Algebra

Erzhuo Wang

June 24, 2024

Contents

1 Abstract Algebra **5**

1.1 Group Theory 5

1.2 Field Theory 9

2 Commutative Algebra **19**

2.1 Basic Definition in Ring Thoery 19

2.2 Basic Definition in Module 23

2.3 Specturm 33

2.4 Chain conditions 38

2.5 Localization 40

2.6 Intergral Extension 46

2.7 Flatness 47

2.8 Dimension Theory and Hilbert's Nullstellensatz 48

2.9 Completion 53

3 Homological Algerba **55**

3.1 Basic Definition in Category 55

3.2 Abelian Category 63

3.3 Derived Functor 66

3.4 Ext and Tor 69

3.5 Group Cohomology 70

4 Theory of Scheme **71**

4.1 Sheaf Theory 71

5 Representation Theory **77**

5.1 Definition 77

5.2 Character 83

5.3 Induced representation 86

Chapter 1

Abstract Algebra

1.1 Group Theory

Definition 1.1.1. 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_α. This means that there is a finite sequence $(x_1, \ldots, x_n)$ of elements of the groups G_α such that $x = x_1 \cdots x_n$. Such a sequence is called a word (of length n) in the groups G_α; it is said to represent the element x of G.

Definition 1.1.2. A word representing x of the form $(y_1, \ldots, y_m)$, where no group G_α contains both y_i and y_{i+1}, and where $y_i \neq 1$ for all i is called a reduced word.

Definition 1.1.3 (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_α if for each $x \in G$, there is only one reduced word in the groups G_α 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 1.1.4. Suppose the groups G_α 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 1.1.5. 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_α, then G satisfies the following condition: Given any group H and any family of homomorphisms $h_\alpha : G_\alpha \to H$, there exists a homomorphism $h : G \to H$ whose restriction to G_α equals h_α, for each α. Furthermore, h is unique.

Definition 1.1.6 (external free product)**.** Let $\{G_\alpha\}_{\alpha \in J}$ be an indexed family of groups. Suppose that G is a group, and that $i_\alpha : G_\alpha \to G$ 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_α, relative to the monomorphisms i_α.

Proposition 1.1.7 (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 $i_\alpha : G_\alpha \to G$ such that G is the free product of the groups $i_\alpha\left(G_\alpha\right)$.

Proof: We define a word (of length n) in the elements of the groups G_α to be an n-tuple $w=(x_1,\ldots,x_n)$ of elements of $\bigcup G_\alpha$. It is called a reduced word if $\alpha_i \neq \alpha_{i+1}$ for all i, where α_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_{α_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_α. Let $P(W)$ denote the set of all bijective functions $\pi : W \to W$. 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 α and each $x \in G_\alpha$, we define a set map $\pi_x : W \to W$. It will satisfy the following conditions:

(1) If $x = 1_\alpha$, the identity element of G_α, then π_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 $w = (x_1,\ldots,x_n)$ denote the general nonempty element of W, and let α_1 denote the index such that $x_1 \in G_{\alpha_1}$. If $x \neq 1_\alpha$, define π_x as follows:

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

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

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

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

If $x = 1_\alpha$, define π_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 $G'_\alpha = i_\alpha\left(G_\alpha\right)$. We show that G is the free product of the groups G'_α.

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 π_x nor π_y is the identity map of W and show that $\pi_x \neq \pi_y$. But this is easy, for $\pi_x(\varnothing) = (x)$ and $\pi_y(\varnothing) = (y)$, and these are different words. Second, we show that no nonempty reduced word

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

in the groups G'_α represents the identity element of G. Let α_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

$$\pi_{x_1}\left(\pi_{x_2}\left(\cdots\left(\pi_{x_n}(\varnothing)\right)\right)\right) = (x_1, \ldots, x_n)\,,$$

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

Proposition 1.1.8. 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 1.1.9 (extension property)**.** Let $\{G_\alpha\}$ be a family of groups; let G be a group, let $i_\alpha : G_\alpha \to G$ be a family of homomorphisms. The following statement are equivalent:

(1) If each i_α is a monomorphism and G is the free product of the groups $i_\alpha\left(G_\alpha\right)$

(2) (coproduct)Given a group H and a family of homomorphisms $h_\alpha : G_\alpha \to H$, there exists a homomorphism $h : G \to H$ such that $h \circ i_\alpha = h_\alpha$ for each α.

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

Proposition 1.1.10 (Uniqueness of free products)**.** Let $\{G_\alpha\}_{\alpha\in J}$ be a family of groups. Suppose G and G' are groups and $i_\alpha : G_\alpha \to G$ and $i'_\alpha : G_\alpha \to G'$ are families of monomorphisms, such that the families $\{i_\alpha\left(G_\alpha\right)\}$ and $\{i'_\alpha\left(G_\alpha\right)\}$ generate G and G', respectively. If both G and G' have the extension property, then there is a unique isomorphism $\phi : G \to G'$ such that $\phi \circ i_\alpha = i'_\alpha$ for all α.

Proposition 1.1.11. 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

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

Proof: By Proposition 1.1.10 and Propostion 1.1.9, it suffice to show $G_1/N_1 \to G/N, G_2/N_2 \to G/N$ satisfies extension property.

$$\begin{tikzcd}
 & G_1 \arrow[r, "\pi_1"] \arrow[dl, "i_1"'] & G_1/N_1 \arrow[dr, "h_1"] \arrow[dddl, dashed, "\tilde{i}_1"] & \\
G_1*G_2 \arrow[rrr, dashed, "i_1*i_2"] \arrow[ddr, bend right] & & & H \\
 & G_2 \arrow[ul, "i_2"] \arrow[r] & G_2/N_2 \arrow[ur] \arrow[dl, dashed, "\tilde{i}_2"] & \\
 & G_1*G_2/N \arrow[uurr, bend right, "gN \mapsto (i_1*i_2)(g)"'] & &
\end{tikzcd}$$

Definition 1.1.12 (free group)**.** Let $\{a_\alpha\}$ be a family of elements of a group G. Suppose each a_α generates an infinite cyclic subgroup G_α 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_α 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 1.1.13. Let $\{a_\alpha\}_{\alpha\in J}$ be an arbitrary indexed family. Let G_α denote the set of all symbols of the form a_α^n for $n \in \mathbb{Z}$. We make G_α into a group by defining

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

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

Theorem 1.1.14. 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 $h : F \to G$ 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_β. In this case, we call the family $\{r_\beta\}$ a complete set of relations for G.

Definition 1.1.15. 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 1.1.16. $f : G \to H$ is a surjective group homomorphism, $\tilde{f} : G_{ab} \to H_{ab}$ is the natural homomorphism induced by f. Let $i : G \to G_{ab}$ be the natrual projection. Then $\mathrm{Ker}\tilde{f} = i(\mathrm{Ker} f)$

Example 1.1.17. Consider

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

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

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 $F = F(a_1, \ldots, a_n) \to G$, which induces a surjective homomorphism $\tilde{f} : F_{ab} \to G_{ab}$. Then by Proposition 1.1.16, G_{ab} is isomorphic to $\mathbb{Z}a_1 \oplus \ldots \mathbb{Z}a_n/(2(a_1 + \cdots + a_n))$.

1.2 Field Theory

Theorem 1.2.1. Let $p(x) \in F[x]$ be an irreducible polynomial of degree n over the field F and let K be the field $F[x]/(p(x))$. Let $\theta = x \bmod (p(x)) \in K$. Then the elements

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

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

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

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

Definition 1.2.2. Let K be an extension of the field F and let S be a subset of K. Then the smallest subfield of K containing both F and the elements $s \in S$, denoted $F(S)$ is called the field generated by S over F. If the field K is generated by a single element α over $F, K = F(\alpha)$, then K is said to be a simple extension of F and the element α is called a primitive element for the extension.

Theorem 1.2.3. Let F be a field and let $p(x) \in F[x]$ be an irreducible polynomial. Suppose K is an extension field of F containing a root α of $p(x) : p(\alpha) = 0$. Let $F(\alpha)$ denote the subfield of K generated over F by α. Then

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

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

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

Theorem 1.2.4. Let $\varphi : F \xrightarrow{\sim} F'$ be an isomorphism of fields. Let $p(x) \in F[x]$ be an irreducible polynomial and let $p'(x) \in F'[x]$ be the irreducible polynomial obtained by applying the map φ to the coefficients of $p(x)$. Let α be a root of $p(x)$ (in some extension of F) and let β be a root of $p'(x)$ (in some extension of F'). Then there is an isomorphism

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

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

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

Definition 1.2.5. The element $\alpha \in K$ is said to be algebraic over F if α is a root of some nonzero polynomial $f(x) \in F[x]$. If α is not algebraic over F, then α is said to be transcendental over F. The extension K/F is said to be algebraic if every element of K is algebraic over F.

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

Theorem 1.2.6. Let α be algebraic over the field F and let $F(\alpha)$ be the field generated by α over F. Then

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

so that in particular

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

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

Proposition 1.2.7. The element $\alpha \in K$ is algebraic over F if and only if the simple extension $F(\alpha)/F$ is finite. More precisely, if α is an element of an extension of degree n over F then α satisfies a polynomial of degree at most n over F and if α satisfies a polynomial of degree n over F then the degree of $F(\alpha)$ over F is at most n.

Definition 1.2.8. 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 1.2.9. $F(\alpha,\beta) = (F(\alpha))(\beta)$, i.e., the field generated over F by α and β is the field generated by β over the field $F(\alpha)$ generated by α. In general, if $a_1, \ldots, a_n$ be elements of K, then $F(a_1, \ldots, a_n) = ((F(a_1)(a_2)) \ldots)(a_n)$

Corollary 1.2.10. If $K \subset L \subset M$ are field extensions, $L/K, M/L$ are algebraic extensions, then M/K is algerbaic.

Definition 1.2.11 (spilting field)**.** The extension field K of F is called a splitting field for the polynomial $f(x) \in F[x]$ if $f(x)$ factors completely into linear factors (or splits completely) in $K[x]$ and $f(x)$ does not factor completely into linear factors over any proper subfield of K containing F.

Theorem 1.2.12. For any field F, if $f(x) \in F[x]$ then there exists an extension K of F which is a splitting field for $f(x)$.

Proof: We first show that there is an extension E of F over which $f(x)$ splits completely into linear factors by induction on the degree n of $f(x)$. If $n = 1$, then take $E = F$. Suppose now that $n > 1$. If the irreducible factors of $f(x)$ over F are all of degree 1 , then F is the splitting field for $f(x)$ and we may take $E = F$. Otherwise, at least one of the irreducible factors, say $p(x)$ of $f(x)$ in $F[x]$ is of degree at least 2 . Hence, there is an extension E_1 of F containing a root α of $p(x)$. Over E_1 the polynomial $f(x)$ has the linear factor $x - \alpha$. The degree of the remaining factor $f_1(x)$ of $f(x)$ is $n-1$, so by induction there is an extension E of E_1 containing all the roots of $f_1(x)$. Since $\alpha \in E, E$ is an extension of F containing all the roots of $f(x)$. Now let K be the intersection of all the subfields of E containing F which also contain all the roots of $f(x)$. Then K is a field which is a splitting field for $f(x)$.

Theorem 1.2.13. Let $\varphi : F \xrightarrow{\sim} F'$ be an isomorphism of fields. Let $f(x) \in F[x]$ be a polynomial and let $f'(x) \in F'[x]$ be the polynomial obtained by applying φ to the coefficients of $f(x)$. Let E be a splitting field for $f(x)$ over F and let E' be a splitting field for $f'(x)$ over F'. Then the isomorphism φ extends to an isomorphism $\sigma : E \xrightarrow{\sim} E'$, i.e., σ restricted to F is the isomorphism φ :

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

Definition 1.2.14. The field $\bar{F}$ is called an algebraic closure of F if $\bar{F}$ is algebraic over F and if every polynomial $f(x) \in F[x]$ splits completely over $\bar{F}$ (so that $\bar{F}$ can be said to contain all the elements algebraic over F).

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

Theorem 1.2.15. Let $\bar{F}$ be an algebraic closure of F. Then F is algebraically closed.

Proof: By Corollary 1.2.10.

Theorem 1.2.16. For any field F, algebraic closure of F exists and is unique up to isomorphism.

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

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

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

Uniqueness: It is suffice to show:

Lemma 1.2.17. Let $\varphi : F \xrightarrow{\sim} F'$ be an isomorphism of fields, $\bar{F}'$ bethe algebraic closure of F', E/F is a algebraic extension, then there's $\sigma : E \to \bar{F}'$ ring homomorphism satisfying $\sigma|_F = \varphi$

Proof of the lemma: By Zorn's Lemma and Theorem 1.2.4. □

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

Definition 1.2.18 (separable)**.** A polynomial $f(x) \in F[x]$ is separable if $f(x)$ has no multiple root in $\bar{F}$.

Proposition 1.2.19. A polynomial $f(x)$ has a multiple root $\alpha \in \bar{F}$ if and only if α is also a root of $f'(x)$. In particular, $f(x)$ is separable if and only if it is relatively prime to its derivative: $(f(x), D_x f(x)) = 1$.

Remark 1.2.20. For any two polynomials $f(x), g(x) \in F[x]$, they have the same g.c.d in $F[x]$ and $\bar{F}[x]$ since Euclidean division doesn't change if we replace F by any extension field of F.

Definition 1.2.21. $\alpha \in \bar{F}$ is separable if $m_\alpha(x) \in F[x]$ is separable polynomial.

