrightarrow \dots \\ J : 0 &\longrightarrow B \longrightarrow J^0 \longrightarrow J^1 \longrightarrow \dots \end{aligned}$$

there are  $f_i, i \geq 0$  making the following diagram commute

$$\begin{array}{ccccccc} 0 & \longrightarrow & A & \longrightarrow & I^0 & \longrightarrow & I^1 \longrightarrow \dots \\ & & \downarrow f & & \downarrow f_0 & & \downarrow f_1 \\ 0 & \longrightarrow & B & \longrightarrow & J^0 & \longrightarrow & J^1 \longrightarrow \dots \end{array}$$

and  $f_i$  is unique up to homotopy.

**Definition 3.3.12.** Let  $T : \mathcal{A} \rightarrow \mathcal{B}$  be left exact an additive covariant functor. Suppose we have an injective resolution of  $A$

$$I : 0 \longrightarrow A \longrightarrow I^0 \longrightarrow I^1 \longrightarrow \dots$$

This gives rise to a cochain complex of objects of  $\mathcal{B}$

$$TI : 0 \longrightarrow T(I^0) \longrightarrow T(I^1) \longrightarrow \dots \longrightarrow T(I^n) \longrightarrow \dots$$

We define  $R^n T(A) = H^n(TI)$  for  $n \geq 0$  and call it  $n$ -th right derived functors of  $T$ . (Proposition 3.3.11) gives us that induced morphism of the functor.

**Proposition 3.3.13.**  $R^0 T$  and  $T$  are naturally isomorphic.



**Theorem 3.3.14** (long exact cohomology sequence in right derived functor). Let  $\mathcal{A}$  be an abelian category with enough injectives,  $\mathcal{B}$  an abelian category, and let  $T : \mathcal{A} \rightarrow \mathcal{B}$  be an additive functor. Suppose we have an exact sequence

$$0 \rightarrow A' \xrightarrow{\varphi} A \xrightarrow{\psi} A'' \rightarrow 0$$

Then there exist canonical connecting morphisms  $\omega^n : R^n T(A'') \rightarrow R^{n+1} T(A')$  for  $n \geq 0$  with the property that the following sequence is exact

$$\begin{aligned} 0 \rightarrow R^0 T(A') \rightarrow R^0 T(A) \rightarrow R^0 T(A'') \xrightarrow{\omega^0} R^1 T(A') \rightarrow \dots \\ \dots \rightarrow R^n T(A'') \xrightarrow{\omega^n} R^{n+1} T(A') \rightarrow R^{n+1} T(A) \rightarrow R^{n+1} T(A'') \rightarrow \dots \end{aligned}$$

**Remark 3.3.15.** Left derived functor can be obtained if we replace the injective resolution by projective resolution and all the theorem between left derived functor and right derived functor are similar.

## 3.4 Ext and Tor

**Definition 3.4.1.** Consider the opposite category of left  $R$ -module,  $\text{Hom}(\square, D)$  is a left exact functor. Denote the  $n$ -th right derived functor of  $\text{Hom}(\square, D)$  by  $\text{Ext}_R^n(\square, D)$

**Definition 3.4.2.** Consider category of left  $R$ -module,  $\text{Hom}(D, \square)$  is a left exact functor. Denote the  $n$ -th right derived functor of  $\text{Hom}(D, \square)$  by  $\text{ext}_R^n(D, \square)$

**Proposition 3.4.3.**

$$\text{ext}_R^n(A, B) \simeq \text{Ext}_R^n(A, B)$$

Hence we won't use the notation  $\text{ext}$  anymore.

Long exact cohomology sequence has the following obvious corollary:

**Corollary 3.4.4.** For an  $R$ -module  $Q$  the following are equivalent:

- (1)  $Q$  is injective,
- (2)  $\text{Ext}_R^1(A, Q) = 0$  for all  $R$ -modules  $A$ , and
- (3)  $\text{Ext}_R^n(A, Q) = 0$  for all  $R$ -modules  $A$  and all  $n \geq 1$ .

**Corollary 3.4.5.** For an  $R$ -module  $P$  the following are equivalent:

- (1)  $P$  is projective,
- (2)  $\text{Ext}_R^1(P, B) = 0$  for all  $R$ -modules  $B$ , and
- (3)  $\text{Ext}_R^n(P, B) = 0$  for all  $R$ -modules  $B$  and all  $n \geq 1$ .

**Proposition 3.4.6.** Show that  $\text{Ext}_R^n(A_1 \oplus A_2, B) \cong \text{Ext}_R^n(A_1, B) \oplus \text{Ext}_R^n(A_2, B)$  for all  $n \geq 0$

**Example 3.4.7.** Let  $R = \mathbb{Z}$  and let  $A = \mathbb{Z}/m\mathbb{Z}$  for some  $m \geq 2$ . By the proposition we have  $\text{Ext}_{\mathbb{Z}}^0(\mathbb{Z}/m\mathbb{Z}, D) \cong \text{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, D)$ , and it follows that  $\text{Ext}_{\mathbb{Z}}^0(\mathbb{Z}/m\mathbb{Z}, D) \cong mD$ , where  $mD = \{d \in D \mid md = 0\}$  are the elements of  $D$  that have order dividing  $m$ . For the higher cohomology groups, we use the simple projective resolution

$$0 \longrightarrow \mathbb{Z} \xrightarrow{m} \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \longrightarrow 0$$

for  $A$  given by multiplication by  $m$  on  $\mathbb{Z}$ . Taking homomorphisms into a fixed  $\mathbb{Z}$  module  $D$  gives the cochain complex

$$0 \longrightarrow \text{Hom}_{\mathbb{Z}}(\mathbb{Z}, D) \xrightarrow{m} \text{Hom}_{\mathbb{Z}}(\mathbb{Z}, D) \longrightarrow 0 \longrightarrow \dots$$

We have  $D \cong \text{Hom}_{\mathbb{Z}}(\mathbb{Z}, D)$  and under this isomorphism we have  $\text{Ext}_{\mathbb{Z}}^1(\mathbb{Z}/m\mathbb{Z}, D) \cong D/mD$  for any abelian group  $D$ . It follows immediately from the definition and the cochain complex above that  $\text{Ext}_{\mathbb{Z}}^n(\mathbb{Z}/m\mathbb{Z}, D) = 0$  for all  $n \geq 2$  and any abelian group  $D$ , which we summarize as

$$\begin{aligned} \text{Ext}_{\mathbb{Z}}^0(\mathbb{Z}/m\mathbb{Z}, D) &\cong mD \\ \text{Ext}_{\mathbb{Z}}^1(\mathbb{Z}/m\mathbb{Z}, D) &\cong D/mD \\ \text{Ext}_{\mathbb{Z}}^n(\mathbb{Z}/m\mathbb{Z}, D) &= 0, \quad \text{for all } n \geq 2 \end{aligned}$$

**Example 3.4.8.** Suppose  $A$  is a torsion abelian group. Then we have  $\text{Ext}^0(A, \mathbb{Z}) \cong \text{Hom}(A, \mathbb{Z}) = 0$  since  $\mathbb{Z}$  is torsion free. The sequence  $0 \rightarrow \mathbb{Z} \rightarrow \mathbb{Q} \rightarrow \mathbb{Q}/\mathbb{Z} \rightarrow 0$  gives an injective resolution of  $\mathbb{Z}$ . Applying  $\text{Hom}(A, \dots)$  gives the cochain complex

$$0 \longrightarrow \text{Hom}(A, \mathbb{Z}) \longrightarrow \text{Hom}(A, \mathbb{Q}) \longrightarrow \text{Hom}(A, \mathbb{Q}/\mathbb{Z}) \longrightarrow 0 \longrightarrow \dots$$

and since  $\mathbb{Q}$  is also torsion free, this shows that

$$\text{Ext}_{\mathbb{Z}}^1(A, \mathbb{Z}) \cong \text{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z}).$$

The group  $\text{Hom}(A, \mathbb{Q}/\mathbb{Z})$  is called the Pontriagin dual group to  $A$ . If  $A$  is a finite abelian group the Pontriagin dual of  $A$  is isomorphic to  $A$ . In particular,  $\text{Ext}^1(A, \mathbb{Z}) \cong A$  is nonzero for all nonzero finite abelian groups  $A$ .

**Example 3.4.9.** Suppose  $R = \mathbb{Z}$  and  $A$  and  $B$  are  $\mathbb{Z}$ -modules, i.e., are abelian groups. The group  $B$  can be embedded in an injective  $\mathbb{Z}$ -module  $Q_0$  and the quotient,  $Q_1$ , of  $Q_0$  by the image of  $B$  is again injective. Hence we have an injective resolution

$$0 \longrightarrow B \longrightarrow Q_0 \longrightarrow Q_1 \longrightarrow 0$$

of  $B$ . Applying  $\text{Hom}_{\mathbb{Z}}(A, \square)$  to this sequence gives the cochain complex

$$0 \longrightarrow \text{Hom}_{\mathbb{Z}}(A, Q_0) \longrightarrow \text{Hom}_{\mathbb{Z}}(A, Q_1) \longrightarrow 0 \longrightarrow \dots$$

from which it follows immediately that

$$\text{Ext}_{\mathbb{Z}}^n(A, B) = 0$$

for all abelian groups  $A$  and  $B$  and all  $n \geq 2$ .