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

Definition 1.2.22 (perfect field)**.** A field $F \subset \bar{F}$ is perfect if and only if every finite extension of F is separable.

Lemma 1.2.23. Let $p(x)$ be an irreducible polynomial over a field F of characteristic p. Then there is a unique integer $k \geq 0$ and a unique irreducible separable polynomial $p_{\text{sep}}(x) \in F[x]$ such that

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

Proposition 1.2.24. A field F is perfect if and only if it is a field of characteristic 0 or a field of characteristic $p > 0$ such that every element has a p-th root.

Proof: '$\Longleftarrow$': case 1: If $\operatorname{chap} F = 0$, then by Proposition 1.2.19, F is perfect.

case 2: If $\operatorname{chap} F = p$, $\alpha \in \bar{F}$, and $p(x) = m_\alpha(x) \in F[x]$ is inseparable, by Lemma 1.2.23, there's irreducible polynomial $q(x)$ such that $p(x) = q(x^p)$. Hence

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

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

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

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

Corollary 1.2.25. In the proof of above Proposition, we can get: If $\operatorname{chap} F = 0$ and $p(x) = x^p - \alpha \in F[x]$, either $p(x)$ is irreducible or $p(x) = (x - \beta)^p$ for some $\beta \in F$.

Example 1.2.26. $\mathbb{Q}, \mathbb{F}_q$ are perfect fields and $\mathbb{F}_p(t)$ is not perfect field.

Definition 1.2.27. Given field extensions $F \subset E \subset \bar{F}$, E is called purely inseparable if for each $\alpha \in E$ the minimal polynomial of α over F has only one distinct root. It is easy to see that the following are equivalent:

(1) E/F is purely inseparable

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

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

Definition 1.2.28. Let $F \subset E \subset \bar{F}$ be field extensions, we call E/F normal if for all $\alpha \in E$, all the roots of $m_\alpha(x)$ lie in E.

Definition 1.2.29. Let $F \subset E \subset \bar{F}$ be field extensions. Let $\operatorname{Aut}(E/F)$ be the collection of automorphisms of K which fix F.

Theorem 1.2.30. Let $F \subset E \subset \bar{F}$ be field extensions, the following statements are equivalent:

(1) E/F is normal.

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

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

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

(2)$\Longrightarrow$(1): By Lemma 1.2.16

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

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

Proposition 1.2.31. Given field extensions $F \subset E \subset \bar{F}$, then all F-algerba homomorphisms from E to E are in $\operatorname{Aut}(E/F)$ i.e. $\operatorname{Aut}(E/F) = \{F\text{-algebra homomorphism between } E \text{ and } E\}$

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

Theorem 1.2.32. Let E be the splitting field over F of the polynomial $f(x) \in F[x]$. Then

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

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

Definition 1.2.33. Let E/F be a finite extension. Then E is said to be Galois over F and E/F is a Galois extension if $|\operatorname{Aut}(E/F)| = [E : F]$. If E/F is Galois the group of automorphisms $\operatorname{Aut}(E/F)$ is called the Galois group of E/F, denoted $\operatorname{Gal}(E/F)$.

Proposition 1.2.34. We have 4 characterizations of Galois extensions E/F :

(1) splitting fields of separable polynomials over F

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

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

(4) finite, normal and separable extensions.

Theorem 1.2.35 (Fundamental Theorem of Galois Theory)**.** $F \subset K \subset \bar{F}$ be field extensions. K/F be a Galois extension and set $G = \operatorname{Gal}(K/F)$. Then there is a bijection:

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

given by the correspondences

$$\begin{tikzcd}
E \arrow[r] & \{\text{elements of } G \text{ fixing } E\} \\
\text{fix field of } H & H \arrow[l]
\end{tikzcd}$$

which are inverse to each other. Under this correspondence,

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

$$\begin{tikzcd}
\{F\text{-algebra homomorphism between } E \text{ and } \bar{F}\} \arrow[dr, "\text{Extended by 1.2.16 and 1.2.31}"] & \\
\{\text{left cosets of } H \text{ in } G\} \arrow[u, "\sigma H \mapsto \sigma|_E"'] \arrow[r, "\sigma H \mapsto \sigma|_E"] & \{\sigma|_E : \sigma \in G\}
\end{tikzcd}$$

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

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

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

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

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

In particular, by (1) and Theorem 1.2.30, E is normal(hence Galios) over F if and only if H is a normal subgroup in G. If this is the case, then the Galois group is isomorphic to the quotient group

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

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

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

Theorem 1.2.36. Suppose K/F is a Galois extension and F'/F is any extension. Then KF'/F' is a Galois extension, with Galois group

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

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

Corollary 1.2.37. Suppose K/F is a Galois extension and F'/F is any finite extension. Then

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

Theorem 1.2.38. Let K_1 and K_2 be Galois extensions of a field F. Then

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

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

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

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

Corollary 1.2.39. E/F be finite separable extension, there's Galois extension K_1 contains E(for example, the composite of the splitting fields of the minimal polynomials for a basis for E over F). Take S be the set of all the Galios extenison of F which contains E, then

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

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

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

Corollary 1.2.40. If K/F is finite and separable, then K/F is simple. In particular, any finite extension of fields of characteristic 0 is simple.

Corollary 1.2.41. K_1 and K_2 are separable extensions over F, then K_1K_2 also separable over F. In particular, all the separable elements in $\bar{F}$ form a field. We call it separable closure of F and denote it by F_{sep}.

Proposition 1.2.42. $\bar{F}/F_{sep}$ is pruely inseparable extension and F_{sep} is separable and normal extension.

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

Theorem 1.2.43. Let G be a topological group, and let $\mathcal{N}$ be a neighbourhood base for the identity element e of G. Then

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

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

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

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

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

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

Definition 1.2.44. Given field extensions $F \subset E \subset \bar{F}$, E/F is called Galios extension iff E/F is separable and normal.

Theorem 1.2.45. $(L_i)_{i\in I}$ are all finite Galios extenison of F contained in E, notice that $\mathrm{Gal}(E/L_iL_j) \subset \mathrm{Gal}(E/L_i)\cap\mathrm{Gal}(E/L_j)$ for $i, j \in I$ and for all $\sigma \in \mathrm{Gal}(E/F)$, $\sigma^{-1}\mathrm{Gal}(E/L_i)\sigma = \mathrm{Gal}(E/L_i)$. Hence $(\mathrm{Gal}(E/L_i)_{i\in I}$ induce a topological group structure on $\mathrm{Gal}(E/F)$ such that $(\mathrm{Gal}(E/L_i)_{i\in I}$ form a neighborhood at e of G. We call it Krull topology.

Theorem 1.2.46 (infinite Galios correspondence)**.**

Definition 1.2.47.

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

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

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

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

Proposition 1.2.49. *E/F be a field extension, $\alpha_1, \ldots, \alpha_n \in E$, $F_i = F(a_1, \ldots, a_i)$, then $\{\alpha_1, \ldots, \alpha_n\}$ is algebracally independent over F, if and only if α_i is transcendental over F_{i-1} for all $i = 1, \ldots, n$.*

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*

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

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

given by the correspondences

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

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

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

Definition 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 interchapter 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! □

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

Definition 2.1.13. The interchapter of all maximal ideals of a ring $A \neq 0$ is called the Jacobson radical, or simply the radical of A and written $rad(A)$.

Proposition 2.1.14. $x \in rad(A)$ 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, $m = rad(A)$ 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 $I_1, I_2, ..., I_n$ are ideals which are coprime(i.e. $I_i + I_j = A$ for all $i \neq j$) in pairs then $I_1 I_2 \dots I_n = I_1 \cap I_2 \cdots \cap I_n$

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

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

and the isomorphism map is given by

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

Theorem 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. $P \supset I_1 \dots I_n$, then $P \supset I_i$ for some $1 \leq i \leq n$.

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

Definition 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: $r = p_1 \dots p_n$

2. the decomposition in (1) is unique up to associates.

Proposition 2.1.23. A intergral domain R is U.F.D if and only if every irreducible element is prime and there's no infinite sequence (a_n) in R satisfying: $a_i | a_{i+1}$, a_i and a_j are not associate.

Definition 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.

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:

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

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

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

is a R-module structure.

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

Definition 2.2.3. $f : R \to B$ is a ring homomorphism, then B naturally has a R-module structure, we call B(with both a ring structure and A-module sturcte) a R-algebra.

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

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

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

Definition 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 $a \equiv 1 (\mathrm{mod}\, I)$. If in addition $I \subset rad(A)$, 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 $rad(A)$. 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 $\bar{M} = M/\mathrm{m}M$. Now $\bar{M}$ is a finite-dimensional vector space over k, and we write $\boldsymbol{n}$ for its dimension. Then:

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

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

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

Proof:

(1) and (2): By Corollary 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 $\varphi : F \longrightarrow M$ from the free module $F = Ae_1 \oplus \cdots \oplus Ae_n$ to M by $\varphi\left(\sum a_i e_i\right) = \sum a_i \omega_i$; if we set $K = \mathrm{Ker}(\varphi)$ then, from the minimal basis property(1),

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

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

Proposition 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 I, consider a A/I-module isomorphism

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

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

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

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

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

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

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

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

$$\begin{tikzcd}
 & L_2 \arrow[r, "f"] \arrow[d, "\beta"] & L_1 \arrow[r, "g"] \arrow[d, "\alpha"] & M \arrow[r] \arrow[d, "\mathrm{id}"] & 0 \\
0 \arrow[r] & K \arrow[r, "\psi"] & N \arrow[r, "\varphi"] & M \arrow[r] & 0
\end{tikzcd}$$

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

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

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

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

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

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

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

Proposition 2.2.15. Let A be a ring and let $A[x]$ be the ring of polynomials in an indeterminate x, with coefficients in A. Let $f = a_0 + a_1x + \cdots + a_nx^n \in A[x]$. Prove that

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

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

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

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

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

Definition 2.2.16. Let R be a ring, let A_R be a right R-module, let ${}_RB$ be a left R module, and let G be an (additive) abelian group. A function $f : A \times B \to G$ is called R-biadditive if, for all $a, a' \in A, b, b' \in B$, and $r \in R$, we have

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

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

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

Definition 2.2.17 (Tensor product)**.** Given a ring R and modules A_R and ${}_RB$, then their tensor product is an abelian group $A \otimes_R B$ and an R-biadditive function $h : A \times B \to A \otimes_R B$

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

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

Proposition 2.2.18. If R is a commutative ring and A, B are R-modules, then $A \otimes_R B$ is an R-module($r(a \otimes b) = (ra \otimes b)$), the function $h : A \times B \to A \otimes_R B$ is R-bilinear, and, for every R-module M and every R-bilinear function $g : A \times B \to M$, there exists a unique R-homomorphism $\tilde{g} : A \otimes_R B \to M$ making the following diagram commute.

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

Proposition 2.2.19. A is a ring, I is an ideal of A, M is a A-module, then $M \otimes_A (A/I) \simeq M/IM$ as A/I-module.

Proposition 2.2.20. If R is a ring, and $A_{R}, {}_RB$ are R-modules, then there are R-module isomorphisms:

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

Theorem 2.2.21. If R and S are rings and A_R, ${}_RB_S$, S_C are (bi)modules, then there is an isomorphism:

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

Theorem 2.2.22 (Commutativity)**.** If R is a commutative ring and M_R, ${}_RN$ are modules, then there is a R-isomorphism

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

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

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

Theorem 2.2.23. Let R be a ring, A,$\{A_i\}_{i\in I}$ are right R-modules, B and $\{B_j\}_{j\in J}$ left R-modules. Then there are group isomorphisms:

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

Theorem 2.2.24 (Adjoint Associativity)**.** Let R and S be rings, let A be a right R-module, let B be an (R, S)-bimodule and let C be a right S-module. Then there is an natural bijection(acturally a isomorphism of abelian groups):

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

given by

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

and

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

Remark 2.2.25. 'natrual' in above theorem means: ${}_RB_S$ is a bi-module, then $(\_\_ \otimes_R B, \mathrm{Hom}_S(B, \_\_))$ is a adjoint pair between right R-module category and right S-module category.

Remark 2.2.26. (1) If ${}_RB_S$ is a bi-module, C is a right R-module, $\mathrm{Hom}_S(B, C)$ has a natrual right R-module sturct. Notice that we can define $fr(b) = f(rb)$, then $fr(bs) = f(r(bs)) = f((rb)s) = f(rb)s = (fr(b))s$,$f(r_1r_2)(b) = (fr_1)r_2(b)$. It makes $\mathrm{Hom}_S(B, C)$ to be a right R-module.

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

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

Proposition 2.2.27. If M is a left R-module, then there's left R-module isomorphism

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

Theorem 2.2.28. Let R be a ring with. If A is a right R-module and F is a free left R-module with basis Y, thell 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 2.2.29. If R is a ring with identity and A_R and ${}_RB$ are free R-modules with bases X and Y respectively, then $A \otimes_R B$ is a free (right) R-module($(a \otimes b)r = ar \otimes b$) with basis $W = \{x \otimes y : x \in X, y \in Y\}$.

Proposition 2.2.30. 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

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

Lemma 2.2.31 (The Short Five Lemma)**.** Let R be a ring and

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

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

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

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

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

Definition 2.2.32 (Spilt 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)

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

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

(5)

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

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

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

Lemma 2.2.33 (Snake lemma). Let

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

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

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

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

Proposition 2.2.34.