**Definition 3.4.10.**  $D$  is a right  $R$ -module, then  $D \otimes_R \square$  is a right exact functor from category of left  $R$ -module to abelian group. We denote the  $n$ -th left derived functor of  $D \otimes_R \square$  by  $\text{Tor}_R^n(D, \square)$

**Definition 3.4.11.** If  $D$  is a left  $R$ -module,  $\square \otimes_R D$  is a right exact functor from category of right  $R$ -module to abelian group, we denote its the  $n$ -th left derived functor by  $\text{tor}_n^R(\square, D)$

**Theorem 3.4.12.**  $\text{tor}_n^R(A, B) = \text{Tor}_n^R(A, B)$

**Proposition 3.4.13.** For a right  $R$ -module  $D$  the following are equivalent:

- (1)  $D$  is a flat  $R$ -module,
- (2)  $\text{Tor}_1^R(D, B) = 0$  for all left  $R$ -modules  $B$ , and
- (3)  $\text{Tor}_n^R(D, B) = 0$  for all left  $R$ -modules  $B$  and all  $n \geq 1$ .

**Example 3.4.14.** Let  $R = \mathbb{Z}$  and let  $B = \mathbb{Z}/m\mathbb{Z}$  for some  $m \geq 2$ .  $\text{Tor}_0^{\mathbb{Z}}(D, \mathbb{Z}/m\mathbb{Z})$  is isomorphic to  $D \otimes \mathbb{Z}/m\mathbb{Z}$ , so we have  $\text{Tor}_0^{\mathbb{Z}}(D, \mathbb{Z}/m\mathbb{Z}) \cong D/mD$ .

For the higher groups we apply  $D \otimes_{\mathbb{Z}} \square$  to the projective resolution

$$0 \longrightarrow \mathbb{Z} \xrightarrow{m} \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \longrightarrow 0$$

of  $B$  and use the isomorphisms  $D \otimes \mathbb{Z} \cong D$  and  $D \otimes \mathbb{Z}/m\mathbb{Z} \cong D/mD$ . This gives

$$\cdots \longrightarrow 0 \longrightarrow D \xrightarrow{m} D \longrightarrow 0.$$

It follows that  $\text{Tor}_1^{\mathbb{Z}}(D, \mathbb{Z}/m\mathbb{Z}) \cong {}_mD$  is the subgroup of  $D$  annihilated by  $m$  and that  $\text{Tor}_n^{\mathbb{Z}}(D, \mathbb{Z}/m\mathbb{Z}) = 0$  for all  $n \geq 2$ , which we summarize as

$$\begin{aligned} \text{Tor}_0(D, \mathbb{Z}/m\mathbb{Z}) &\cong D/mD \\ \text{Tor}_1(D, \mathbb{Z}/m\mathbb{Z}) &\cong {}_mD \\ \text{Tor}_n(D, \mathbb{Z}/m\mathbb{Z}) &= 0, \quad \text{for all } n \geq 2 \end{aligned}$$

## 3.5 Group Cohomology

Assume  $G$  is a finite group.

**Definition 3.5.1.** Consider a left exact functor  $\square^G$  : category of left  $\mathbb{Z}[G]$ -module to abelian group, with  $A^G = \{a \in A : ga = a \quad \forall g \in G\}$  and a right exact functor  $\square_G$  : category of left  $\mathbb{Z}[G]$ -module to abelian group with  $A_G = A/I_G A$  where  $I_G$  is the left ideal of  $\mathbb{Z}[G]$  generated by  $\sigma - 1$ . Then, we have  $\square^G = \text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, \square)$  and  $\square_G = \mathbb{Z} \otimes_{\mathbb{Z}[G]} \square$ .

**Definition 3.5.2.** Let  $A$  be a  $G$ -module and let  $N_G : A \rightarrow A$  be the  $G$ -module endomorphism  $a \mapsto N_G a$ . We then have  $I_G A \subseteq \ker N_G$  and  $\text{im } N_G \subseteq A^G$ , thus  $N_G$  induces a morphism  $\hat{N}_G : A_G \rightarrow A^G$  of trivial  $G$ -modules.

**Definition 3.5.3.** Let  $N_G = \sum_{\sigma \in G} \sigma$ . Define Tate cohomology group:

$$H^n(G, A) = \begin{cases} \text{Ext}_{\mathbb{Z}[G]}^n(\mathbb{Z}, A) & \text{if } n \geq 1 \\ A^G / N_G A & \text{if } n = 0 \\ {}_{N_G} A / I_G A & \text{if } n = -1 \\ \text{Tor}_{-n-1}^{\mathbb{Z}[G]}(\mathbb{Z}, A) & \text{if } n \leq -2 \end{cases}$$

**Theorem 3.5.4** (standard projective resolution of  $\mathbb{Z}$ ). Let  $G$  be a finite group. The standard resolution of  $\mathbb{Z}$  by  $G$ -modules is the exact sequence of (both left and right)  $G$ -module homomorphisms

$$\cdots \longrightarrow \mathbb{Z}[G^{n+1}] \xrightarrow{d_n} \mathbb{Z}[G^n] \longrightarrow \cdots \xrightarrow{d_1} \mathbb{Z}[G] \xrightarrow{d_0} \mathbb{Z} \longrightarrow 0,$$

where the boundary maps  $d_n$  are defined by

$$d_n(g_0, \dots, g_n) := \sum_{i=0}^n (-1)^i (g_0, \dots, \hat{g}_i, \dots, g_n)$$

and extended  $\mathbb{Z}$ -linearly (the notation  $\hat{g}_i$  means omit  $g_i$  from the tuple). The map  $d_0$  sends each  $g \in G$  to 1, and extends to the map  $\sum_g a_g g \mapsto \sum_g a_g$ , which is also known as the augmentation map and may be denoted  $\varepsilon$ .

**Proposition 3.5.5.** Let  $A$  be a  $G$ -module. For every  $n \geq 0$  we have an isomorphism of abelian groups

$$\Phi^n : \text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^{n+1}], A) \xrightarrow{\sim} C^n(G, A)$$

that sends  $\varphi : \mathbb{Z}[G^{n+1}] \rightarrow A$  to the function  $f : G^n \rightarrow A$  defined by

$$f(g_1, \dots, g_n) := \varphi(1, g_1, g_1 g_2, \dots, g_1 g_2 \cdots g_n).$$

And under this isomorphism, we have an exact sequence of abelian group

$$0 \longrightarrow C^0(G, A) \xrightarrow{d^0} C^1(G, A) \xrightarrow{d^1} C^2(G, A) \longrightarrow \cdots$$

where

$$\begin{aligned} d^n(f)(g_0, \dots, g_n) &:= g_0 f(g_1, \dots, g_n) - f(g_0 g_1, g_2, \dots, g_n) + f(g_0, g_1 g_2, \dots, g_n) \\ &\quad \cdots + (-1)^n f(g_0, \dots, g_{n-2}, g_{n-1} g_n) + (-1)^{n+1} f(g_0, \dots, g_{n-1}). \end{aligned}$$

for  $n \geq 1$  and  $d_0(a)(g) := g a$  for  $n = 0$

The group  $C^n(G, A)$  contains subgroups of  $n$ -cocycles and  $n$ -coboundaries defined by

$$Z^n(G, A) := \ker d^n \quad \text{and} \quad B^n(G, A) := \text{im } d^{n-1},$$

and we have  $H^n(G, A) = Z^n(G, A) / B^n(G, A)$  for all  $n \geq 1$

**Corollary 3.5.6** (cohomology group of degree 1). For the group  $H^1(G, A)$ , the 1-cocycles are the functions  $x : G \rightarrow A$  with  $\partial_2 x = 0$ , thus satisfying the property

$$x(\sigma\tau) = \sigma x(\tau) + x(\sigma) \quad \text{for } \sigma, \tau \in G.$$

Because this relation is similar to the one of being a homomorphism, the 1-cocycles are often also called crossed homomorphisms. The 1-coboundaries are obviously the functions

$$x(\sigma) = \sigma a - a, \quad \sigma \in G,$$

with fixed  $a \in A = A_0$  (i.e.,  $x = \partial_1 a$ ). If the group  $G$  acts trivially (i.e., as the identity) on  $A$ , then obviously  $Z^1(G, A) = \text{Hom}(G, A)$  and  $B^1(G, A) = 0$ ; therefore

$$H^1(G, A) = \text{Hom}(G, A)$$

And we define  $\text{Hom}(G, \mathbb{Q}/\mathbb{Z}) = \chi(G)$ .

**Definition 3.5.7.** Let  $G$  be a group and let  $A$  be an abelian group. The abelian group

$$\text{Ind}^G(A) := \mathbb{Z}[G] \otimes_{\mathbb{Z}} A$$

with  $G$ -action defined by  $g(z \otimes a) = (gz) \otimes a$  is the induced  $G$ -module associated to  $A$ .