(1)

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

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

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

is an exact sequence of abelian groups.(Hom$(D,\Box)$ is left exact in $\{R$-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

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

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

Definition 2.2.35 (Projective module)**.** Let R be a ring. The following conditions on an R-module P are equivalent.

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

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

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

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

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

(5) if

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

is any short exact sequence of R-modules, then

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

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

Proposition 2.2.36. Every free module F over a ring R is projective.

Proposition 2.2.37. 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 2.2.38. 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 2.2.39 (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.

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

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

(3) If J is a submodule of B, then there's submodule K such that $B = J \oplus K$.

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

(5) if

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

is any short exact sequence of R-modules, then

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

is an exact sequence of abelian groups.

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

Proposition 2.2.40. A direct product of R-modules $\prod_{i \in I} J_i$ is injective ifand only if J_i is injective for every $J_i, i \in I$.

Proposition 2.2.41. 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 2.2.42. 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 2.2.43. Let R be a ring and let M be an R-module. Then M is contained in an injective R-module.

Proposition 2.2.44. Any modules over a PID, it is a projective module if and only if it is a free module.

Definition 2.2.45 (Flat module)**.** Let A be a right R-module. Then the following are equivalent:

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

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

is a short exact sequence, then

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

is also a short exact sequence.

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

Similarly, we can define left flat R-module.

Proposition 2.2.46. Projective modules are flat.

Example 2.2.47. $\mathbb{Q}/\mathbb{Z}$ is not flat.

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

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

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

Proposition 2.2.48. $\sum_{i\in I} A_i$ flat if and only if each $A_i, i \in I$ flat.

Proof: Since tensor product commute with direct sum.

Example 2.2.49.

	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{Q}/\mathbb{Z}$	$\mathbb{Z} \oplus \mathbb{Q}$
flat	✓	✓(By 2.7.2)	×(2.2.47)	✓(2.2.48)
projective	✓	×(By 2.2.44)	×	×(2.2.37)
injective	×(By 2.2.41)	✓(By 2.2.41)	✓(By 2.2.41)	×(2.2.40)

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

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

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

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

Proof: By Theorem 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) X is compact.

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

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

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

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

Proposition 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 =Spec$A$. When thinking of x as a prime ideal of A, we denote it by P_x. Show that:

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

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

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

Definition 2.3.4. A topological space X is said to be irreducible if $X \neq \varnothing$ and satisfies the following three equivalent conditions:

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

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

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

Proposition 2.3.5. Let X be a topological space.

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

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

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

Proposition 2.3.6. A is a ring, Spec$A$ is the specturm of A.

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

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

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

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

given by the correspondences

$$I \longrightarrow V(I)$$

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

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

Proposition 2.3.8. Let $\varphi : A \to B$ be a ring homomorphism. Let $X =$Spec$A$ and $Y =$Spec$B$. Let ϕ to be the map:

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

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

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

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

(4) If φ is surjective, then ϕ is a homeomorphism of Y onto the closed subset $V(\mathrm{Ker}(\phi))$ 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 $X = \operatorname{Spec} A$ is the spectrum of a ring, then

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

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

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

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

Definition 2.3.11. A topological space is called Noetherian if the closed subsets of X satisfy the descending chain condition, i.e., for closed subsets $Y_1, Y_2, Y_3, \ldots$ with $Y_{i+1} \subset Y_i$ for all positive integers i, there exists an integer n such that $Y_i = Y_n$ for all $i \geq n$. An equivalent condition is that the open subsets satisfy the ascending chain condition.

Example 2.3.12. R is a Noetherian ring, then $X = \operatorname{Spec}(R)$ is a Notherian 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 $Z_1, ..., Z_n \subset X$ such that $X = Z_1 \cup \ldots Z_n$ and $Z_i \nsubseteq Z_j$ for $i \neq j$.

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

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

Corollary 2.3.14. A Notherian ring has only finite many minimal prime ideals.

Proof: By Example 2.3.14 and Theorem 2.3.13.

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

Definition 2.3.15. We will interpret the elements of A as functions from the affine n-space to k, by defining $f(P)=f\left(a_1,\ldots,a_n\right)$, where $f\in A$ and $P\in\mathbf{A}^n$. Thus if $f\in A$ is a polynomial, we can talk about the set of zeros of f, namely $Z(f)=\{P\in\mathbf{A}^n\mid f(P)=0\}$. More generally, if T is any subset of A, we define the zero set of T to be the common zeros of all the elements of T, namely

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

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

Proposition 2.3.16. The union of two algebraic sets is an algebraic set. The intersection of any family of algebraic sets is an algebraic set. The empty set and the whole space are algebraic sets.

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

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

Definition 2.3.17. We define the Zariski topology on $\mathbf{A}^n$ by taking the open subsets to be the complements of the algebraic sets. This is a topology, because according to the proposition, the intersection of two open sets is open, and the union of any family of open sets is open. Furthermore, the empty set and the whole space are both open.

Definition 2.3.18. For any subset $Y\subseteq\mathbf{A}^n$, let us define the ideal of Y in A by

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

Proposition 2.3.19. (1) If $T_1\subseteq T_2$ are subsets of A, then $Z\left(T_1\right)\supseteq Z\left(T_2\right)$.

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

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

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

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

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

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

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

2.4 Chain conditions

Definition 2.4.1 (Notherian)**.** ring(R-module) A is said to be Noetherian if it satisfies the following three equivalent conditions:

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

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

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

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

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

Corollary 2.4.4. If $M_i (1 \leqslant i \leqslant n)$ are Noetherian (resp. Artinian) A-modules, so is $\bigoplus_{i=1}^n M_i$.

Proof: Apply Theorem 2.4.3 to the exact sequence

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

Corollary 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 $(M_i)\,(0 \leqslant i \leqslant n)$ of submodules of M such that

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

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

Proposition 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:

$$P_1 \supset P_1P_2 \cdots \supset P_1 \dots P_n \supset \dots$$

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, $/Ann(M)$ is a Noetherian ring.

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

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

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

Proposition 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) $I \cap S \neq \varnothing$

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

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

(1)⇒(2):Consider $1/1 \in S^{-1}I$.

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

(3)⇒(1):Consider $1/1 \in S^{-1}I$.

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

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

given by the following maps:

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

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

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

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

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

Definition 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 natrual way:

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

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

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

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

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

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

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

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

Remark 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 $f : N \to M$ be the embeding. Therefore $S{-}1N$ can be regarded as a submodule of $S^{-1}M$.

Remark 2.5.12. If P is a prime ideal of A, $S = A - P$,$f : M \to N$ 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 $S^{-1}f : S^{-1}M \to S^{-1}(M/N)$ given by the natrual homomorphism $f : M \to M/N$ is an surjective.In particular,$S^{-1}M/S^{-1}N \simeq S^{-1}(M/N)$ as $S^{-1}A$-module and A-mdoule.

Theorem 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 isomorphisc map is given by the bi-linear map:

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

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

and the universal property of tensor product.

Remark 2.5.15. 'natrually' in above theorem means: given two covariant functors:$S^{-1}A \otimes \_\_$ and $S^{-1}\_\_$, then the isomorphic map induced by φ induce a natrual transformation between these two functors.

Proposition 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:

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

Proposition 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 $f : M \to N$ be A-module homomorphism, $f_P : M_P \to N_P$ be homomorphism induced by prime ideal P. Then the following are equivalent:

(1) f is injective

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

(3) f_m is injective for maximal ideals m.

Proposition 2.5.19 (flat is a local property)**.** Let $f : M \to N$ be A-module homomorphism, $f_P : M_P \to N_P$ be homomorphism induced by prime ideal P. Then the following are equivalent:

(1) f is flat A-module.

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

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

Proposition 2.5.20. Let M be a finitely generated A-module, S a multiplicatively closed subset of A. Then $S^{-1}(\mathrm{Ann}(M) = \mathrm{Ann}(S^{-1}M)$.

Definition 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 $\mathrm{Supp}(M) = \{P \in \mathrm{Spec}(A) : M_P \neq 0\}$.

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

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

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

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

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

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

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

Proof:

(1):By Theorem 2.5.17

(2):By Proposition 2.5.13 and Proposition 2.5.7.

(3):By Theorem 2.5.10.

(4):Notice that $M_P \neq 0 \Leftrightarrow \mathrm{Ann}(M_P) \neq R$. 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 2.2.29, 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

$$M_k \otimes_k N_k = (M \otimes_R k) \otimes_k (k \otimes_R N)$$
$$\cong M \otimes_R (k \otimes_k k) \otimes_R N \cong (M \otimes_R N) \otimes_R k = (M \otimes_R N)_k$$

□

(6):trivial.

Proposition 2.5.24 (universal property of localization)**.** Let $g : A \to B$ be a ring homomorphism such that $g(s)$ is a unit in B for all $s \in S$. Then there exists a unique ring homomorphism $h : S^{-1}A \to B$ such that $g = h \circ f$.

Theorem 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

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

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

Proof: By theorem 2.5.13 and universal property of localization.

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

(1) $f = hg$

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

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

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

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

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

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

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

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

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

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

Corollary 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 $A_{\mathfrak{p}} \simeq B_{\mathrm{P}}$.

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:

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

2.6 Intergral Extension

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

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

where the a_4 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.

Proposition 2.6.3. Let $x_i (1 \leqslant i \leqslant n)$ be elements of B, each integral over A. Then the ring $A\left[x_1, \ldots, x_n\right]$ is a finitely-generated A-module.

Proposition 2.6.4. The set C of elements of B which are integral over A is a subring of B containing A.

Definition 2.6.5. The ring C containing all the integral elements in B is called the integral closure of A in B. If $C = A$, then A is said to be integrally closed in B. If $C = B$, the ring B is said to be integral over A.

Proposition 2.6.6. Let $A \subseteq B \subseteq C$ be rings. Suppose that A is Noetherian, that C is finitely generated as an A-algebra and that C is either finitely generated as a B-module or integral over B. Then B is finitely generated as an A-algebra.

2.7 Flatness

Theorem 2.7.1 (Base Change)**.** If $f : A \to B$ is a ring homomorphism and M is a flat A-module, then $M_B = B \otimes_A M$ is a flat B-module.

Proof: By Theorem 2.2.20.

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

Proof: By Theorem 2.5.14.

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

Proof: By Theorem 2.2.20.

Definition 2.7.4 (faithfully flat)**.**

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 $\dim Y \leqslant \dim X$.

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

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

Example 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 Notherian 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 :

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

Here also we have the inequality

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

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

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

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

Proof: By Proposition 2.3.8,

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

Theorem 2.8.6 (Ratliff, 1972)**.** A strictly increasing (or decreasing) chain $\mathfrak{p}_0, \mathfrak{p}_1, \ldots$ of prime ideals is said to be saturated if there do not exist prime ideals strictly contained between any two consecutive terms. We say that A is a catenary ring if the following condition is satisfied; for any prime ideals $\mathfrak{p}$ and $\mathfrak{p}'$ of A with $\mathfrak{p} \subset \mathfrak{p}'$, there exists a saturated chain of prime ideals starting from $\mathfrak{p}$ and ending at $\mathfrak{p}'$, and all such chains have the same (finite) length.

If a local domain $(A, \mathfrak{m})$ is catenary then for any prime ideal p we have $\operatorname{ht} \mathfrak{p} + \operatorname{coht} \mathfrak{p} = \dim A$. 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 $\alpha_1, \ldots, \alpha_n \in L$; then

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

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

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

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

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

Theorem 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 $E = k[x_1, \ldots, x_n]$. If E is not algebraic over k, by Proposition 1.2.49, we can renumber the x_1 so that $x_1, \ldots, x_r$ are algebraically independent over k, where $r \geqslant 1$, and each of $x_{r+1}, \ldots, x_n$ is algebraic over the field $F = k(x_1, \ldots, x_r)$. Hence E is a finite algebraic extension of F and therefore finitely generated as an F-module. Applying Proposition 2.6.6 to $k \subseteq F \subseteq E$, it follows that F is a finitely generated k-algebra, say $F = k[y_1, \ldots, y_3]$. Each y_j is of the form f_j/g_j, where f_j and g_j are polynomials in $x_1, \ldots, x_r$. It contradicts to the fact that there are infinitely many irreducible polynomials in the ring $k[x_1, \ldots, x_r]$ (adapt Euclid's proof of the existence of infinitely many prime numbers).

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

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

Theorem 2.8.10 (Hilbert's Nullstellensatz)**.** If k is algebracally closed, then

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

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

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

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

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

To prove this, introduce the ideal

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

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

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

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

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

$B \subset M$ means that:

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

and

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

But by our assumptionon g, (2.1) implies that $g(a_1,\ldots,a_n) = 0$.A contradiction! Hence we can only conclude that the ideal B would not have been a proper ideal.

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

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

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

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

Clearing denominators, this gives:

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

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

Theorem 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 2.3.19 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 $\operatorname{Frac}(A)/k$. For convenience, we denote it by $\deg_k A$.

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

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

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

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

By Proposition 1.2.49, we may assume that $\beta_1,\ldots,\beta_r$ is a transcendence basis for $k(\beta_1,\ldots,\beta_n)/k$. Then $\alpha_1,\ldots,\alpha_r$ are also algebraically independent over k, so that they form a transcendence basis for $k(\alpha_1,\ldots,\alpha_n)$ over k. Now set $S=k\left[X_1,\ldots,X_r\right]-\{0\};S$ is a multiplicative set in $k[X_1,\ldots,X_n]$ with $P\cap S=\varnothing$ and $Q\cap S=\varnothing$. Setting $R=k\left[X_1,\ldots,X_n\right]$ and $K=k\left(X_1,\ldots,X_r\right)$, we have $R_S\simeq K\left[X_{r+1},\ldots,X_n\right]$, and

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

so that R_S/PR_S is algebraic over $K=k\left(X_1,\ldots,X_r\right)\simeq k\left(\alpha_1,\ldots,\alpha_r\right)$, and therefore PR_S is a maximal ideal of R_S. Similarly, QR_S is a maximal ideal of R_S. This contradicts to Proposition 2.5.8.

Now let us prove that $r\leqslant\dim A$ 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 $A=k\left[\alpha_1,\ldots,\alpha_n\right]$ with α_1 transcendental over k; setting $S=k\left[X_1\right]-\{0\}$ and $R=k\left[X_1,\ldots,X_n\right]$ we get

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

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

2.9 Completion

Definition 2.9.1. Let A be a ring and M an A-module; for a directed set Λ, suppose that $\mathscr{F} = \{M_\lambda\}_{\lambda\in\Lambda}$ is a family of submodules of M indexed by Λ and such that $\lambda < \mu \Rightarrow M_\lambda \supset M_\mu$. Then $\mathscr{F}$ is a family of subgroups of M containing 0 and making M into a topological group under addition. In this topology, for any $x \in M$ a system of neighbourhoods of x is given by $\{x + M_\lambda\}_{\lambda\in\Lambda}$. In addition, when $M = A$, each M_λ is an ideal, then multiplication is also continuous:

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

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

Definition 2.9.2. Since for $\lambda < \mu$ there is a natural linear map $\varphi^\mu_\lambda : M/M_\mu \longrightarrow M/M_\lambda$, we can construct the inverse system $\{M/M_\lambda; \varphi_{\lambda\mu}\}$ of A-modules; its inverse limit $\varprojlim M/M_\lambda$ is called the completion of M, and is written $\hat{M}$. We give each M/M_λ the discrete topology, the direct product $\prod_\lambda M/M_\lambda$ the product topology, and $\hat{M}$ the subspace topology in $\prod_\lambda M/M_\lambda(\hat{M}$ is the set of the coherent sequences). Let $\psi : M \longrightarrow \hat{M}$ be the natural A-linear map;

Proposition 2.9.3. ψ is continuous, and $\psi(M)$ is dense in $\hat{M}$. If ψ is an isomorphism, we say A is complete.

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

Proposition 2.9.4. ψ is injective if and only if M is Hausdorff if and only if $\bigcap_\lambda M_\lambda = 0$.

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

Proof: Notice that

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

.

Lemma 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 Algerba

3.1 Basic Definition in Category

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

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

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

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

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

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

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

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

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

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

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

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

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

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 $\operatorname{Hom}_{\mathcal{C}^{\text{opp}}}(X, Y) := \operatorname{Hom}_{\mathcal{C}}(Y, X)$ with the obvious composition law.

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

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

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

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

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

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

Definition 3.1.5 (contravariant functor)**.** A contravariant functor from $\mathcal{C}$ to $\mathcal{D}$ is by definition a covariant functor $F : \mathcal{C}^{\text{opp}} \to \mathcal{D}$, where $\mathcal{C}^{\text{opp}}$ is the opposite category of $\mathcal{C}$. Sometimes we use the notation $F : \mathcal{C} \to \mathcal{D}$ for a contravariant functor, in which case we explicitly state that F is contravariant.

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

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

(1) Let $f : X \to Y$ 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 $f : A \to B$ in a category $\mathcal{C}$ is an isomorphism if there exists a morphism $g : B \to A$ in $\mathcal{C}$ with

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

The morphism g is called the inverse of f.

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

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

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

$$\begin{tikzcd}
SA \arrow[r, "\tau_A"] \arrow[d, "Sf"'] & TA \arrow[d, "Tf"] \\
SA' \arrow[r, "\tau_{A'}"'] & TA'
\end{tikzcd}$$

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

Proposition 3.1.10. Given functors $F, G, H : \mathcal{C} \to \mathcal{D}$ and natural transformations $\alpha : F \to G$ and $\beta : G \to H$, we have the (vertically) composite natural transformation $\beta\alpha : F \to H$. Functors $\mathcal{C} \to \mathcal{D}$ and natural transformations form a category Fun $(\mathcal{C}, \mathcal{D})$. Isomorphisms in this category are called natural isomorphisms. A natural transformation α is a natural isomorphism if and only if α_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 $F : \mathcal{C} \to \mathcal{D}$ such that there exist a functor $G : \mathcal{D} \to \mathcal{C}$ and natural isomorphisms $\mathrm{id}_{\mathcal{C}} \simeq GF$ and $FG \simeq \mathrm{id}_{\mathcal{D}}$ The functors F and G are then called quasi-inverses of each other.

Definition 3.1.12 (essentially surjective)**.** A functor $F : \mathcal{C} \to \mathcal{D}$ 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 $F : \mathcal{C} \to \mathcal{D}$ 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 $A \to X$. Any two initial objects in a category $\mathcal{C}$, should they exist, are isomorphic.

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

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

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

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

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

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

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

Example 3.1.19 (coproduct in category of topological space)**.** $(X_i)_{i\in I}$ be a family of topological space, $f_i : X_i \to X$ be a family of continuous map. $\bigsqcup_{i\in I} A_i = \big\{(a_i,i) \in \big(\bigcup_{i\in I} A_i\big) \times I : a_i \in A_i\big\}$ be the disjoint union of $(X_i)_{\in I}$. Define U open in $\bigsqcup_{i\in I} A_i$ if and only if $f_i^{-1}(U)$ open in X_i for all $i \in I$. Then $\bigsqcup_{i\in I} A_i$ with continous maps $\alpha_i : a_i \mapsto (a_i,i)$ is the coproduct of a family of topological space.

Example 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

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

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

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

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

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

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

Definition 3.1.24 (pushout/fibered coproduct)**.** Given two morphisms $f : A \to B$ and $g : A \to C$ in a category $\mathcal{C}$, a pushout (or fibered sum) is a triple (D, α, β) with $\beta g = \alpha f$ that is a solution to the universal mapping problem: for every triple (Y, α', β') with $\beta' g = \alpha' g$, there exists a unique morphism $\theta : D \to Y$ making the diagram commute. The pushout is often denoted by $B \cup_A C$.

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

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

Example 3.1.25. In category of Commutative Rings, $f : A \to B, g : A \to B$ be ring homomorphism, then the pushout is given by tensor product of A-algebra B and A-algebra C and homorphism:

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

Definition 3.1.26 (inverse system)**.** Given a partially ordered set I and a category $\mathcal{C}$, an inverse system in $\mathcal{C}$ is an ordered pair $\left((M_i)_{i\in I}, \left(\psi_i^j\right)_{j\succeq i}\right)$, abbreviated $\left\{M_i, \psi_i^j\right\}$, where $(M_i)_{i\in I}$ is an indexed family of objects in $\mathcal{C}$ and $\left(\psi_i^j : M_j \to M_i\right)_{j\succeq i}$ is an indexed family of morphisms for which $\psi_i^i = 1_{M_i}$ for all i, and such that the following diagram commutes whenever $k \succeq j \succeq i$.

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

Definition 3.1.27 (inverse limit)**.** Let I be a partially ordered set, let $\mathcal{C}$ be a category, and let $\{M_i, \psi_i^j\}$ be an inverse system in $\mathcal{C}$ over I. The inverse limit (also called projective limit or limit) is an object $\varprojlim M_i$ and a family of projections $\left(\alpha_i : \varprojlim M_i \to M_i\right)_{i \in I}$ such that:

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

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

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

Example 3.1.28. In the category of topological group, inverse limit exists. Inverse limit of Finite discrete group is called pro-finite group. A topological group is pro-finite group if and only if it is totally disconnected and compact.

Definition 3.1.29 (direct system)**.** Given a partially ordered set I and a category $\mathcal{C}$, a direct system in $\mathcal{C}$ is an ordered pair $\left((M_i)_{i\in I}, (\varphi_j^i)_{i \preceq j}\right)$, abbreviated $\{M_i, \varphi_j^i\}$, where $(M_i)_{i \in I}$ is an indexed family of objects in $\mathcal{C}$ and $\left(\varphi_j^i : M_j \to M_i\right)_{i \preceq j}$ is an indexed family of morphisms for which $\varphi_i^i = 1_{M_i}$ for all i, and such that the following diagram commutes whenever $i \preceq j \preceq k$.

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

Definition 3.1.30 (direct limit)**.** Let I be a partially ordered set, let $\mathcal{C}$ be a category, and let $\{M_i, \varphi_j^i\}$ be a direct system in $\mathcal{C}$ over I. The direct limit (also called inductive limit or colimit) is an object $\varinjlim M_i$ and insertion morphisms $\left(\alpha_i : M_i \to \varinjlim M_i\right)_{i \in I}$.

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

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

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

Example 3.1.31. M is a smooth manifold, $p \in M$, $C_p^\infty(M)$ be the germ of smooth function at p, then $C_p^\infty(M)$ is the direct limit of the direct system $\left\{(C^\infty(U))_{p\in U \text{ open in } M}, (\mathrm{res}_V^U)_{V\subset U}\right\}$ where res be the restriction map from the bigger open subset to the smaller one.

Definition 3.1.32. Recall that a direct system $\left\{A_i, \alpha_j^i\right\}$ in a category $\mathcal{C}$ over a partially ordered index set I can be construed as a covariant functor $A : I \to \mathcal{C}$, where $A(i) = A_i$ and $A\left(\kappa_j^i\right) = \alpha_j^i$.

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

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

Proposition 3.1.33. Let I be a directed set, and let $\left\{A_i, \alpha_j^i\right\}, \left\{B_i, \beta_j^i\right\}$, and $\left\{C_i, \gamma_j^i\right\}$ be direct systems of left R-modules over I. If : $\left\{A_i, \alpha_j^i\right\} \to \left\{B_i, \beta_j^i\right\}$ and $s : \left\{B_i, \beta_j^i\right\} \to \left\{C_i, \gamma_j^i\right\}$ are morphisms of direct systems, and if

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

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

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

Definition 3.1.34. A inverse system can by viewed as a functor from opposite category of partially ordered set to category $\mathcal{C}$. A morphism between inverse system is a natrual transformation between inverse system.

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

Proposition 3.1.35. In ${}_R\mathrm{Mod}$, let $r : \left\{A_i, \alpha_j^i\right\} \to \left\{B_i, \beta_j^i\right\}$ and $s : \left\{B_i, \beta_j^i\right\} \to \left\{C_i, \gamma_j^i\right\}$ be morphisms of inverse systems over any (not necessarily directed) index set I. If

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

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

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

Definition 3.1.36. A covariant functor $F : \mathcal{A} \to \mathcal{C}$ preserves direct limits if, whenever $\left(\varinjlim A_i, \left(\alpha_i : A_i \to \varinjlim A_i\right)\right)$ is a direct limit of a direct system $\left\{A_i, \varphi_j^i\right\}$ in $\mathcal{A}$, then $\left(F\left(\varinjlim A_i\right), \left(F\alpha_i : FA_i \to F\left(\varinjlim A_i\right)\right)\right)$ is a direct limit of the direct system $\left\{FA_i, F\varphi_j^i\right\}$ in $\mathcal{C}$.

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

Definition 3.1.37. Let $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{D} \to \mathcal{C}$ be covariant functors. The ordered pair (F, G) is an adjoint pair if, for each $C \in \mathrm{obj}(\mathcal{C})$ and $D \in \mathrm{obj}(\mathcal{D})$, there are bijections

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

such that the following diagram commute:

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

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

Example 3.1.38 (Hom and Tensor)**.** If $B = {}_RB_S$ is a bimodule, $\square \otimes_R B : \mathrm{Mod}_R \to \mathrm{Mod}_S$ and $\mathrm{Hom}_S(B, \square) : \mathrm{Mod}_S \to \mathrm{Mod}_R$ be two functors. then $(\square \otimes_R B, \mathrm{Hom}_S(B, \square))$ is an adjoint pair. Similarly, if $B = {}_SB_R$ is a bimodule, $B \otimes_R \square :_R \mathrm{Mod} \to_S \mathrm{Mod}$ and $\mathrm{Hom}_S(B, \square) :_S \mathrm{Mod} \to_R \mathrm{Mod}$ be two functors. then $(B \otimes_R \square, \mathrm{Hom}_S(B, \square))$ is an adjoint pair.

Example 3.1.39 (Free and Forget)**.**

Example 3.1.40 (Induced Representation)**.** G is a finite group, H be a subgroup of G, then $\mathbb{C}[G]$ be a $(\mathbb{C}[G], \mathbb{C}[H])$ bi-module, funcotr $\mathbb{C}[G] \otimes_{\mathbb{C}[H]} \square :_{\mathbb{C}[H]} \mathrm{Mod} \to_{\mathbb{C}[G]} \mathrm{Mod}$ and funcotr $\mathrm{Hom}_{\mathbb{C}[G]}(\mathbb{C}[G], \square)$ be an adjoint pair, since $\mathrm{Hom}_{\mathbb{C}[G]}(\mathbb{C}[G], \square) \simeq \mathrm{Res}^{\mathbb{C}[G]}_{\mathbb{C}[H]}$(Restriction from $\mathbb{C}[G]$-module to $\mathbb{C}[H]$-module), we have $(\mathbb{C}[G] \otimes_{\mathbb{C}[H]} \square, \mathrm{Res}^{\mathbb{C}[G]}_{\mathbb{C}[H]})$ is an adjoint pair.