**Definition 3.5.8.** Let  $G$  be a group and let  $A$  be an abelian group. The abelian group

$$\text{CoInd}^G(A) := \text{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A)$$

with  $G$ -action defined by  $(g\varphi)(z) := \varphi(zg)$  is the coinduced  $G$ -module associated to  $A$ .

**Theorem 3.5.9.** Let  $G$  be a finite group and  $A$  an abelian group. The  $G$ -modules  $\text{Ind}^G(A)$  and  $\text{CoInd}^G(A)$  are isomorphic.

*Proof:* A canonical  $G$ -module isomorphism given by

$$\begin{aligned} \alpha : \text{CoInd}^G(A) &\xrightarrow{\sim} \text{Ind}^G(A) \\ \varphi &\mapsto \sum_{g \in G} g^{-1} \otimes \varphi(g) \\ (g^{-1} \mapsto a) &\longleftrightarrow g \otimes a \end{aligned}$$

**Theorem 3.5.10** (long exact cohomology sequence for Tate cohomology). If

$$0 \longrightarrow A \xrightarrow{i} B \xrightarrow{j} C \longrightarrow 0$$

is an exact sequence of  $G$ -modules and  $G$ -homomorphisms, then there exists a canonical homomorphism

$$\delta_q : H^q(G, C) \longrightarrow H^{q+1}(G, A).$$

The map  $\delta_q$  is called the connecting homomorphism or also the  $\delta$  homomorphism. And the induced infinite sequence

$$\cdots \longrightarrow H^q(G, A) \xrightarrow{\bar{i}_q} H^q(G, B) \xrightarrow{\bar{j}_q} H^q(G, C) \xrightarrow{\delta_q} H^{q+1}(G, A) \longrightarrow \cdots$$

is also exact. It is called the long exact cohomology sequence.

*Proof.* By the following commute diagram and snake lemma:

$$\begin{array}{ccccccc}
 & & N_G A / I_G A & \longrightarrow & N_G B / I_G B & \longrightarrow & N_G C / I_G C \\
 & \nearrow & \downarrow & & \downarrow & & \downarrow \\
 \text{Tor}_1^{\mathbb{Z}[G]}(\mathbb{Z}, C) & \longrightarrow & A_G & \xrightarrow{f} & B_G & \longrightarrow & C_G \longrightarrow 0 \\
 & & \times N_G \downarrow & & \downarrow & & \times N_G \downarrow \\
 0 & \longrightarrow & A^G & \longrightarrow & B^G & \longrightarrow & C^G \longrightarrow \text{Ext}_{\mathbb{Z}[G]}^1(\mathbb{Z}, A) \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & A^G / N_G A & \longrightarrow & B^G / N_G B & \longrightarrow & A^C / N_G C \\
 & & \nwarrow & & \nearrow & & \nearrow
 \end{array}$$

□

**Theorem 3.5.11.** Let  $G$  be a group and  $A$  an abelian group. Then  $(\text{CoInd}^G(A))^G \simeq A$  and  $H^n(G, \text{CoInd}^G(A)) = 0$  for all  $n \geq 1$ .

*Proof:* For all  $n \geq 1$  we have an isomorphisms of abelian groups

$$\begin{aligned}
 \alpha : \text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^n], \text{CoInd}^G(A)) &\xrightarrow{\sim} \text{Hom}_{\mathbb{Z}}(\mathbb{Z}[G^n], A) \\
 \varphi &\mapsto (z \mapsto \varphi(z)(1)) \\
 (z \mapsto (y \mapsto \phi(yz))) &\longleftrightarrow \phi
 \end{aligned}$$

Since  $\mathbb{Z}$  is a projective  $\mathbb{Z}$ -module, we have for all  $n \geq 1$ ,  $H^n(G, \text{CoInd}^G(A)) = \text{Ext}_{\mathbb{Z}}^n(\mathbb{Z}, A) = 0$  and  $(\text{CoInd}^G(A))^G = \text{Ext}_{\mathbb{Z}}^0(\mathbb{Z}, A) = A$

**Theorem 3.5.12.** Let  $G$  be a group and  $A$  an abelian group. Then  $(\text{Ind}^G(A))_G \simeq A$  and  $H^{-n-1}(G, \text{Ind}^G(A)) = 0$  for all  $n \geq 1$ .

*Proof:* Viewing  $\mathbb{Z}[G^n]$  as a right  $\mathbb{Z}[G]$ -module and  $\mathbb{Z}[G]$  as a left  $\mathbb{Z}[G]$ -module, for all  $n \geq 1$ ,

$$\mathbb{Z}[G^n] \otimes_{\mathbb{Z}[G]} (\mathbb{Z}[G] \otimes_{\mathbb{Z}} A) \simeq (\mathbb{Z}[G^n] \otimes_{\mathbb{Z}[G]} \mathbb{Z}[G]) \otimes_{\mathbb{Z}} A \simeq \mathbb{Z}[G^n] \otimes_{\mathbb{Z}} A$$

Hence  $H^{-n-1}(G, A) = \text{Tor}_n^{\mathbb{Z}}(\mathbb{Z}, A) = 0$  for all  $n \geq 1$  and  $(\text{Ind}^G(A))_G \simeq A$ .

**Proposition 3.5.13.** Let  $G$  be a finite group and let  $B$  be an induced or co-induced  $G$ -module associated to some abelian group  $A$ . Then  $H^n(G, A) = 0$  for all  $n \in \mathbb{Z}$ .

*Proof:* It suffices to check for  $B = \mathbb{Z}[G] \otimes_{\mathbb{Z}} A$ , we have  $H^{-1}(G, B) = H^0(G, 0)$ . And by the definition of  $H^{-1}(G, \square)$  and  $H^{-1}(G, \square)$  and Theorem 2.2.30, we can explicitly write down the form of  $N_G B$  and  $I_G B$ .

**Lemma 3.5.14.** For a  $G$ -module  $A$  we define the  $G$ -actions on  $\text{Ind}^G(A) := \mathbb{Z}[G] \otimes_{\mathbb{Z}} A$  by  $g(z \otimes a) := gz \otimes ga$  and on  $\text{CoInd}^G(A) := \text{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A)$  by  $g\varphi := (z \mapsto g\varphi(g^{-1}z))$ . Let  $A$  be a  $G$ -module and let  $A^\circ$  denote the corresponding abelian group. We have  $G$ -module isomorphisms

$$\begin{aligned}
 \Phi : \text{Ind}^G(A) &\xrightarrow{\sim} \text{Ind}^G(A^\circ), & \Phi(g \otimes a) &:= g \otimes g^{-1}a \\
 \Psi : \text{CoInd}^G(A) &\xrightarrow{\sim} \text{CoInd}^G(A^\circ), & \Psi(\varphi) &:= (g \mapsto g\varphi(g^{-1}))
 \end{aligned}$$

**Lemma 3.5.15.** Let  $A$  be a  $G$ -module. The map  $\pi : \text{Ind}^G(A) \rightarrow A$  defined by  $z \otimes a \mapsto \varepsilon(z)a$  is a surjective morphism of  $G$ -modules with kernel  $I_G \otimes A$  (submodule of  $\mathbb{Z}[G] \otimes_{\mathbb{Z}} A$ ).

The map  $\iota : A \rightarrow \text{CoInd}^G(A)$  defined by  $a \mapsto (z \mapsto \varepsilon(z)a)$  for  $g \in G$  is an injective morphism of  $G$ -modules with cokernel isomorphic to  $\text{Hom}_{\mathbb{Z}}(I_G, A)$  (by restricting the map  $\varphi : \mathbb{Z}[G] \rightarrow A$  to  $I_G$ ).

**Theorem 3.5.16** (dimension shifting). Let  $A$  be a  $G$ -module and let  $H$  be any subgroup of  $G$ . Then for all  $n \in \mathbb{Z}$  we have

$$H^{n+1}(H, A) \simeq H^n(H, \text{Hom}_{\mathbb{Z}}(I_G, A)) \quad \text{and} \quad H^{n-1}(H, A) \simeq H^n(H, I_G \otimes_{\mathbb{Z}} A).$$

*Proof:* By long exact Tate cohomology sequence.

**Theorem 3.5.17.** Let  $G$  be a finite group and let  $A$  be a  $G$ -module. The Tate cohomology groups  $H^n(G, A)$  are all torsion groups of exponent dividing  $\#G$ .

*Proof:* It suffices to prove the case  $n = 0$ . For any  $a \in A^G$  we have  $N_G a = (\#G)a$ , thus every element of  $H^0(G, A) = A^G/N_G A$  has order dividing  $\#G$ .

**Corollary 3.5.18.** Let  $G$  be a finite group and let  $A$  be a  $G$ -module. If multiplication by  $\#G$  induces an isomorphism  $A \rightarrow A$  then  $H^n(G, A) = 0$  for all  $n \in \mathbb{Z}$ .

**Theorem 3.5.19.** There is a canonical isomorphism  $H^{-2}(G, \mathbb{Z}) \cong G^{\text{ab}}$ .

*Proof:* Since  $\mathbb{Z}[G]$  is a  $G$ -induced module, it has trivial cohomology, and we obtain from the exact cohomology sequence associated with

$$0 \longrightarrow I_G \longrightarrow \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$$

the isomorphism

$$\delta : H^{-2}(G, \mathbb{Z}) \longrightarrow H^{-1}(G, I_G)$$

Since  $H^{-1}(G, I_G) = I_G/I_G^2$  it suffices to produce an isomorphism  $G/G' \cong I_G/I_G^2$ . (Note that  $G$  is written multiplicatively and  $I_G$  is written additively.) For this we consider the map

$$G \longrightarrow I_G/I_G^2, \quad \sigma \longmapsto (\sigma - 1) + I_G^2.$$

Because  $\sigma \cdot \tau - 1 = (\sigma - 1) + (\tau - 1) + (\sigma - 1) \cdot (\tau - 1)$ , this map is a homomorphism. Since  $I_G/I_G^2$  is abelian, the kernel of this homomorphism contains the commutator subgroup  $G'$ , which implies that we have a homomorphism

$$\log : G/G' \longrightarrow I_G/I_G^2.$$

In order to show that the map  $\log$  is bijective, we use that  $I_G$  is the free abelian group generated by  $\sigma - 1$ , where  $\sigma \in G \setminus \{1\}$ . Hence setting

$$\sigma - 1 \longmapsto \sigma \cdot G'$$

defines an evidently surjective homomorphism from  $I_G$  to  $G/G'$ . Because

$$(\sigma - 1) \cdot (\tau - 1) = (\sigma\tau - 1) - (\sigma - 1) - (\tau - 1) \longmapsto \sigma\tau\sigma^{-1}\tau^{-1}G' = \bar{1},$$

the elements in  $I_G^2$  lie in the kernel, so that we obtain a homomorphism

$$\exp : I_G/I_G^2 \longrightarrow G/G', \quad (\sigma - 1) + I_G^2 \longmapsto \sigma G'$$

with the property that  $\log \circ \exp = \text{id}$  and  $\exp \circ \log = \text{id}$ . Therefore the map  $\log : G/G' \rightarrow I_G/I_G^2$  is an isomorphism.

**Proposition 3.5.20.** Let  $G = \langle g \rangle$  be a finite cyclic group and let  $A$  be a  $G$ -module. For all  $n \in \mathbb{Z}$ , we have  $H^{2n+1}(G, A) = H^1(G, A)$ ,  $H^{2n}(G, A) = H^0(G, A)$ .

**Definition 3.5.21** (Restriction and inflation).



# Chapter 4

## Representation Theory

### 4.1 Definition

**Definition 4.1.1.**  $G$  is a finite group, a representation of  $G$  over a field  $F$  is a group homomorphism  $\rho : G \rightarrow \text{GL}(V)$  where  $V$  is a vector space over  $F$ .

**Proposition 4.1.2.** If  $F$  is a field and  $G$  is a finite group, there's a one-to-one correspondence:

$$\{F[G]\text{-module}\} \longleftrightarrow \{\text{representation of } G \text{ over } F\}.$$

**Definition 4.1.3.** Two representations of  $G$  are equivalent (or similar) if the  $FG$ -modules affording them are isomorphic modules.

**Proposition 4.1.4.** Let  $R$  be a ring and let  $M$  be a nonzero  $R$ -module.

- (1) The module  $M$  is said to be irreducible (or simple) if its only submodules are 0 and  $M$ ; otherwise  $M$  is called reducible.
- (2) The module  $M$  is said to be indecomposable if  $M$  cannot be written as  $M_1 \oplus M_2$  for any nonzero submodules  $M_1$  and  $M_2$ ; otherwise  $M$  is called decomposable.
- (3) The module  $M$  is said to be completely reducible (or semisimple) if it is a direct sum of irreducible submodules.
- (4) A representation is called irreducible, reducible, indecomposable, decomposable or completely reducible according to whether the  $F[G]$ -module affording it has the corresponding property.
- (5) If  $M$  is a completely reducible  $R$ -module, any direct summand of  $M$  is called a constituent of  $M$  (i.e.,  $N$  is a constituent of  $M$  if there is a submodule  $N'$  of  $M$  such that  $M = N \oplus N'$ ).
- (6) Let  $R$  be a ring. A left ideal of  $R$  which is simple as a left  $R$ -module is said to be minimal.

**Remark 4.1.5.** By the definition of irreducible representation, a finite group has no infinite-dimension irreducible representation.

**Definition 4.1.6** (simple ring). A simple ring is a ring has no proper, nonzero 2-sided ideals.

**Theorem 4.1.7** (Maschke's theorem). Let  $G$  be a finite group and let  $F$  be a field whose characteristic does not divide  $|G|$ . If  $V$  is any  $F[G]$ -module and  $U$  is any submodule of  $V$ , then  $V$  has a submodule  $W$  such that  $V = U \oplus W$

*Proof:* The idea of the proof of Maschke's Theorem is to produce an  $F[G]$ -module homomorphism

$$\pi : V \rightarrow U$$

which is a projection onto  $U$ , i.e., which satisfies the following two properties:

- (1)  $\pi(u) = u$  for all  $u \in U$
- (2)  $\pi(\pi(v)) = \pi(v)$  for all  $v \in V$

Then we have  $V = \text{Ker}\pi \oplus U$ .

Let  $W_0$  be subspace of  $V$  such that  $V = U \oplus W_0$ .  $\pi_0$  be the projection onto  $U$ . For each  $g \in G$  define

$$g\pi_0g^{-1} : V \rightarrow U \quad \text{by} \quad g\pi_0g^{-1}(v) = g \cdot \pi_0(g^{-1} \cdot v), \quad \text{for all } v \in V$$

Define

$$\pi = \frac{1}{n} \sum_{g \in G} g\pi_0g^{-1}$$

Then  $\pi$  is a  $F[G]$ -module homomorphism and satisfies above propositions.

**Corollary 4.1.8.**  $\text{char } F \nmid |G|$ , then every representation of finite group  $G$  of finite degree over  $F$  is completely reducible.

**Definition 4.1.9.**  $R$  is a ring.

- (1) A nonzero element  $e$  in a ring  $R$  is called an idempotent if  $e^2 = e$ .
- (2) Idempotents  $e_1$  and  $e_2$  are said to be orthogonal if  $e_1e_2 = e_2e_1 = 0$ .
- (3) An idempotent  $e$  is said to be primitive if it cannot be written as a sum of two (commuting) orthogonal idempotents.
- (4) The idempotent  $e$  is called a primitive central idempotent if  $e \in Z(R)$  and  $e$  cannot be written as a sum of two orthogonal idempotents in the ring  $Z(R)$ .

**Lemma 4.1.10.** Any quotient of a semisimple module is semisimple.

*Proof:* Let  $M$  be a completely reducible module, say  $M = \bigoplus_{i \in I} M_i$  with each  $M_i$  irreducible, and let  $\varphi : M \rightarrow N$  be a surjective homomorphism. Then  $N$  is the sum of the images of the submodules  $M_i \subset M$  :

$$N = \sum_{i \in I} \varphi(M_i)$$

It's clear that  $\varphi(M_i)$  is 0 or  $\varphi(M_i) \cong M_i$ . By Zorn's lemma (take a maximal subset such that it's a direct sum), there's  $J \subset I$  such that

$$N = \bigoplus_{i \in J} \varphi(M_i)$$

Hence  $N$  is semisimple

**Lemma 4.1.11.** Let  $R$  be an arbitrary nonzero ring.

- (1) If  $M$  and  $N$  are simple  $R$ -modules and  $\varphi : M \rightarrow N$  is a nonzero  $R$ -module homomorphism, then  $\varphi$  is an isomorphism.
- (2) (Schur's Lemma) If  $M$  is a simple  $R$ -module, then  $\text{Hom}_R(M, M)$  is a division ring.

*Proof:* Notice that

- (a)  $E_{ij}A$  is the matrix whose  $i^{\text{th}}$  row equals the  $j^{\text{th}}$  row of  $A$  and all other rows are zero.
- (b)  $AE_{ij}$  is the matrix whose  $j^{\text{th}}$  column equals the  $i^{\text{th}}$  column of  $A$  and all other columns are zero.
- (c)  $E_{pq}AE_{rs}$  is the matrix whose  $p, s$  entry is  $a_{qr}$  and all other entries are zero.

Hence (1): By (c).

(2): By  $AE_{ij} = E_{ij}A$ .

(3): trivial.

(4):  $L_i$  is simple by (a). Direct sum is obvious. Let  $M$  be any simple  $R$ -module. Since  $Im = m$  for all  $m \in M$  and since  $I = \sum_{i=1}^n e_i$ , there exists some  $i$  and some  $m \in M$  such that  $e_i m \neq 0$ . For this  $i$  and  $m$  the map  $re_i \mapsto re_i m$  is a nonzero  $R$ -module homomorphism from the simple  $R$ -module  $Re_i$  to the simple module  $M$ . By Schur's Lemma, it is an isomorphism. Also, the map  $r \mapsto rE_{i1}$  gives  $Re_i \cong Re_1$ .