Proposition 3.1.41. *Let (F, G) be an adjoint pair offunctors, where $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{D} \to \mathcal{C}$. Then F preserves direct limits and G preserves inverse limits.*

3.2 Abelian Category

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

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

(2) composition map

$$\operatorname{Hom}(A,B) \times \operatorname{Hom}(B,C) \to \operatorname{Hom}(A,C)$$

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

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

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

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

Proposition 3.2.3. If $\mathcal{C}$ and $\mathcal{D}$ are additive categories and $T : \mathcal{C} \to \mathcal{D}$ is an additive functor of either variance, then $T(A \oplus B) \cong T(A) \oplus T(B)$ for all $A,B \in \operatorname{obj}(\mathcal{C})$.

Definition 3.2.4. A morphism $u : B \to C$ in a category $\mathcal{C}$ is a monomorphism (or is monic) if u can be canceled from the left; that is, for all objects A and all morphisms $f,g : A \to B$, we have that $uf = ug$ implies $f = g$.

$$A \overset{f}{\underset{g}{\rightrightarrows}} B \xrightarrow{u} C$$

Definition 3.2.5. A morphism $v : B \to C$ in a category $\mathcal{C}$ is an epimorphism (or is epic) if v can be canceled from the right; that is, for all objects D and all morphisms $h,k : C \to D$, we have that $hv = kv$ implies $h = k$.

$$B \xrightarrow{v} C \overset{h}{\underset{k}{\rightrightarrows}} D$$

Definition 3.2.6 (kernel,cokernel)**.** If $u : A \to B$ is a morphism in an additive category $\mathcal{A}$, then its kernel $\ker u$ is a morphism $i : K \to A$ that satisfies the following universal mapping property: $u \circ l = 0$ and, for every $g : X \to A$ with $ug = 0$, there exists a unique $\theta : X \to K$ with $i\theta = g$.

$$\begin{tikzcd}
X \arrow[d, dashed, "\theta"] \arrow[dr, "g"] \arrow[drr, "0"] & & \\
K \arrow[r, "l"] & A \arrow[r, "u"] & B
\end{tikzcd}$$

$$\begin{tikzcd}
A \arrow[r, "u"] \arrow[drr, "0"'] & B \arrow[r, "\pi"] \arrow[dr, "h"'] & C \arrow[d, dashed, "\theta"'] \\
 & & Y
\end{tikzcd}$$

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

Proposition 3.2.7. Let $u : A \to B$ be a morphism in an additive category $\mathcal{A}$.

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

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

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

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

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

Proposition 3.2.8. Every kernel is monomorphism, every cokernel is epimorphism.

Definition 3.2.9. Let $\mathcal{A}$ be an additive category admitting kernels and cokernels and let $f : A \to B$ 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 $g : \ker(f) \to A$ and $h : B \to \operatorname{coker}(f)$ are the canonical morphisms.

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

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

as the following diagram

$$\begin{tikzcd}
\mathrm{Ker} f \arrow[r, "g"] & A \arrow[r, "f"] \arrow[d] & B \arrow[r, "h"] & \mathrm{coker} f \\
 & \mathrm{coker} g \arrow[r, "\tilde{f}"] & \mathrm{Ker} h \arrow[u] &
\end{tikzcd}$$

Definition 3.2.10. 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 $f : A \to B$, the morphism $\operatorname{coim}(f) \to \operatorname{im}(f)$ is an isomorphism.(AB2)

Proposition 3.2.11. 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 $f : A \to B$ can be decomposed into

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

where g is an epimorphism and h is a monomorphism.

Definition 3.2.12. 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 $\mathrm{im}(f) \to \ker(g)$ is an isomorphism. We say that a sequence $A^0 \to A^1 \to \cdots \to A^n$ is exact if it is exact at each $A^i, 1 \leq i \leq n-1$.

$$\begin{tikzcd}
A \arrow[rr, "f"] \arrow[dr] & & B \arrow[rr, "g"] & & C \\
& \mathrm{im} f \arrow[ur] \arrow[rr, dashed, "\theta"] & & \mathrm{Ker} g \arrow[ul] &
\end{tikzcd}$$

Definition 3.2.13. Let $\mathcal{C}$ and $\mathcal{D}$ be abelian categories. An additive functor $F : \mathcal{C} \to \mathcal{D}$ is left exact (resp. right exact) if for any exact sequence $0 \to X' \to X \to X''$ (resp. $X' \to X \to X'' \to 0$) the sequence $0 \to F(X') \to F(X) \to F(X'')$ (resp. $F(X') \to F(X) \to F(X'') \to 0$) is exact. The functor F is exact if it is right exact and left exact. A functor F is exact if and only if for all exact sequences $X \xrightarrow{u} Y \xrightarrow{v} Z$ the sequence

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

is exact.

Proposition 3.2.14. Let $F : \mathcal{A} \to \mathcal{B}$ be an additive functor between abelian categories. Then the following conditions are equivalent: (1) F is left exact. (2) For every short exact sequence $0 \to X \to Y \to Z \to 0$ in $\mathcal{A}, 0 \to FX \to FY \to FZ$ is an exact sequence in $\mathcal{B}$.

Proposition 3.2.15. Let $F : \mathcal{A} \to \mathcal{B}$ be an additive functor between abelian categories. Then the following conditions are equivalent:

(1) F is exact.

(2) For every short exact sequence $0 \to X \to Y \to Z \to 0$ in $\mathcal{A}, 0 \to FX \to FY \to FZ \to 0$ 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 3.2.16. An object P in an abelian category $\mathcal{A}$ is projective if, for every epic $g : B \to C$ and every $f : P \to C$, there exists $h : P \to B$ with $f = gh$.

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

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

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 $\mathcal{A}, d_X^n : X^n \to X^{n+1}$ 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 $X \to Y$ is a collection of morphisms $(f^n)_{n\in\mathbb{Z}}$ of morphisms $f^n : X^n \to Y^n$ 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

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

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

$$\begin{tikzcd}
 & \mathrm{im} d^{n-1} \arrow[rr, hook] \arrow[dr, hook] & & \mathrm{Ker} d^n \arrow[dl, hook] & \\
X^{n-1} \arrow[ur, two heads] \arrow[rr, "d^{n-1}"] & & X^n \arrow[rr, "d^n"] & & X^{n+1}
\end{tikzcd}$$

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

$$\begin{tikzcd}
 & \mathrm{im} d^{n-1} \arrow[rr] \arrow[dr] \arrow[ddd] & & \mathrm{Ker} d^n \arrow[rr] \arrow[dl] \arrow[ddd] & & H^n(X) \arrow[ddd, "H^n(f)"] \\
X^{n-1} \arrow[ur] \arrow[rr, "d^{n-1}"] \arrow[d, "f^{n-1}"'] & & X^n \arrow[rr, "d^n"] \arrow[d, "f^n"'] & & X^{n+1} \arrow[d, "f^{n+1}"] & \\
Y^{n-1} \arrow[rr, "e^{n-1}"'] \arrow[dr] & & Y^n \arrow[rr, "e^n"'] & & Y^{n+1} & \\
 & \mathrm{im} e^{n-1} \arrow[rr] \arrow[ur] & & \mathrm{Ker} e^n \arrow[rr] \arrow[ul] & & H^n(Y)
\end{tikzcd}$$

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

Theorem 3.3.5 (long exact sequence cohomology)**.** Let $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ be a short exact sequence of complexes. Then we have a long exact sequence

$$\begin{tikzcd}
H^n(A) \arrow[r, "H^n(f)"] & H^n(B) \arrow[r, "H^n(g)"] & H^n(C) \arrow[dll, "\delta_n"] \\
H^{n+1}(A) \arrow[r, "H^{n+1}(f)"] & H^{n+1}(B) \arrow[r, "H^{n+1}(g)"] & H^{n+1}(C) \arrow[dll, "\delta_{n+1}"] \\
H^{n+2}(A) & &
\end{tikzcd}$$

where δ_n are called connecting morphisms.

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

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] \arrow[d] & B \arrow[r] \arrow[d] & C \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & A' \arrow[r] & B' \arrow[r] & C' \arrow[r] & 0
\end{tikzcd}$$

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

$$\begin{tikzcd}
H^n(A) \arrow[r, "H^n(f)"] \arrow[d] & H^n(B) \arrow[r, "H^n(g)"] \arrow[d] & H^n(C) \arrow[r, "\delta_n"] \arrow[d] & H^{n+1}(A) \arrow[r, "H^{n+1}(f)"] \arrow[d] & H^{n+1}(B) \arrow[r, "H^{n+1}(g)"] \arrow[d] & H^{n+1}(C) \arrow[d] \\
H^n(A') \arrow[r] & H^n(B') \arrow[r] & H^n(C') \arrow[r, "\delta'_n"'] & H^{n+1}(A') \arrow[r] & H^{n+1}(B') \arrow[r] & H^{n+1}(C')
\end{tikzcd}$$

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

$$\cdots \to P^{-n} \to \cdots \to P^0 \to X \to 0$$

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

$$0 \to X \to I^0 \to \cdots \to I^n \to \cdots$$

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

Proposition 3.3.8. Consider the following diagram:

$$\begin{tikzcd}
0 \arrow[r] & X \arrow[r, "u"] & I^0 \arrow[rr] \arrow[dr] & & I^1 \\
 & & & \operatorname{coker}(u) \arrow[ur] &
\end{tikzcd}$$

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

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

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

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

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

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

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

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

Proposition 3.3.10. If $f,g:X\to Y$ are homotopic, then $H^nf=H^ng:H^nX\to H^nY$.

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

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

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

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] \arrow[d, "f"] & I^0 \arrow[r] \arrow[d, "f_0"] & I^1 \arrow[r] \arrow[d, "f_1"] & \ldots \\
0 \arrow[r] & B \arrow[r] & J^0 \arrow[r] & J^1 \arrow[r] & \ldots
\end{tikzcd}$$

and f_i is unique up to homotopy.

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

$$I:\quad 0\longrightarrow A\longrightarrow I^0\longrightarrow I^1\longrightarrow\cdots$$

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

$$TI:\quad 0\longrightarrow T\left(I^0\right)\longrightarrow T\left(I^1\right)\longrightarrow\cdots\longrightarrow T\left(I^n\right)\longrightarrow\cdots$$

We define $R^nT(A)=H^n(TI)$ 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^0T 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 $T : \mathcal{A} \longrightarrow \mathcal{B}$ be an additive functor. Suppose we have an exact sequence

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

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

$$\begin{aligned} 0 \longrightarrow R^0T\left(A'\right) \longrightarrow R^0T(A) \longrightarrow R^0T\left(A''\right) \xrightarrow{\omega^0} R^1T\left(A'\right) \longrightarrow \cdots \\ \cdots \longrightarrow R^nT\left(A''\right) \xrightarrow{\omega^n} R^{n+1}T\left(A'\right) \longrightarrow R^{n+1}T(A) \longrightarrow R^{n+1}T\left(A''\right) \longrightarrow \cdots \end{aligned}$$

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, $\operatorname{Hom}(\square, D)$ is a left exact functor. Denote the n-th right derived funcotr of $\operatorname{Hom}(\square, D)$ by $\operatorname{Ext}_R^n(\square, D)$

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

Proposition 3.4.3.

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

Hence we won't use the notation 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) $\operatorname{Ext}_R^1(A, Q) = 0$ for all R-modules A, and

(3) $\operatorname{Ext}_R^n(A, Q) = 0$ 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) $\operatorname{Ext}_R^1(P, B) = 0$ for all R-modules B, and

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

Proposition 3.4.6. Show that $\operatorname{Ext}_R^n\left(A_1 \oplus A_2, B\right) \cong \operatorname{Ext}_R^n\left(A_1, B\right) \oplus \operatorname{Ext}_R^n\left(A_2, B\right)$ 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 $\mathrm{Ext}^0_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, D) \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, D)$, and it follows that $\mathrm{Ext}^0_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, D) \cong mD$, 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

$$0 \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, D) \xrightarrow{m} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, D) \longrightarrow 0 \longrightarrow \cdots .$$

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

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

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

$$0 \longrightarrow \mathrm{Hom}(A, \mathbb{Z}) \longrightarrow \mathrm{Hom}(A, \mathbb{Q}) \longrightarrow \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z}) \longrightarrow 0 \longrightarrow \cdots$$

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

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

The group 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, $\mathrm{Ext}^1(A, \mathbb{Z}) \cong A$ is nonzero for all nonzero finite abelian groups A.

Example 3.4.9.