**Lemma 4.1.12.** Let  $\Delta$  be a division ring, let  $n \in \mathbb{Z}^+$ , let  $R$  be the ring of all  $n \times n$  matrices with entries from  $\Delta$  and let  $I$  be the identity matrix (= the 1 of  $R$ ).

- (1) The only two-sided ideals of  $R$  are 0 and  $R$ .
- (2) The center of  $R$  consists of the scalar matrices  $\alpha I$ , where  $\alpha$  is in the center of  $\Delta$ :  $Z(R) = \{\alpha I \mid \alpha \in Z(\Delta)\}$ , and this is a field isomorphic to  $Z(\Delta)$ . In particular, if  $\Delta$  is a field, the center of  $R$  is the subring of all scalar matrices. The only central idempotent in  $R$  is  $I$  (in particular,  $I$  is primitive).
- (3) Let  $e_i$  be the matrix with a 1 in position  $i, i$  and zeros elsewhere. Then  $e_1, \dots, e_n$  are orthogonal primitive idempotents and  $\sum_{i=1}^n e_i = I$ .
- (4)  $L_i = Re_i$  is the left ideal consisting of arbitrary entries in column  $i$  and zeros in all other columns.  $L_i$  is a simple left  $R$ -module. Every simple left  $R$ -module is isomorphic to  $L_1$  (in particular, all  $L_i$  are isomorphic  $R$ -modules) and as a left  $R$ -module we have  $R = L_1 \oplus \dots \oplus L_n$ .

**Lemma 4.1.13.** Let  $R = R_1 \times R_2 \times \cdots \times R_r$ , where  $R_i$  is the ring of  $n_i \times n_i$  matrices over the division ring  $\Delta_i$ , for  $i = 1, 2, \dots, r$ .

- (1) Let  $z_i$  be the  $r$ -tuple with the identity of  $R_i$  in position  $i$  and zero in all other positions. Then  $R_i = z_i R$  and for any  $a \in R_i$ ,  $z_i a = a$  and  $z_j a = 0$  for all  $j \neq i$ . The elements  $z_1, \dots, z_r$  are all of the primitive central idempotents of  $R$ . They are pairwise orthogonal and  $\sum_{i=1}^r z_i = 1$ .
- (2) Let  $N$  be any left  $R$ -module and let  $z_i N = \{z_i x \mid x \in N\}$ ,  $1 \leq i \leq r$ . Then  $z_i N$  is a left  $R$ -submodule of  $N$ , each  $z_i N$  is an  $R_i$ -module on which  $R_j$  acts trivially for all  $j \neq i$ , and

$$N = z_1 N \oplus z_2 N \oplus \cdots \oplus z_r N.$$

- (3) Let  $M_i$  be the unique simple  $R_i$ -module in Lemma 4.1.12. We may consider  $M_i$  as an  $R$ -module by letting  $R_j$  act trivially for all  $j \neq i$ . Then  $M_1, \dots, M_r$  are pairwise nonisomorphic simple  $R$ -modules and any simple  $R$ -module is isomorphic to one of  $M_1, \dots, M_r$ . Explicitly, the  $R$ -module  $M_i$  is isomorphic to the simple left ideal  $(0, \dots, 0, L^{(i)}, 0, \dots, 0)$  of all elements of  $R$  whose  $i^{\text{th}}$  component,  $L^{(i)}$ , consists of matrices with arbitrary entries in the first column and zeros elsewhere.

*Proof:* (3): we show  $M_1, \dots, M_r$  are pairwise non-isomorphic: Suppose  $i \neq j$  and suppose  $\varphi : M_i \rightarrow M_j$  is an  $R$ -module isomorphism. If  $s_i \in M_i$  then  $s_i = z_i s_i$  so

$$\varphi(s_i) = \varphi(z_i s_i) = z_i \varphi(s_i) = 0,$$

since  $\varphi(s_i) \in M_j$  and  $z_i$  acts trivially on  $M_j$ . This contradicts the fact that  $\varphi$  is an isomorphism and proves that  $M_1, \dots, M_r$  are pairwise nonisomorphic simple  $R$ -modules.

**Definition 4.1.14** (semisimple ring). Let  $R$  be a nonzero ring with  $I$  (not necessarily commutative). Then the following are equivalent:

- (1) every  $R$ -module is projective
- (2) every  $R$ -module is injective
- (3) every  $R$ -module is completely reducible
- (4) the ring  $R$  considered as a left  $R$ -module is a direct sum:

$$R = L_1 \oplus L_2 \oplus \cdots \oplus L_n,$$

where each  $L_i$  is a simple module (i.e., a simple left ideal) with  $L_i = R e_i$ , for some  $e_i \in R$  with (i)  $e_i e_j = 0$  if  $i \neq j$  (ii)  $e_i^2 = e_i$  for all  $i$  (iii)  $\sum_{i=1}^n e_i = 1$

- (5) as rings,  $R$  is isomorphic to a direct product of matrix rings over division rings, i.e.,  $R = R_1 \times R_2 \times \cdots \times R_r$  where  $R_j$  is isomorphic to the ring of all  $n_j \times n_j$  matrices with entries in a division ring  $\Delta_j$ ,  $j = 1, 2, \dots, r$ . The integer  $r$ , the integers  $n_j$ , and the division rings  $\Delta_j$  (up to isomorphism) are uniquely determined by  $R$ .

*Proof:* (1)  $\Leftrightarrow$  (2): By Definition 2.2.41 and Definition 2.2.37.

(3)  $\Rightarrow$  (2): Let  $N$  be a  $R$ -module,  $Q$  is a submodule of  $N$ . Consider all the submodules of  $N$  such that its intersection with  $Q$  is 0. Take a maximal element  $M$  of the set. If  $M + Q \neq N$ . Consider

$$N = \bigoplus_{i \in I} M_i$$

where  $M_i$  is irreducible submodule of  $N$ . Then if  $M + Q \not\supseteq M_i$ , since  $M_i$  is irreducible,  $(M + Q) \cap M_i = \emptyset$ . A contradiction!

(4)  $\Rightarrow$  (3): Since  $R$  itself is a semisimple  $R$ -module, the direct sum of  $R$  is also semisimple. Hence by Lemma 4.1.10, we have every  $R$ -module is semisimple.

(5)  $\Rightarrow$  (4): By Lemma 4.1.12.

(2)  $\Rightarrow$  (5):

Step 1:  $A$  is a ring, then the ring homomorphism  $\varphi : A^{\text{opp}} \rightarrow \text{Hom}_A(A, A)$  given by  $a \mapsto (x \mapsto xa)$  is an isomorphism.

Step 2: Let  $A$  be any ring with 1, let  $L$  be any left  $A$ -module and let  $L^n$  be the direct sum of  $n$  copies of  $L$  with itself. Then the ring homomorphism  $\varphi : \text{Hom}_A(L^n, L^n) \rightarrow M_n(D)$ , where  $D = \text{Hom}_A(L, L)$  given by

$$\varphi \in \text{Hom}_A(L^n, L^n) \mapsto (\varphi_{ij})$$

where  $\varphi_{ij}(a) = j^{\text{th}}$  component of  $\varphi(0, \dots, a, \dots, 0)$ .

Step 3: Use Schur's lemma to show that if  $L$  is a simple  $A$ -module, then  $\text{Hom}_A(L^n, L^n)$  is isomorphic to a matrix ring over a division ring.

Step 4: Let  $S$  be a simple ring (i.e., has no proper, nonzero 2-sided ideals) with 1 satisfying D.C.C. on left ideals, then there's a minimal left ideal in  $S$ . Let  $L$  be a minimal left ideal in  $S$ . Show that  $S \cong L^n$  as left  $S$ -modules, where  $L^n = L \oplus \dots \oplus L$  with  $n$  factors.

By simplicity of  $S$ ,  $LS = S$ , so  $1 = l_1 s_1 + \dots + l_n s_n$  for some  $l_i \in L$  and  $s_i \in S$  with  $n$  minimal. Then the map  $(x_1, \dots, x_n) \mapsto x_1 s_1 + \dots + x_n s_n$  is a surjective homomorphism of left  $S$ -modules. If  $y_1 s_1 + \dots + y_n s_n = 0$  and  $y_1 \neq 0$  in which  $y_i \in L$ . Since  $L$  is a minimal left ideal,  $Sy_1 = L$ . Take  $sy_1 = l_1$ . Then  $1 = l_1 s_1 + \dots + l_n s_n - s(y_1 s_1 + \dots + y_n s_n)$ , a contradiction!

Step 5: Let  $\Delta$  be a division ring, and  $n \in \mathbb{N}$ . Then  $M_n(\Delta^{\text{op}}) \cong M_n(\Delta)^{\text{op}}$ . The isomorphic map is given by  $A \mapsto A^T$ .

Step 6: Show that (2) implies  $R$  has the strict descending chain condition (D.C.C.) on left ideals

If  $I_1 \supset \dots \supset I_n \supset \dots$  be a descending chain of left ideals. Then  $R = I_1 \oplus J_1 = J_1 \oplus J_2 \oplus I_2 = \dots$ . Let

$$J = \bigoplus_{i=1}^{\infty} I_i$$

, then  $R = J \oplus K$ . Consider  $1 = j_1 + \dots + j_s + k$ . Then

$$R = \bigoplus_{i=1}^s I_i \oplus K$$

A contradiction!

Step 7: Show that  $R \cong R_1 \times R_2 \times \cdots \times R_r$  where  $R_j$  a simple ring with identity satisfying D.C.C.

By Zorn's Lemma and Step 6, for all 2-sided ideal  $J$ , there's a minimal 2-sided ideal contained in  $J$ . Take  $R_1$  be a minimal 2-sided ideal of  $R$ . There's a left ideal  $R_2$  such that  $R = R_1 \oplus R_2$ . We can check that  $R_2$  is also a 2-sided ideal of  $R$ . Hence we can write  $R$  as a direct sum of finite many 2-sided minial ideal. If  $R = R_1 \oplus \dots R_r$ , then we have

$$R \cong R_1 \times \cdots \times R_r$$

where  $R_j$  are simple ring with 1 satisfying D.C.C.

Step 8: (local uniqueness) Suppose  $S = M_n(\Delta) \cong M_{n'}(\Delta')$  as rings, where  $\Delta$  and  $\Delta'$  are division rings. Then  $\Delta \cong \Delta'$  and  $n = n'$ .

By Step 6, (6)  $\Rightarrow$  (2) and Lemma 4.1.12,  $S$  is a simple ring satisfying D.C.C. Then let  $J$  be a minimal left ideal, we have  $S = M_n(\Delta) \cong M_m(\text{Hom}_S(L, L)^{\text{opp}})$  for some  $m$ . Then  $\Delta \cong \text{Hom}_S(L, L)^{\text{opp}}$ . By Lemma 4.1.12,  $\Delta \cong \Delta'$ .  $n = n'$  follows from the fact dimensions of  $S$  over  $\Delta$  and  $\Delta'$  are equal.

Step 9: (global uniqueness)  $W_1 \times \dots W_{r'} \cong R_1 \times R_2 \times \cdots \times R_r$  where  $R_i$  and  $W_j$  are simple rings. Then  $r = r'$  and  $R_i \cong W_i$  for some order.

Hint: Show that  $(1, 0, \dots, 0) \mapsto (1, 0, \dots, 0)$ . (reset the order if it's necessary).

**Lemma 4.1.15.** If  $\Delta$  is a division ring that is a finite dimensional vector space over an algebraically closed field  $F$  and  $F \cdot 1 \subseteq Z(\Delta)$ , then  $\Delta = F \cdot 1$ .

*Proof:* For all  $a \in \Delta$ , consider  $F \cdot 1 \subset F[a] \subset \Delta$ . Then  $F[a]$  is an integral domain. Since  $[\Delta : F] < \infty$ ,  $F[a] \cong F[x]/(m(x))$  is a field. Since every algebraically closed field have no nontrivial algebraic extension,  $F[a] = F$ .

**Theorem 4.1.16.** Let  $G$  be a finite group. There's  $\mathbb{C}$ -algebra isomorphism:

$$\mathbb{C}[G] \cong M_{n_1}(\mathbb{C}) \times M_{n_2}(\mathbb{C}) \times \cdots \times M_{n_r}(\mathbb{C})$$

where  $n_1, \dots, n_r$  and  $r$  are uniquely determined. In particular,  $G$  is isomorphic to a finite subgroup of  $\text{GL}_{n_1}(\mathbb{C}) \times \dots \text{GL}_{n_k}(\mathbb{C})$

*Proof:* By Maschke's Theorem, every  $\mathbb{C}[G]$ -module is injective, by equivalent definition of semisimple ring, as rings,  $R = \mathbb{C}[G]$  is isomorphic to a direct product of matrix rings over division rings, i.e.,  $R = R_1 \times R_2 \times \cdots \times R_r$  where  $R_j$  is isomorphic to the ring of all  $n_j \times n_j$  matrices with entries in a division ring  $\Delta_j$ ,  $j = 1, 2, \dots, r$ . The integer  $r$ , the integers  $n_j$ , and the division rings  $\Delta_j$  (up to isomorphism) are uniquely determined by  $R$ .

Let  $\varphi$  be the isomorphic map, then  $\varphi$  induce a ring homomorphism  $\varphi_i : \mathbb{C} \rightarrow \Delta_i$  such that  $\varphi_i(\mathbb{C}) \subset Z(\Delta_i)$ . Then by Lemma 4.1.15, as  $\mathbb{C}$ -algebra,

$$\mathbb{C}[G] \cong M_{n_1}(\mathbb{C}) \times M_{n_2}(\mathbb{C}) \times \cdots \times M_{n_r}(\mathbb{C})$$

where  $n_1, \dots, n_r$  and  $r$  are uniquely determined.

**Theorem 4.1.17.**  $\mathbb{C}[G]$  has exactly  $r$  distinct isomorphism types of irreducible modules and these have complex dimensions  $n_1, n_2, \dots, n_r$  given by Lemma 4.1.13.

**Proposition 4.1.18.**  $\sum_{i=1}^r n_i^2 = |G|$

**Proposition 4.1.19.**  $r$  equals the number of conjugacy classes in  $G$  and the dimension of  $Z(\mathbb{C}G)$ .

*Proof:* Let  $\mathcal{K}_1, \dots, \mathcal{K}_s$  be the distinct conjugacy classes of  $G$  (recall that these partition  $G$ ). For each conjugacy class  $\mathcal{K}_i$  of  $G$  let

$$X_i = \sum_{g \in \mathcal{K}_i} g \in \mathbb{C}G.$$

It's clear that  $X_i \in Z(\mathbb{C}G)$ .

We show the  $X_i$ 's form a basis of  $Z(\mathbb{C}G)$ , which will prove  $s = \dim_{\mathbb{C}} Z(\mathbb{C}G) = r$ . Since the  $X_i$ 's are linearly independent it remains to show they span  $Z(\mathbb{C}G)$ . Let  $X = \sum_{g \in G} \alpha_g g$  be an arbitrary element of  $Z(\mathbb{C}G)$ . Since  $h^{-1}Xh = X$ ,

$$\sum_{g \in G} \alpha_g h^{-1}gh = \sum_{g \in G} \alpha_g g.$$

Since the elements of  $G$  form a basis of  $\mathbb{C}G$  the coefficients of  $g$  in the above two sums are equal:

$$\alpha_{hgh^{-1}} = \alpha_g.$$

Since  $h$  was arbitrary, every element in the same conjugacy class of a fixed group element  $g$  has the same coefficient in  $X$ , hence  $X$  can be written as a linear combination of the  $X_i$ 's.

## 4.2 Character

All representations considered are assumed to be finite dimensional.

**Definition 4.2.1.** A class function is any function from  $G$  into  $F$  which is constant on the conjugacy classes of  $G$ , i.e.,  $f : G \rightarrow F$  such that  $f(g^{-1}xg) = f(x)$  for all  $g, x \in G$ .

**Definition 4.2.2.** If  $\varphi$  is a representation of  $G$  afforded by the  $FG$ -module  $V$ , the character of  $\varphi$  is the function

$$\chi : G \rightarrow F \quad \text{defined by} \quad \chi(g) = \text{tr } \varphi(g),$$

**Proposition 4.2.3.** (1) Equivalent representations have the same character.

(2) the character of a representation is a class function.

(3)  $\chi$  is the character of  $\varphi : G \rightarrow \text{GL}(V)$ . Then  $\chi(1)$  is the degree of  $\varphi$ .

**Proposition 4.2.4.**  $V_1$  and  $V_2$  are  $F[G]$ -module,  $\chi$  and  $\psi$  are their character respectively. Then character of  $V_1 \oplus V_2$  is  $\chi + \psi$ .

**Example 4.2.5.** Consider  $\mathbb{C}[G]$  itself as a  $\mathbb{C}[G]$ -module, we call this representation the regular representation of  $G$ . By Lemma 4.1.12 and Lemma 4.1.13,

$$\chi_\rho(g) = \sum_{i=1}^r \chi_i(1)\chi_i(g) = \begin{cases} |G| & g = e \\ 0 & g \neq e \end{cases}$$

**Lemma 4.2.6.**  $V_1$  and  $V_2$  are finite-dimensional  $k$ -vector space,  $A : V_1 \rightarrow V_1$  and  $B : V_2 \rightarrow V_2$  are linear transforms. Then for the linear transform  $A \otimes B : V_1 \otimes V_2 \rightarrow V_1 \otimes_k V_2$ , we have  $\det(A \otimes B) = \det(A)^{\dim V_2} \det(B)^{\dim V_1}$  and  $\text{tr}(A \otimes B) = \text{tr}(A)\text{tr}(B)$ .