3.5 Group Cohomology

Chapter 4

Theory of Scheme

4.1 Sheaf Theory

Definition 4.1.1 (presheaf)**.** Let (Ouv_X) be the category whose objects are the open sets of X and, for two open sets $U, V \subseteq X, \operatorname{Hom}(U, V)$ is empty if $U \nsubseteq V$, and consists of the inclusion map $U \rightarrow V$ if $U \subseteq V$ (composition of morphisms being the composition of the inclusion maps). A presheaf is a contravariant functor $\mathscr{F}$ from the category (Ouv_X) to the category of category $\mathcal{C}$(such as the category of abelian groups, the category of rings, the category of R-modules, or the category of R-algebras)

Definition 4.1.2. Let $\mathscr{F}$ be a presheaf on a topological space X, let U be an open set in X and let $\mathscr{U}=(U_i)_{i \in I}$ be an open covering of U. We define maps (depending on $\mathscr{U}$)

$$\begin{aligned}
\rho: \mathscr{F}(U) \rightarrow \prod_{i \in I} \mathscr{F}\left(U_i\right), \quad & s \mapsto \left(s_{\mid U_i}\right)_i \\
\sigma: \prod_{i \in I} \mathscr{F}\left(U_i\right) \rightarrow \prod_{(i, j) \in I \times I} \mathscr{F}\left(U_i \cap U_j\right), \quad & \left(s_i\right)_i \mapsto \left(s_{i \mid U_i \cap U_j}\right)_{(i, j)}, \\
\sigma^{\prime}: \prod_{i \in I} \mathscr{F}\left(U_i\right) \rightarrow \prod_{(i, j) \in I \times I} \mathscr{F}\left(U_i \cap U_j\right), \quad & \left(s_i\right)_i \mapsto \left(s_{j \mid U_i \cap U_j}\right)_{(i, j)}.
\end{aligned}$$

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

$$\begin{tikzcd}
\mathscr{F}(U) \arrow[r, "\rho"] & \prod_{i \in I} \mathscr{F}\left(U_i\right) \arrow[r, shift left, "\sigma"] \arrow[r, shift right, "\sigma'"'] & \prod_{(i, j) \in I \times I} \mathscr{F}\left(U_i \cap U_j\right)
\end{tikzcd}$$

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

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

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

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

Definition 4.1.3 (restriction of sheaf)**.** If $\mathscr{F}$ is a presheaf on a topological space X and U is an open subspace of X, we obtain a presheaf $\mathscr{F}\mid_U$ on U by setting $\mathscr{F}\mid_U (V) = \mathscr{F}(V)$ for every open subset V in U. If $\mathscr{F}$ is a sheaf, $\mathscr{F}\mid_U$ is a sheaf on U. We call $\mathscr{F}\mid_U$ the restriction of $\mathscr{F}$ to U.

Definition 4.1.4. The inductive limit

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

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

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

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

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

of the stalks in x by Proposition 3.1.32. We obtain a functor $\mathscr{F} \mapsto \mathscr{F}_x$ from the category of presheaves on X to the category of sets.

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

Proposition 4.1.5. Let X be a topological space, $\mathscr{F}$ and $\mathscr{G}$ presheaves on X, and let $\varphi, \psi : \mathscr{F} \to \mathscr{G}$ be two morphisms of presheaves.

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

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

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

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

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

We claim that this map is injective if $\mathscr{F}$ is a sheaf. Indeed let $s, t \in \mathscr{F}(U)$ such that $s_x = t_x$ for all $x \in U$. Then for all $x \in U$ there exists an open neighborhood $V_x \subseteq U$ of x such that

$s_{|V_x} = t_{|V_x}$. Clearly, $U = \bigcup_{x\in U} V_x$ and therefore $s = t$ by sheaf condition (Sh1). Using the commutative diagram

$$\begin{tikzcd}
\mathscr{F}(U) \arrow[r] \arrow[d, "\varphi_U"] & \prod \mathscr{F}_x \arrow[d, "\prod \varphi_x"] \\
\mathscr{G}(U) \arrow[r] & \prod \mathscr{G}_x
\end{tikzcd}$$

and Proposition 3.1.33, (1) and (3) hold.

(2): By proposition 3.1.33, it suffice to show the bijectivity of φ_x for all $x \in U$ implies the surjectivity of φ_U. Let $t \in \mathscr{G}(U)$. For all $x \in U$ we choose an open neighborhood U^x of x in U and $s^x \in \mathscr{F}\left(U^x\right)$ such that $\left(\varphi_{U^x}\left(s^x\right)\right)_x = t_x$. Then there exists an open neighborhood $V^x \subseteq U^x$ of x with $\varphi_{V^x}\left(s^x{}_{|V^x}\right) = t_{|V^x}$. Then $\left(V^x\right)_{x\in U}$ is an open covering of U and for $x, y \in U$

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

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

Definition 4.1.6. A morphism $\varphi : \mathscr{F} \to \mathscr{G}$ of sheaves injective (resp. surjective, resp. bijective) if $\varphi_x : \mathscr{F}_x \to \mathscr{G}_x$ is injective (resp. surjective, resp. bijective) for all $x \in X$.

Remark 4.1.7. If $\varphi : \mathscr{F} \to \mathscr{G}$ is a morphism of sheaves, φ is surjective if and only if for all open subsets $U \subseteq X$ and every $t \in \mathscr{G}(U)$ there exist an open covering $U = \bigcup_i U_i$ (depending on t) and sections $s_i \in \mathscr{F}\left(U_i\right)$ such that $\varphi_{U_i}\left(s_i\right) = t_{|U_i}$, i.e., locally we can find a preimage of t. But the surjectivity of φ does not imply that $\varphi_U : \mathscr{F}(U) \to \mathscr{G}(U)$ is surjective for all open sets U of X

Definition 4.1.8. If $\mathscr{F}, \mathscr{G}$ are (pre-)sheaves on X such that $\mathscr{F}(U) \subseteq \mathscr{G}(U)$ for all $U \subseteq X$ open, and such that the following diagram commute

$$\begin{tikzcd}
\mathscr{F}(U) \arrow[r, "\subset"] & \mathscr{G}(U) \\
\mathscr{F}(V) \arrow[r, "\subset"'] \arrow[u, "\mathrm{res}_U^V"] & \mathscr{G}(V) \arrow[u, "\mathrm{res}_U^V"']
\end{tikzcd}$$

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

Definition 4.1.9 (sheafification)**.** Let $\mathscr{F}$ be a presheaf on a topological space X. Then there exists a pair $\left(\tilde{\mathscr{F}}, \iota_{\mathscr{F}}\right)$, where $\tilde{\mathscr{F}}$ is a sheaf on X and $\iota_{\mathscr{F}} : \mathscr{F} \to \tilde{\mathscr{F}}$ is a morphism of presheaves, such that the following holds: If $\mathscr{G}$ is a sheaf on X and $\varphi : \mathscr{F} \to \mathscr{G}$ is a morphism of presheaves, then there exists a unique morphism of sheaves $\tilde{\varphi} : \tilde{\mathscr{F}} \to \mathscr{G}$ with $\tilde{\varphi} \circ \iota_{\mathscr{F}} = \varphi$. And the following properties hold:

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

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

$$\begin{tikzcd}
\mathscr{F} \arrow[r, "\iota_{\mathscr{F}}"] \arrow[d, "\varphi"'] & \tilde{\mathscr{F}} \arrow[d, "\tilde{\varphi}"] \\
\mathscr{G} \arrow[r, "\iota_{\mathscr{G}}"'] & \tilde{\mathscr{G}}
\end{tikzcd}$$

commutative.

(3) φ is injective(surjective, bijective) if and only if $\tilde{\varphi}$ is injective(surjective, bijective).

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

Proof: For $U \subseteq X$ open, elements of $\tilde{\mathscr{F}}(U)$ are by definition families of elements in the stalks of $\mathscr{F}$ which locally give rise to sections of $\mathscr{F}$. More precisely, we define

$$\tilde{\mathscr{F}}(U) := \Bigg\{ (s_x) \in \prod_{x \in U} \mathscr{F}_x : \forall x \in U, \exists \text{ an open neighborhood } W \subseteq U \text{ of } x, \\ \text{and } \ t \in \mathscr{F}(W) \text{ s.t. } \forall w \in W : s_w = t_w \Big\} .$$

For $U \subseteq V$ the restriction map $\tilde{\mathscr{F}}(V) \to \tilde{\mathscr{F}}(U)$ is induced by the natural projection $\prod_{x \in V} \mathscr{F}_x \to \prod_{x \in U} \mathscr{F}_x$. Then it is easy to check that $\tilde{\mathscr{F}}$ is a sheaf.

For $U \subseteq X$ open, we define $\iota_{\mathscr{F},U} : \mathscr{F}(U) \to \tilde{\mathscr{F}}(U)$ by $s \mapsto (s_x)_{x \in U}$. The definition of $\tilde{\mathscr{F}}$ shows that $\iota_{\mathscr{F},x} : \mathscr{F}_x \to \tilde{\mathscr{F}}_x$ is bijective.

Now let $\mathscr{G}$ be a presheaf on X and let $\varphi : \mathscr{F} \to \mathscr{G}$ be a morphism. Sending $(s_x)_x \in \tilde{\mathscr{F}}(U)$ to $(\varphi_x(s_x))_x \in \tilde{\mathscr{G}}(U)$ defines a morphism $\tilde{\mathscr{F}} \to \tilde{\mathscr{G}}$. By Proposition 4.1.5, this is the unique morphism making the diagram commutative.

If we assume in addition that $\mathscr{G}$ is a sheaf, then the morphism of sheaves $\iota_{\mathscr{G}} : \mathscr{G} \to \tilde{\mathscr{G}}$, which is bijective on stalks, is an isomorphism by Proposition 4.1.5(3). Composing the morphism $\tilde{\mathscr{F}} \to \tilde{\mathscr{G}}$ with $\iota_{\mathscr{G}}^{-1}$, we obtain the morphism $\tilde{\varphi} : \tilde{\mathscr{F}} \to \mathscr{G}$. Finally, the uniqueness of $\left(\tilde{\mathscr{F}}, \iota_{\mathscr{F}}\right)$ is a formal consequence.

Definition 4.1.10 (direct image)**.** Let $f : X \to Y$ be a continuous map of topological spaces. Let $\mathscr{F}$ be a presheaf on X. We define a presheaf $f_*\mathscr{F}$ on Y by

$$(f_*\mathscr{F})(V) = \mathscr{F}\left(f^{-1}(V)\right)$$

the restriction maps given by the restriction maps for $\mathscr{F}$. We call $f_*\mathscr{F}$ the direct image of $\mathscr{F}$ under f. Whenever $\varphi : \mathscr{F}_1 \to \mathscr{F}_2$ is a morphism of presheaves, the family of maps $f_*(\varphi)_V := \varphi_{f^{-1}(V)}$ for $V \subseteq Y$ open is a morphism $f_*(\varphi) : f_*\mathscr{F}_1 \to f_*\mathscr{F}_2$. Therefore f_* is a functor from the category of presheaves on X to the category of presheaves on Y.

Proposition 4.1.11. (1) If $\mathscr{F}$ is a sheaf on X, $f_*\mathscr{F}$ is a sheaf on Y. Therefore f_* also defines a functor $f_* : (\mathrm{Sh}(X)) \to (\mathrm{Sh}(Y))$.

(2) If $g : Y \to Z$ is a second continuous map, there exists an identity $g_*\left(f_*\mathscr{F}\right) = (g \circ f)_*\mathscr{F}$ which is functorial in $\mathscr{F}$.

Definition 4.1.12 (inverse image)**.** Let $f : X \to Y$ be a continuous map and let $\mathscr{G}$ be a presheaf on Y. Define a presheaf on X by

$$U \mapsto \varinjlim_{V \supseteq f(U)} \mathscr{G}(V),$$

the restriction maps being induced by the restriction maps of $\mathscr{G}$ and the universal property of direct limit:

$$\begin{tikzcd}
\varinjlim_{V \supseteq f(U)} \mathscr{G}(V) \arrow[rr, dashed, "\mathrm{res}_W^U"'] & & \varinjlim_{V \supseteq f(W)} \mathscr{G}(V) \\
& \mathscr{G}(V_1) \arrow[ul] \arrow[ur] \arrow[d] & \\
& \mathscr{G}(V_2) \arrow[uul] \arrow[uur] &
\end{tikzcd}$$

We denote this presheaf by $f^+\mathscr{G}$. Let $f^{-1}\mathscr{G}$ be the sheafification of $f^+\mathscr{G}$. We call $f^{-1}\mathscr{G}$ the inverse image of $\mathscr{G}$ under f.

Proposition 4.1.13. If X is an open subspace of Y, and $f : X \to Y$ is the inclusion map, $\mathscr{G}$ is a sheaf on Y, then $f^{-1}\mathscr{G} \simeq \mathscr{G}|_X$.

Proposition 4.1.14. f^{-1} is a functor from categroy of presheaf on Y to categroy of sheaf on X.

Proof: If $\varphi : \mathscr{G}_1 \to \mathscr{G}_2$ is a morphism of presheaf on Y, then $f^{-1}\varphi : f^{-1}\mathscr{G}_1 \to f^{-1}\mathscr{G}_1$ is induced by universal property of direct limit and Proposition 4.1.9.

Proposition 4.1.15 (stalks of direct image)**.** Notice that

$$\left(f^{-1}\mathscr{G}\right)_x \cong \left(f^+\mathscr{G}\right)_x = \varinjlim_{x \in U} \left(f^+\mathscr{G}\right)(U)$$

Since f is continous,

$$\varinjlim_{x \in U} \varinjlim_{f(U) \subset V} \mathscr{G}(V) \cong \varinjlim_{f(x) \in V} \mathscr{G}(V)$$

Proposition 4.1.16. Now let $g : Y \to Z$ be a second continuous map and let $\mathscr{H}$ be a presheaf on Z. Fix an open subset U in X. An open subset $W \subseteq Z$ contains $g(f(U))$ if and only if it contains a subset of the form $g(V)$, where $V \subseteq Y$ is an open set containing $f(U)$.This implies that $f^+\left(g^+\mathscr{H}\right) \cong (g \circ f)^+\mathscr{H}$. Furthermore, Proposition 4.1.9 and Proposition 4.1.15 implies that the natural morphism $f^{-1}\left(g^+\mathscr{H}\right) \to f^{-1}\left(g^{-1}\mathscr{H}\right)$ induces isomorphisms on all stalks. Hence

$$f^{-1}\left(g^{-1}\mathscr{H}\right) \cong (g \circ f)^{-1}\mathscr{H},$$

Theorem 4.1.17 (adjoint pair (f^{-1}, f_*)). Let $f : X \to Y$ be a continuous map, let $\mathscr{F}$ be a sheaf on X and let $\mathscr{G}$ be a presheaf on Y. Then there is a bijection

$$\begin{gathered}\operatorname{Hom}_{(\operatorname{Sh}(X))}\left(f^{-1}\mathscr{G}, \mathscr{F}\right) \leftrightarrow \operatorname{Hom}_{(\operatorname{PreSh}(Y))}\left(\mathscr{G}, f_*\mathscr{F}\right), \\ \varphi \mapsto \varphi^b, \\ \psi^\sharp \longleftrightarrow \psi\end{gathered}$$

and (f^{-1}, f_*) is an adjoint pair between $\operatorname{PreSh}(Y)$ and $\operatorname{Sh}(X)$.

Proof: Let $\varphi : f^{-1}\mathscr{G} \to \mathscr{F}$ be a morphism of sheaves on X, and let $V \subseteq Y$ be open. Since $f\left(f^{-1}(V)\right) \subseteq V$, we have a map $\mathscr{G}(V) \to f^+\mathscr{G}\left(f^{-1}(V)\right)$, and we define φ_V^b as the composition

$$\mathscr{G}(V) \to f^+\mathscr{G}\left(f^{-1}(V)\right) \longrightarrow f^{-1}\mathscr{G}\left(f^{-1}(V)\right) \xrightarrow{\varphi_{f^{-1}(V)}} \mathscr{F}\left(f^{-1}(V)\right) = f_*\mathscr{F}(V).$$

Conversely, let $\psi : \mathscr{G} \to f_*\mathscr{F}$ be a morphism of presheaves on Y. To define the morphism $\psi^\sharp$ it suffices to define a morphism of presheaves $f^+\mathscr{G} \to \mathscr{F}$, which we call again $\psi^\sharp$. Let U be open in X, and $s \in f^+\mathscr{G}(U)$. If V is some open neighborhood of $f(U), U$ is contained in $f^{-1}(V)$. Let V be such a neighborhood such that there exists $s_V \in \mathscr{G}(V)$ representing s. Then $\psi_V\left(s_V\right) \in f_*\mathscr{F}(V) = \mathscr{F}\left(f^{-1}(V)\right)$. Let $\psi_U^\sharp(s) \in \mathscr{F}(U)$ be the restriction of the section $\psi_V\left(s_V\right)$ to U.

Proposition 4.1.18. Let $f : X \to Y$ be a continuous map, let $\mathscr{F}$ be a sheaf on X and let $\mathscr{G}$ be a presheaf on Y, and a morphism of presheaves $\psi : \mathscr{G} \to f_*\mathscr{F}$. Then for each $x \in X$, the map

$$\psi_x^\sharp : \mathscr{G}_{f(x)} \cong \left(f^{-1}\mathscr{G}\right)_x \longrightarrow \mathscr{F}_x$$

induced by $\psi^\sharp : f^{-1}\mathscr{G} \to \mathscr{F}$ on stalks can be described in terms of ψ as follows: For every open neighborhood $V \subseteq Y$ of $f(x)$, we have maps

$$\mathscr{G}(V) \xrightarrow{\psi_V} \mathscr{F}\left(f^{-1}(V)\right) \longrightarrow \mathscr{F}_x,$$

and taking the inductive limit over all V we obtain the map $\psi_x^\sharp : \mathscr{G}_{f(x)} \to \mathscr{F}_x$.

Chapter 5

Representation Theory

5.1 Definition

Definition 5.1.1. G is a finite group, a representation of G over a field F is a group homomorphism $\rho : G \to \mathrm{GL}(V)$ where V is a vector space over F.

Proposition 5.1.2. 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 5.1.3. Two representations of G are equivalent (or similar) if the FG-modules affording them are isomorphic modules.

Proposition 5.1.4. 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 5.1.5. By the definition of irreducible representation, a finite group has no infinite-dimention irreducible representation.

Definition 5.1.6 (simple ring)**.** A simple ring is a ring has no proper, nonzero 2-sided ideals.

Theorem 5.1.7 (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

$$\pi : V \to U$$

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

(1) $\pi(u) = u \quad$ for all $u \in U$

(2) $\pi(\pi(v)) = \pi(v) \quad$ for all $v \in V$

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

Let W_0 be subspace of V such that $V = U \oplus W_0$. π_0 be the projection onto U. For each $g \in G$ define

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

Define

$$\pi = \frac{1}{n} \sum_{g \in G} g\pi_0 g^{-1}$$

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

Corollary 5.1.8. chap $F \nmid |G|$, then every representation of finite group G of finite degree over F is completely reducible.

Definition 5.1.9. 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 $e_1 e_2 = e_2 e_1 = 0$.

(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 5.1.10. 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 $\varphi : M \to N$ be a surjective homomorphism. Then N is the sum of the images of the submodules $M_i \subset M$:

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

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 5.1.11. Let R be an arbitrary nonzero ring.

(1) If M and N are simple R-modules and $\varphi : M \to N$ is a nonzero R-module homomorphism, then φ is an isomorphism.

(2) (Schur's Lemma) If M is a simple R-module, then $\operatorname{Hom}_R(M, M)$ is a division ring.

Proof: Notice that

(a) $E_{ij}A$ is the matrix whose i^{th} row equals the j^{th} row of A and all other rows are zero.

(b) AE_{ij} is the matrix whose j^{th} column equals the i^{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 5.1.12. Let Δ be a division ring, let $n \in \mathbb{Z}^+$, let R be the ring of all $n \times n$ matrices with entries from Δ 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 αI, where α 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 Δ 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 $e_1, \ldots, e_n$ 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 $R = L_1 \oplus \cdots \oplus L_n$.

Lemma 5.1.13. 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 Δ_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 5.1.12. 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 $\left(0, \dots, 0, L^{(i)}, 0, \dots, 0\right)$ of all elements of R whose i^{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 $\varphi : M_i \to M_j$ 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 φ is an isomorphism and proves that $M_1, \dots, M_r$ are pairwise nonisomorphic simple R-modules.

Definition 5.1.14 (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 $L_i = Re_i$, 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 Δ_j, $j = 1, 2, \dots, r$. The integer r, the integers n_j, and the division rings Δ_j (up to isomorphism) are uniquely determined by R.

Proof: (1) $\Leftrightarrow$ (2): By Definition 2.2.39 and Definition 2.2.35.

(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, $(M+Q) \cap M_i = \varnothing$. A contradiction!

(4) $\Rightarrow$ (3): Since R itself is a semisimple R-module, the direct sum of R is also semisimple. Hence by Lemma 5.1.10, we have every R-module is semisimple.

(5) $\Rightarrow$ (4): By Lemma 5.1.12.

(2) $\Rightarrow$ (5):

Step 1: A is a ring, then the ring homomorphism $\varphi : A^{\text{opp}} \to \text{Hom}_A(A, A)$ 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 $\varphi : \text{Hom}_A(L^n, L^n) \to M_n(D)$, 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 $\varphi(0, \ldots, a, \ldots, 0)$.

Step 3: Use Schur's lemma to how 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 $L^n = L \oplus \cdots \oplus L$ with n factors.

By simplicity of S, $LS = S$, so $1 = l_1 s_1 + \cdots + l_n s_n$ for some $l_i \in L$ and $s_i \in S$ with n minimal. Then the map $(x_1, \ldots, x_n) \mapsto x_1 s_1 + \cdots + x_n s_n$ is a surjective homomorphism of left S-modules. If $y_1 s_1 + \cdots + y_n s_n = 0$ 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 $1 = l_1 s_1 + \ldots l_n s_n - s(y_1 s_1 + \cdots + y_n s_n)$, a contradiction!

Step 5: Let Δ be a division ring, and $n \in \mathbb{N}$. Then $M_n(\Delta^{op}) \cong M_n(\Delta)^{op}$. 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 $I_1 \supset \ldots I_n \supset \ldots$ be a decending chain of left ideals. Then $R = I_1 \oplus J_1 = J_1 \oplus J_2 \oplus I_2 = \ldots$. Let

$$J = \bigoplus_{i=1}^{\infty} I_i$$

, then $R = J \oplus K$. Consider $1 = j_1 + \ldots j_s + k$. 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 $R = R_1 \oplus \ldots R_r$, 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 Δ and Δ' are division rings. Then $\Delta \cong \Delta'$ and $n = n'$.

By Step 6, (6) $\Rightarrow$ (2) and Lemma 5.1.12, S is a simple ring satisfying D.C.C. Then let J be a minimal left ideal, we have $S = M_n(\Delta) \cong M_m(\mathrm{Hom}_S(L, L)^{\mathrm{opp}})$ for some m. Then $\Delta \cong \mathrm{Hom}_S(L, L)^{\mathrm{opp}}$. By Lemma 5.1.12, $\Delta \cong \Delta'$. $n = n'$ follows from the fact dimensions of S over Δ and Δ' are equal.

Step 9: (global uniqueness) $W_1 \times \ldots W_{r'} \cong R_1 \times R_2 \times \cdots \times R_r$ where R_i and W_j are simple rings. Then $r = r'$ and $R_i \cong W_i$ for some order.

Hint: Show that $(1, 0, \ldots, 0) \mapsto (1, 0, \ldots, 0)$.(reset the order if it's necessary).

Lemma 5.1.15. If Δ 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 5.1.16. 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 $n_1, \ldots, n_r$ and r are uniquely determined. In particular, G is isomorphic to a finite subgroup of $\mathrm{GL}_{n_1}(\mathbb{C}) \times \ldots \mathrm{GL}_{n_k}(\mathbb{C})$

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 Δ_j, $j = 1, 2, \ldots, r$. The integer r, the integers n_j, and the division rings Δ_j (up to isomorphism) are uniquely determined by R.

Let φ be the isomorphic map, then φ induce a ring homomorphism $\varphi_i : \mathbb{C} \to \Delta_i$ such that $\varphi_i(\mathbb{C}) \subset Z(\Delta_i)$. Then by Lemma 5.1.15, 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 $n_1, \ldots, n_r$ and r are uniquely determined.

Theorem 5.1.17. $\mathbb{C}[G]$ has exactly r distinct isomorphism types of irreducible modules and these have complex dimensions $n_1, n_2, \ldots, n_r$ given by Lemma 5.1.13.

Proposition 5.1.18. $\sum_{i=1}^{r} n_i^2 = |G|$

Proposition 5.1.19. r equals the number of conjugacy classes in G and the dimension of $Z(\mathbb{C}G)$.

Proof: Let $\mathcal{K}_1, \ldots, \mathcal{K}_s$ be the distinct conjugacy classes of G (recall that these partition G). For each conjugacy class $\mathcal{K}_i$ of G let

$$X_i = \sum_{g \in \mathcal{K}_i} g \quad \in \mathbb{C}G.$$

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 $h^{-1}Xh = X$,

$$\sum_{g \in G} \alpha_g h^{-1} g h = \sum_{g \in G} \alpha_g g.$$

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.

5.2 Character

All representations considered are assumed to be finite dimensional.

Definition 5.2.1. A class function is any function from G into F which is constant on the conjugacy classes of G, i.e., $f : G \to F$ such that $f\left(g^{-1}xg\right) = f(x)$ for all $g, x \in G$.

Definition 5.2.2. If φ is a representation of G afforded by the FG-module V, the character of φ is the function

$$\chi : G \to F \quad \text{ defined by } \quad \chi(g) = \operatorname{tr}\varphi(g),$$

Proposition 5.2.3. (1) Equivalent representations have the same character.

(2) the character of a representation is a class function.

(3) χ is the character of $\varphi : G \to \mathrm{GL}(V)$. Then $\chi(1)$ is the degree of φ.

Proposition 5.2.4. V_1 and V_2 are $F[G]$-module, χ and ψ are their character respectively. Then character of $V_1 \oplus V_2$ is $\chi + \psi$.

Example 5.2.5. Consider $\mathbb{C}[G]$ itself as a $\mathbb{C}[G]$-module, we call this representation the regular representation of G. By Lemma 5.1.12 and Lemma 5.1.13,

$$\chi_\rho(g) = \sum_{i=1}^{r} \chi_i(1)\chi_i(g) = \begin{cases} |G| & g = e \\ 0 & g \neq e \end{cases}$$

Lemma 5.2.6. V_1 and V_2 are finite-dimensional k-vector space, $A : V_1 \to V_1$ and $B : V_2 \to V_2$ are linear transforms. Then for the linear transform $A \otimes B : V_1 \otimes V_2 \to V_1 \otimes_k V_2$, we have $\det(A \otimes B) = \det(A)^{\dim V_2} \det(B)^{\dim V_1}$ and $\mathrm{tr}(A \otimes B) = \mathrm{tr}(A)\mathrm{tr}(B)$.