**Proposition 4.2.7.**  $\rho_1 : G \rightarrow \text{GL}(V_1)$  and  $\rho_2 : G \rightarrow \text{GL}(V_2)$  are representations of  $G$ . Then the representation  $\rho_1 \otimes \rho_2 : G \rightarrow \text{GL}(V_1 \otimes_k V_2)$  defined by

$$g \mapsto \rho_1(g) \otimes \rho_2(g)$$

is called tensor product of  $\rho_1$  and  $\rho_2$ . And by lemma 4.2.6 we have  $\chi_{\rho_1 \otimes \rho_2} = \chi_{\rho_1} \chi_{\rho_2}$

**Proposition 4.2.8.** (1) Two representations are equivalent if and only if they have the same character. (linearly independent of characters)

(2) characters of irreducible representation form a basis of class function.

*Proof:* Let  $M_1, \dots, M_r$  be the distinct irreducible  $\mathbb{C}[G]$ -module defined by Lemma 4.1.12 and Lemma 4.1.13, Let  $z_1, z_2, \dots, z_r$  be the primitive central idempotents of  $\mathbb{C}[G]$ . Let  $\chi_i$  be the character of  $M_i$ . Notice that if  $j \neq i$  then  $z_j M_i = 0$ , i.e.,  $z_j$  acts as the zero matrix on  $M_j$ , hence  $\chi_j(z_i) = 0$ , and  $z_i$  acts as the identity on  $M_i$ , hence  $\chi_i(z_i) = n_i$ . Hence  $\chi_1, \dots, \chi_r$  are linearly independent as class functions on  $G$ . By Proposition 4.1.19,  $\chi_1, \dots, \chi_r$  form a basis of class functions on  $G$ .

**Corollary 4.2.9.** Let  $G$  be a finite group. There's  $\mathbb{C}$ -algebra isomorphism:

$$\varphi : \mathbb{C}[G] \cong M_{n_1}(\mathbb{C}) \times M_{n_2}(\mathbb{C}) \times \dots \times M_{n_r}(\mathbb{C})$$

Then representation  $\rho_1, \dots, \rho_r$  given by  $\varphi(g) = (\rho_1(g), \dots, \rho_r(g))$  is isomorphic to the irreducible representation defined by Lemma 4.1.12 and Lemma 4.1.13.

*Proof:* Check the character.

**Definition 4.2.10.** For class functions  $\theta$  and  $\psi$  define

$$(\theta, \psi) = \frac{1}{|G|} \sum_{g \in G} \theta(g) \overline{\psi(g)}$$

(where the bar denotes complex conjugation). One easily checks that  $(,)$  is Hermitian: for  $\alpha, \beta \in \mathbb{C}$

$$(1) (\alpha\theta_1 + \beta\theta_2, \psi) = \alpha(\theta_1, \psi) + \beta(\theta_2, \psi),$$



$$(2) \quad (\theta, \alpha\psi_1 + \beta\psi_2) = \bar{\alpha}(\theta, \psi_1) + \bar{\beta}(\theta, \psi_2), \text{ and}$$

$$(3) \quad (\theta, \psi) = (\psi, \theta).$$

**Proposition 4.2.11.** Consider all the distinct irreducible representation  $\rho_1, \dots, \rho_r$  with characters  $\chi_1, \dots, \chi_r$ . There's a  $\mathbb{C}$ -algebra homomorphism

$$\varphi : \mathbb{C}[G] \rightarrow M_{n_1}(\mathbb{C}) \times M_{n_2}(\mathbb{C}) \times \dots \times M_{n_r}(\mathbb{C})$$

induced by  $\varphi(g) = (\rho_1(g), \dots, \rho_r(g))$ . This homomorphism is an isomorphism.

*Proof:* Let  $\tau = \sum_{g \in G} \alpha_g g$ ,  $\varphi(\tau) = 0$ . If  $\alpha_{g_0} \neq 0$ , then

$$\chi_i(g_0^{-1}\tau) = \sum_{g \in G} \alpha_g \chi_i(g_0^{-1}g) = 0$$

Hence

$$\sum_{i=1}^r \chi_i(1) \sum_{g \in G} \alpha_g \chi_i(g_0^{-1}g) = 0$$

So we have  $\alpha_{g_0} = 0$ , a contradiction!

**Corollary 4.2.12.** Let  $z_1, \dots, z_r$  be the orthogonal primitive central idempotents in  $\mathbb{C}[G]$  such that  $\varphi(z_i) = (O, \dots, I_{n_i}, \dots, O)$ . Then

$$z_i = \frac{\chi_i(1)}{|G|} \sum_{g \in G} \chi_i(g^{-1}) g$$

*Proof:* Let

$$z_i = \sum_{g \in G} \alpha_g g$$

If  $\rho$  is the character of regular representation of  $G$ , then

$$\sum_{j=1}^r \chi_j(1) \chi_j(z_i g^{-1}) = \rho(z_i g^{-1}) = \alpha_g |G|.$$

It's easy to check that  $\chi_j(z_i g^{-1}) = \chi_i(g^{-1}) \delta_{ij}$ , then

$$z_i = \sum_{g \in G} \frac{1}{|G|} \sum_{j=1}^r \chi_j(1) \chi_j(g^{-1}) \delta_{ij} g = \frac{\chi_i(1)}{|G|} \sum_{g \in G} \chi_i(g^{-1}) g$$

**Lemma 4.2.13.** If  $\psi$  is any character of  $G$  then  $\psi(x)$  is a sum of roots of 1 in  $\mathbb{C}$  and  $\psi(x^{-1}) = \overline{\psi(x)}$  for all  $x \in G$ .

*Proof:* Let  $n = |G|$ . Notice that  $\psi(1) = \psi(g^n) = \psi(g)^n$ , then  $\psi(g)$  can be diagonalized.

**Theorem 4.2.14** (The First Orthogonality Relation for Group Characters). Let  $G$  be a finite group and let  $\chi_1, \dots, \chi_r$  be the irreducible characters of  $G$  over  $\mathbb{C}$ . Then

$$(\chi_i, \chi_j) = \delta_{ij}$$

*Proof:* The orthonormality of the irreducible characters will follow directly from the orthogonality of the central primitive idempotents via the following calculation:

$$\begin{aligned} z_i \delta_{ij} &= z_i z_j \\ &= \frac{\chi_i(1)}{|G|} \frac{\chi_j(1)}{|G|} \sum_{g,h \in G} \chi_i(g^{-1}) \chi_j(h^{-1}) gh \\ &= \frac{\chi_i(1)}{|G|} \frac{\chi_j(1)}{|G|} \sum_{y \in G} \left[ \sum_{x \in G} \chi_i(xy^{-1}) \chi_j(x^{-1}) \right] y \end{aligned}$$

By the expression of the coefficient of  $z_i$ , we have

$$\delta_{ij} \frac{\chi_i(1)}{|G|} \chi_i(g^{-1}) = \frac{\chi_i(1)\chi_j(1)}{|G|^2} \sum_{x \in G} \chi_i(xg^{-1}) \chi_j(x^{-1}).$$

Simplifying (and replacing  $g$  by  $g^{-1}$ ) gives

$$\delta_{ij} \frac{\chi_i(g)}{\chi_j(1)} = \frac{1}{|G|} \sum_{x \in G} \chi_i(xg) \chi_j(x^{-1}) \quad \text{for all } g \in G$$

Taking  $g = 1$ , we have

$$\delta_{ij} = \frac{1}{|G|} \sum_{x \in G} \chi_i(x) \chi_j(x^{-1})$$

Then by Lemma 4.2.13, we get the final result.

**Theorem 4.2.15** ((The Second Orthogonality Relation for Group Characters)). Denote the number of conjugate conjugacy class of  $x$  by  $|C_G(x)|$ , then

$$\sum_{i=1}^r \chi_i(x) \overline{\chi_i(y)} = \begin{cases} |C_G(x)| & \text{if } x \text{ and } y \text{ are conjugate in } G \\ 0 & \text{otherwise.} \end{cases}$$

*Proof:* Take  $x_i$  to be the element of  $C_i$ , notice that

$$|G| \delta_{jk} = |G| (\chi_j, \chi_k) = \sum_{i=1}^r |C_i| \chi_j(x_i) \overline{\chi_k(x_i)}$$

Let  $W = \text{diag}\{|C_1|, \dots, |C_r|\}$ ,  $X = (\chi_i(x_j))$ . Then  $WXX^H = \text{diag}\{|G|, \dots, |G|\}$ ,

## 4.3 Induced representation

**Definition 4.3.1.** Let  $H$  be a subgroup of the finite group  $G$  and let  $V$  be an  $FH$ -module affording the representation  $\varphi$  of  $H$ . The  $FG$ -module  $FG \otimes_{FH} V$  is called the induced module of  $V$  and the representation of  $G$  it affords is called the induced representation of  $\varphi$ . If  $\psi$  is the character of  $\varphi$  then the character of the induced representation is called the induced character and is denoted by  $\text{Ind}_H^G(\psi)$ .