Proposition 5.2.7. $\rho_1 : G \to \mathrm{GL}(V_1)$ and $\rho_1 : G \to \mathrm{GL}(V_2)$ are representations of G. Then the representation $\rho_1 \otimes \rho_2 : G \to \mathrm{GL}(V_1 \otimes_k V_2)$ defined by

$$g \mapsto \rho_1(g) \otimes \rho_2(g)$$

is called tensor product of ρ_1 and ρ_2. And by lemma 5.2.6 we have $\chi_{\rho_1 \otimes \rho_2} = \chi_{\rho_1}\chi_{\rho_2}$

Proposition 5.2.8. (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 $M_1, \ldots, M_r$ be the distinct irreducible $C[G]$-module defined by Lemma 5.1.12 and Lemma 5.1.13, Let $z_1, z_2, \ldots, z_r$ be the primitive central idempotents of $\mathbb{C}[G]$. Let χ_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 $\chi_1, \ldots, \chi_r$ are linearly independent as class functions on G. By Proposition 5.1.19, $\chi_1, \ldots, \chi_r$ form a basis of class functions on G.

Corollary 5.2.9. Let G be a finite group. There's $\mathbb{C}$-algebra isomorphism:

$$\varphi : \mathbb{C}[G] \cong M_{n_1}(\mathbb{C}) \times M_{n_2}(\mathbb{C}) \times \cdots \times M_{n_r}(\mathbb{C})$$

Then representation $\rho_1, \ldots, \rho_r$ given by $\varphi(g) = (\rho_1(g), \ldots, \rho_r(g))$ is isomorphic to the irreducible representation defined by Lemma 5.1.12 and Lemma 5.1.13.

Proof: Check the character.

Definition 5.2.10. For class functions θ and ψ 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) $(\theta, \alpha\psi_1 + \beta\psi_2) = \bar{\alpha}\,(\theta, \psi_1) + \bar{\beta}\,(\theta, \psi_2)$, and

(3) $(\theta, \psi) = (\psi, \theta)$.

Proposition 5.2.11. Consider all the distinct irreducible representation $\rho_1, \ldots, \rho_r$ with characters $\chi_1, \dot{;}\chi_r$. There's a $\mathbb{C}$-algebra homomorphism

$$\varphi : \mathbb{C}[G] \to M_{n_1}(\mathbb{C}) \times M_{n_2}(\mathbb{C}) \times \cdots \times M_{n_r}(\mathbb{C})$$

induced by $\varphi(g) = (\rho_1(g), \ldots, \rho_r(g))$. 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 5.2.12. Let $z_1, \ldots, z_r$ be the orthogonal primitive central idempotents in $\mathbb{C}[G]$ such that $\varphi(z_i) = (O, \ldots, I_{n_i}, \ldots, O)$. Then

$$z_i = \frac{\chi_i(1)}{|G|} \sum_{g \in G} \chi_i\left(g^{-1}\right) g$$

Proof: Let

$$z_i = \sum_{g \in G} \alpha_g g$$

If ρ is the character of regular representation of G, then

$$\sum_{j=1}^{r} \chi_j(1)\chi_j\left(z_i g^{-1}\right) = \rho\left(z_i g^{-1}\right) = \alpha_g |G|.$$

It's esay to check that $\chi_j(z_i g^{-1}) = \chi_i(g^{-1})\delta_{ij}$, then

$$z_i = \sum_{g \in G} \frac{1}{|G|} \sum_{j=1}^{r} \chi_j(1)\chi_j(g^{-1})\delta_{ij} g = \frac{\chi_i(1)}{|G|} \sum_{g \in G} \chi_i\left(g^{-1}\right) g$$

Lemma 5.2.13. If ψ is any character of G then $\psi(x)$ is a sum of roots of 1 in $\mathbb{C}$ and $\psi\left(x^{-1}\right) = \overline{\psi(x)}$ 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 5.2.14 (The First Orthogonality Relation for Group Characters)**.** Let G be a finite group and let $\chi_1, \ldots, \chi_r$ 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:

$$\begin{aligned} z_i\delta_{ij} &= z_iz_j \\ &= \frac{\chi_i(1)}{|G|}\frac{\chi_j(1)}{|G|}\sum_{g,h\in G}\chi_i\left(g^{-1}\right)\chi_j\left(h^{-1}\right)gh \\ &= \frac{\chi_i(1)}{|G|}\frac{\chi_j(1)}{|G|}\sum_{y\in G}\left[\sum_{x\in G}\chi_i\left(xy^{-1}\right)\chi_j\left(x^{-1}\right)\right]y \end{aligned}$$

By the expression of the coefficient of z_i, we have

$$\delta_{ij}\frac{\chi_i(1)}{|G|}\chi_i\left(g^{-1}\right) = \frac{\chi_i(1)\chi_j(1)}{|G|^2}\sum_{x\in G}\chi_i\left(xg^{-1}\right)\chi_j\left(x^{-1}\right).$$

Simplifying (and replacing g by g^{-1}) gives

$$\delta_{ij}\frac{\chi_i(g)}{\chi_j(1)} = \frac{1}{|G|}\sum_{x\in G}\chi_i(xg)\chi_j\left(x^{-1}\right) \qquad \text{for all } g\in G$$

Taking $g=1$, we have

$$\delta_{ij} = \frac{1}{|G|}\sum_{x\in G}\chi_i(x)\chi_j\left(x^{-1}\right)$$

Then by Lemma 5.2.13, we get the finial result.

Theorem 5.2.15 ((The Second Orthogonality Relation for Group Characters))**.** Denote the number of conjacgue 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 $W=\operatorname{diag}\{|C_1|,\ldots,|C_r|\}$, $X=(\chi_i(x_j))$. Then $WXX^H=\operatorname{diag}\{|G|,\ldots,|G|\}$,

5.3 Induced representation

Definition 5.3.1. Let H be a subgroup of the finite group G and let V be an FH-module affording the representation φ 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 φ. If ψ is the character of φ then the character of the induced representation is called the induced character and is denoted by $\operatorname{Ind}_H^G(\psi)$.

Proposition 5.3.2. Let H be a subgroup of the finite group G and let $g_1, \ldots, g_m$ be representatives for the distinct left cosets of H in G. Let V be an FH-module affording the matrix representation φ of H of degree n under the bais $v_1, \ldots, v_n$ 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

$$g_1 \otimes v_1, g_1 \otimes v_2, \ldots, g_1 \otimes v_n, g_2 \otimes v_1, \ldots, g_2 \otimes v_n, \ldots\ldots, g_m \otimes v_n$$

, Φ defined for each $g \in G$ by

$$\Phi(g) = \begin{pmatrix} \varphi\left(g_1^{-1} g g_1\right) & \cdots & \varphi\left(g_1^{-1} g g_m\right) \\ \vdots & \vdots & \vdots \\ \varphi\left(g_m^{-1} g g_1\right) & \cdots & \varphi\left(g_m^{-1} g g_m\right) \end{pmatrix}$$

where each $\varphi\left(g_i^{-1} g g_j\right)$ is an $n \times n$ block appearing in the i, j block position of $\Phi(g)$, and where $\varphi\left(g_i^{-1} g g_j\right)$ is defined to be the zero block whenever $g_i^{-1} g g_j \notin H$.

Corollary 5.3.3. If ψ is the character afforded by V then the induced character is given by

$$\operatorname{Ind}_H^G(\psi)(g) = \sum_{i=1}^m \psi\left(g_i^{-1} g g_i\right)$$

where $\psi\left(g_i^{-1} g g_i\right)$ is defined to be 0 if $g_i^{-1} g g_i \notin H$, and

$\operatorname{Ind}_H^G(\psi)(g) = 0$ if g is not conjugate in G to some element of H. In particular, if H is a normal subgroup of G then $\operatorname{Ind}_H^G(\psi)$ is zero on all elements of $G - H$.

Theorem 5.3.4. Let G be a group, let H be a subgroup of G and let ψ and ψ' be characters of H.

(1) (Induction of characters is additive) $\operatorname{Ind}_H^G(\psi + \psi') = \operatorname{Ind}_H^G(\psi) + \operatorname{Ind}_H^G(\psi')$.

(2) (Induction of characters is transitive) If $H \leq K \leq G$ then

$$\operatorname{Ind}_K^G\left(\operatorname{Ind}_H^K(\psi)\right) \cong \operatorname{Ind}_H^G(\psi)$$

Proposition 5.3.5 (Frobenius reciprocity)**.** Let G be a group, let H be a subgroup of G and let ψ and φ be characters of H and G. Then

$$\langle \psi, \operatorname{Res} \varphi \rangle_{\mathrm{H}} = \langle \operatorname{Ind} \psi, \varphi \rangle_{\mathrm{G}}$$

Proof: Take V be a $\mathbb{C}[G]$-module and W be a $\mathbb{C}[H]$-module such that ψ is the character of W and φ is the character of V. Let $\tilde{V}$ be the $\mathbb{C}[H]$-module induced by V.

By Theorem 2.2.24,

$$\langle \psi, \operatorname{Res} \varphi \rangle_{\mathrm{H}} = \dim_{\mathbb{C}} \operatorname{Hom}(W, \tilde{V}) = \dim_{\mathbb{C}} \operatorname{Hom}(\mathbb{C}[G] \otimes_{\mathbb{C}[H]} W, V) = \langle \operatorname{Ind} \psi, \varphi \rangle_{\mathrm{G}}$$

Proposition 5.3.6. G is a group, H and K are the subgroup of G. Let $\{s_1, \ldots, s_r\}$ be the representation elements of double coset decomposition of G by H and K. i.e.

$$G = Ks_1H \cup \ldots Ks_rH$$

where $Ks_iH \cap Ks_jH = \varnothing$ if $i \neq j$. (V, p) be a representation of H and $\mathrm{Ind}_H^G(\rho)$ be the induced representation. The restriction $\mathrm{Res}_K\left(\mathrm{Ind}_H^G(\rho)\right)$ of the G-representation $\mathrm{Ind}_H^G(\rho)$ to a K-representation decomposes as a direct sum

$$\bigoplus_{i=1}^{r} \mathrm{Ind}_{s_i^{-1}Hs_i \cap K}^{K}\left(\rho^{s_i}\right)$$

$\rho^{s_i}(x) := \rho\left(s_i x s_i^{-1}\right)$ 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

$$\mathbb{C}[G] \otimes_{\mathbb{C}[H]} V \cong \bigoplus_{i=1}^{r} \mathbb{C}[K]s_i\mathbb{C}[H] \otimes_{\mathbb{C}[H]} V \cong \bigoplus_{i=1}^{r} \mathbb{C}[K] \otimes_{\mathbb{C}[K \cap s_iHs_i^{-1}]} \tilde{V}$$

where $\tilde{V}$ is a representation of $K \cap s_iHs_i^{-1}$ defined by $(s_ihs_i^{-1}) \cdot v = hv$ and in this equation, the isomorphisc map between $\mathbb{C}[K] \otimes_{\mathbb{C}[K \cap s_iHs_i^{-1}]} \tilde{V}$ and $\mathbb{C}[K]s_i\mathbb{C}[H] \otimes_{\mathbb{C}[H]} V$ is induced by bi-additive maps

$$\begin{aligned} \mathbb{C}[K] \times \tilde{V} &\to \mathbb{C}[K]s_i\mathbb{C}[H] \otimes_{\mathbb{C}[H]} V \\ (k, v) &\mapsto ks_i \otimes v \end{aligned}$$

and

$$\begin{aligned} \mathbb{C}[K]s_i\mathbb{C}[H] \times V &\to \mathbb{C}[K] \otimes_{\mathbb{C}[K \cap s_iHs_i^{-1}]} \tilde{V} \\ (ks_ih, v) &\mapsto k \otimes hv \end{aligned}$$

Corollary 5.3.7 (Mackey's irreducibility criterion)**.** With all the notations in above Propostion, in order to make the induced representation $\mathrm{Ind}_H^G \rho$ be irreducible, it is necessary and sufficient that the following two conditions be satisfied:

(1) ρ is irreducible.

(2) For each $s \in G - H$ the two representations ρ^s and $\mathrm{Res}_s(\rho)$ of H_s are disjoint.

Proof: Let φ be the character of ρ, by Frobenius reciprocity,

$$\langle \mathrm{Ind}_H^G(\varphi), \mathrm{Ind}_H^G(\varphi) \rangle = \langle \varphi, \mathrm{Res}(\mathrm{Ind}(\varphi)) \rangle$$

Let χ_i be the character of ρ^{s_i}, then by Frobenius reciprocity and Proposition 5.3.6

$$\langle \varphi, \mathrm{Res}(\mathrm{Ind}(\varphi)) \rangle = \sum_{i=1}^{r} \langle \mathrm{Res}_{s_i^{-1}Hs_i \cap H}(\varphi), \chi_i \rangle$$

Corollary 5.3.8. Suppose H is normal in G. In order that $\mathrm{Ind}_H^G(\rho)$ be irreducible, it is necessary and sufficient that ρ be irreducible and not isomorphic to any of its conjugates ρ^s for $s \notin H$.

Definition 5.3.9. Let G be a finite group and let $\chi_1, \ldots, \chi_h$ be its distinct irreducible characters. A class function on G is a character if and only if it is a linear combination of the χ_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

$$R(\mathrm{G}) = \mathbb{Z}\chi_1 \oplus \cdots \oplus \mathbb{Z}\chi_h.$$

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 χ_i form a basis of $F(G)$, by Theorem 2.2.28, we have $\mathbb{C}$-algebra isomorphism

$$F(G) \cong \mathbb{C} \otimes_{\mathbb{Z}} R(G)$$

Theorem 5.3.10.

Theorem 5.3.11 (Artin)**.**

Reference: Matsumura, Atiyah, Gortz 1, GTM73, GTM42, Dummit, GTM52, Miline:Galios Theory, Red book, Hu Yong quan:Galois Theory