**Proposition 4.3.2.** Let  $H$  be a subgroup of the finite group  $G$  and let  $g_1, \dots, g_m$  be representatives for the distinct left cosets of  $H$  in  $G$ . Let  $V$  be an  $FH$ -module affording the matrix representation  $\varphi$  of  $H$  of degree  $n$  under the basis  $v_1, \dots, v_n$ . The  $FG$ -module  $W = FG \otimes_{FH} V$  has dimension  $nm$  over  $F$  and there is a basis of  $W$  such that  $W$  affords the matrix representation under the basis

$$g_1 \otimes v_1, g_1 \otimes v_2, \dots, g_1 \otimes v_n, g_2 \otimes v_1, \dots, g_2 \otimes v_n, \dots, g_m \otimes v_n$$

,  $\Phi$  defined for each  $g \in G$  by

$$\Phi(g) = \begin{pmatrix} \varphi(g_1^{-1}gg_1) & \cdots & \varphi(g_1^{-1}gg_m) \\ \vdots & \ddots & \vdots \\ \varphi(g_m^{-1}gg_1) & \cdots & \varphi(g_m^{-1}gg_m) \end{pmatrix}$$

where each  $\varphi(g_i^{-1}gg_j)$  is an  $n \times n$  block appearing in the  $i, j$  block position of  $\Phi(g)$ , and where  $\varphi(g_i^{-1}gg_j)$  is defined to be the zero block whenever  $g_i^{-1}gg_j \notin H$ .

**Corollary 4.3.3.** If  $\psi$  is the character afforded by  $V$  then the induced character is given by

$$\text{Ind}_H^G(\psi)(g) = \sum_{i=1}^m \psi(g_i^{-1}gg_i)$$

where  $\psi(g_i^{-1}gg_i)$  is defined to be 0 if  $g_i^{-1}gg_i \notin H$ , and

$\text{Ind}_H^G(\psi)(g) = 0$  if  $g$  is not conjugate in  $G$  to some element of  $H$ . In particular, if  $H$  is a normal subgroup of  $G$  then  $\text{Ind}_H^G(\psi)$  is zero on all elements of  $G - H$ .

**Theorem 4.3.4.** Let  $G$  be a group, let  $H$  be a subgroup of  $G$  and let  $\psi$  and  $\psi'$  be characters of  $H$ .

(1) (Induction of characters is additive)  $\text{Ind}_H^G(\psi + \psi') = \text{Ind}_H^G(\psi) + \text{Ind}_H^G(\psi')$ .

(2) (Induction of characters is transitive) If  $H \leq K \leq G$  then

$$\text{Ind}_K^G(\text{Ind}_H^K(\psi)) \cong \text{Ind}_H^G(\psi)$$

**Proposition 4.3.5** (Frobenius reciprocity). Let  $G$  be a group, let  $H$  be a subgroup of  $G$  and let  $\psi$  and  $\varphi$  be characters of  $H$  and  $G$ . Then

$$\langle \psi, \text{Res } \varphi \rangle_H = \langle \text{Ind } \psi, \varphi \rangle_G$$

*Proof:* Take  $V$  be a  $\mathbb{C}[G]$ -module and  $W$  be a  $\mathbb{C}[H]$ -module such that  $\psi$  is the character of  $W$  and  $\varphi$  is the character of  $V$ . Let  $\tilde{V}$  be the  $\mathbb{C}[H]$ -module induced by  $V$ .

By Theorem 2.2.26,

$$\langle \psi, \text{Res } \varphi \rangle_H = \dim_{\mathbb{C}} \text{Hom}(W, \tilde{V}) = \dim_{\mathbb{C}} \text{Hom}(\mathbb{C}[G] \otimes_{\mathbb{C}[H]} W, V) = \langle \text{Ind } \psi, \varphi \rangle_G$$

**Proposition 4.3.6.**  $G$  is a group,  $H$  and  $K$  are the subgroup of  $G$ . Let  $\{s_1, \dots, s_r\}$  be the representation elements of double coset decomposition of  $G$  by  $H$  and  $K$ . i.e.

$$G = Ks_1H \cup \dots \cup Ks_rH$$

where  $Ks_iH \cap Ks_jH = \emptyset$  if  $i \neq j$ .  $(V, \rho)$  be a representation of  $H$  and  $\text{Ind}_H^G(\rho)$  be the induced representation. The restriction  $\text{Res}_K(\text{Ind}_H^G(\rho))$  of the  $G$ -representation  $\text{Ind}_H^G(\rho)$  to a  $K$ -representation decomposes as a direct sum

$$\bigoplus_{i=1}^r \text{Ind}_{s_i^{-1}Hs_i \cap K}^K(\rho^{s_i})$$

$\rho^{s_i}(x) := \rho(s_i x s_i^{-1})$  for  $x$  belonging to the subgroup  $s_i^{-1}Hs_i \cap K$  that depends only on equivalence class of  $s_i$  and not on its chosen representative  $s$ .

*Proof:* Notice that there's  $\mathbb{C}[K]$ -module isomorphism

$$\mathbb{C}[G] \otimes_{\mathbb{C}[H]} V \cong \bigoplus_{i=1}^r \mathbb{C}[K]s_i\mathbb{C}[H] \otimes_{\mathbb{C}[H]} V \cong \bigoplus_{i=1}^r \mathbb{C}[K] \otimes_{\mathbb{C}[K \cap s_i H s_i^{-1}]} \tilde{V}$$

where  $\tilde{V}$  is a representation of  $K \cap s_i H s_i^{-1}$  defined by  $(s_i h s_i^{-1}) \cdot v = h v$  and in this equation, the isomorphisc map between  $\mathbb{C}[K] \otimes_{\mathbb{C}[K \cap s_i H s_i^{-1}]} \tilde{V}$  and  $\mathbb{C}[K]s_i\mathbb{C}[H] \otimes_{\mathbb{C}[H]} V$  is induced by bi-additive maps

$$\begin{aligned} \mathbb{C}[K] \times \tilde{V} &\rightarrow \mathbb{C}[K]s_i\mathbb{C}[H] \otimes_{\mathbb{C}[H]} V \\ (k, v) &\mapsto k s_i \otimes v \end{aligned}$$

and

$$\begin{aligned} \mathbb{C}[K]s_i\mathbb{C}[H] \times V &\rightarrow \mathbb{C}[K] \otimes_{\mathbb{C}[K \cap s_i H s_i^{-1}]} \tilde{V} \\ (k s_i h, v) &\mapsto k \otimes h v \end{aligned}$$

**Corollary 4.3.7** (Mackey's irreducibility criterion). With all the notations in above Proposition, in order to make the induced representation  $\text{Ind}_H^G \rho$  be irreducible, it is necessary and sufficient that the following two conditions be satisfied:

- (1)  $\rho$  is irreducible.
- (2) For each  $s \in G - H$  the two representations  $\rho^s$  and  $\text{Res}_s(\rho)$  of  $H_s$  are disjoint.

*Proof:* Let  $\varphi$  be the character of  $\rho$ , by Frobenius reciprocity,

$$\langle \text{Ind}_H^G(\varphi), \text{Ind}_H^G(\varphi) \rangle = \langle \varphi, \text{Res}(\text{Ind}(\varphi)) \rangle$$

Let  $\chi_i$  be the character of  $\rho^{s_i}$ , then by Frobenius reciprocity and Proposition 4.3.6

$$\langle \varphi, \text{Res}(\text{Ind}(\varphi)) \rangle = \sum_{i=1}^r \langle \text{Res}_{s_i^{-1}Hs_i \cap H}(\varphi), \chi_i \rangle$$

**Corollary 4.3.8.** Suppose  $H$  is normal in  $G$ . In order that  $\text{Ind}_H^G(\rho)$  be irreducible, it is necessary and sufficient that  $\rho$  be irreducible and not isomorphic to any of its conjugates  $\rho^s$  for  $s \notin H$ .

**Definition 4.3.9.** Let  $G$  be a finite group and let  $\chi_1, \dots, \chi_h$  be its distinct irreducible characters. A class function on  $G$  is a character if and only if it is a linear combination of the  $\chi_i$ 's with non-negative integer coefficients. We will denote by  $R^+(G)$  the set of these functions, and by  $R(G)$  the group generated by  $R^+(G)$ , i.e., the set of differences of two characters. We have

$$R(G) = \mathbb{Z}\chi_1 \oplus \cdots \oplus \mathbb{Z}\chi_h.$$

An element of  $R(G)$  is called a virtual character. Since the product of two characters is a character,  $R(G)$  is a subring of the ring  $F(G)$  of class functions on  $G$  with complex values. Since the  $\chi_i$  form a basis of  $F(G)$ , by Theorem 2.2.30, we have  $\mathbb{C}$ -algebra isomorphism

$$F(G) \cong \mathbb{C} \otimes_{\mathbb{Z}} R(G)$$

**Theorem 4.3.10.**

**Theorem 4.3.11** (Artin).

Reference: Matsumura, Atiyah, Gortz 1, GTM73, GTM42, Dummit, GTM52, Milne:Galois Theory, Red book, Hu Yong quan:Galois Theory