Algebra

Wang Chao

August 26, 2019

Contents

Introduction

This is the notes of Algebra I wrote after reading various books and material, including

- *Algebra* by Michael Artin
- *Algebra* by Serge Lang
- *Basic Algebra* by Nathan Jacobson
- *Advanced Modern Algebra* by Joseph Rotman

The following is the convention of notations.

0.1 Notation

Chapter 1

Group Theory

1.1 Definition

Definition 1.1.1. *A **group** $(G, \circ, e)$ is a set G together with a binary operation $\circ : G \times G \to G$ and a* **unit** *$e \in G$ such that*

1. $\forall g \in G : g \circ e = e \circ g = g$
2. ***associativity***: $\forall g, h, s \in G : (g \circ h) \circ s = g \circ (h \circ s)$
3. $\forall g \in G \ \exists g^{-1} \in G : g \circ g^{-1} = g^{-1} \circ g = e$

*g^{-1} is called the **inverse** if g.*

There are similar algebra structures with less restriction, such as **monoid**, **semi-group** and **monad**. Their definitions are listed in Tab 1.1.

	invertibility	existence of unit	associativity
group	$\surd$	$\surd$	$\surd$
monoid	$\times$	$\surd$	$\surd$
semi-group	$\times$	$\times$	$\surd$
monad	$\times$	$\surd$	$\times$
magma	$\times$	$\times$	$\times$

Table 1.1: Comparison between several algebraic structures, $\times$ means not necessary.

Lemma 1.1.2. *Let S be a semi-group, and e be an element not in S. We construct $M = S \cup \{e\}$ and extend $\circ$ in S to $\circ$ in M by defining $e \circ a = a = a \circ e$ for all $a \in M$. Then M is a monoid.*

Lemma 1.1.3. *Let a be an element in a monoid M. Then a is invertible with b as its inverse if and only if $aba = a$ and $ab^2a = 1$.*

Proof. $ab = abab^2a = ab^2a = 1$ and $ba = ab^2aba = ab^2a = 1$. □

Definition 1.1.4. *A **subgroup** of group $(G, \circ, e)$ is $(H, \circ, e)$ where H is a subset of G that contains e, and is closed under $\circ$ and taking inverse. Clearly it's a group.*

When their is no ambiguity, we usually abbreviate $(G, \circ, e)$ for G.

Lemma 1.1.5. *The intersection of a family of subgroups of a group is a subgroup.*

Definition 1.1.6. *Let S be a subgroup of G. S is called* **maximal** *if there's no subgroup H of G such that $G \supsetneq H \supsetneq S$.*

Definition 1.1.7. *Let S be a subset of a group G. $\langle S \rangle$ is the subgroup* **generated by** *S if it is the intersection of all subgroups of G that contain S.*

Lemma 1.1.8. *Let S be a subset of a group G. $\langle S \rangle$ is the set of finite products of elements in $S \cup S^{-1}$.*

Definition 1.1.9. *The **order** of a group G is the cardinality of it as a set, denoted by $|G|$. A group is **finite** if $|G| < \infty$, otherwise it's **infinite**.*

We use a^n to denote

$$\underbrace{a \circ a \circ \cdots \circ a}_{n} \tag{1.1}$$

and a^{-n} to denote

$$\underbrace{a^{-1} \circ a^{-1} \circ \cdots \circ a^{-1}}_{n} \tag{1.2}$$

And we define a^0 to be e.

Definition 1.1.10. *The* **cylic subgroup** *of G generated by $a \in G$ is the group $\langle a \rangle = \{a^n | n \in \mathbb{Z}\}$.*

Definition 1.1.11. *Let G be a group. The* **order** *of $a \in G$ is $|\langle a \rangle|$.*

Definition 1.1.12. *Let G be a group. Elements in G of order 2 are called* **involutions**.

Lemma 1.1.13. *Any finite group of even order contains an involution.*

Proof. Pair a with a^{-1}. □

Definition 1.1.14. *A group is called **Abelian** if it's **commutative**, that is,*

$$\forall g_1, g_2 \in G : g_1 \circ g_2 = g_2 \circ g_1 \tag{1.3}$$

*Otherwise it's called **non-Abelian**.*

Lemma 1.1.15. *When we multiply n elements of an Abelian group in no matter what order, we always get the same result.*

Lemma 1.1.16. *A group is abelian if every element a satisfies $a^2 = e$.*

1.2 Cosets and Quotient Groups

Definition 1.2.1. *Let H be a subgroup of group G. We define an equivalence relation in G as*

$$g_1 \sim g_2 \iff \exists h \in H : g_1 = g_2 h \tag{1.4}$$

*Each equivalent classes are called **left cosets** relative to H, denoted by $[G]_H$. The coset containing g is denoted by $[g]_H$.The subscript is usually omitted if there's no ambiguity. We call the number of cosets the **index** of H, denoted by $[G : H]$.*

Definition 1.2.2. *Similarly we can define an equivalence relation in G as*

$$g_1 \sim g_2 \iff \exists h \in H : g_1 = h g_2 \tag{1.5}$$

*Each equivalent classes are called **right cosets** relative to H, denoted by $[G]_{H,}$. The coset containing g is denoted by $[g]_{H,}$.*

Theorem 1.2.3 (Lagrange)**.** *Let G be a finite group and H is its subgroup, $|G| = |H|[G : H]$.*

Proof. Each $[g] = gH$. So that $|[g]| = |H|$. Each left coset is of cardinality $|H|$. □

Corollary 1.2.4. *If G is a finite group of prime order, G has no proper nontrivial subgroup.*

Corollary 1.2.5. *Let H be a subgroup of group G, and K a subgroup of H. If $[G : K]$ is finite, then $[G : K] = [G : H][H : K]$.*

Lemma 1.2.6. *Let H_1 and H_2 be two subgroups of group G. Then $[G : H_1] > [H_2 : H_1 \cap H_2]$.*

Proof. See Fig 1.1. □

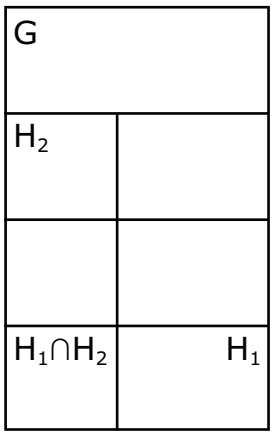


Figure 1.1: A illustrative figure to show $[G : H_1] > [H_2 : H_1 \cap H_2]$.

Definition 1.2.7. *We define a **normal subgroup** H of G to be a subgroup such that*

$$\forall g \in G : g^{-1} H g = H \tag{1.6}$$

Lemma 1.2.8. *A left coset relative to a normal subgroup is a right coset.*

Theorem 1.2.9. *Cosets relative to a normal subgroup H of group G form a group under set product, and the unit element is $[e] = H$. This group is called the* ***quotient group****, denotes as G/H.*

Proof. If $[g]$ and $[g']$ are cosets relative to a normal subgroup H

$$[g] \cdot [g'] = gHg'H = (gg'g'^{-1}H)g'H = gg'(g'^{-1}Hg')H = gg'HH = gg'H = [gg'] \tag{1.7}$$

□

Theorem 1.2.10. *Let G be a group and H be a subgroup of index 2. Then H is a normal subgroup. $\forall g \in G : g^2 \in H$.*

Proof. If $G = H \cup gH$, $\forall h \in H : ghg^{-1} \in H$. □

Theorem 1.2.11. *Let H be a normal subgroup of G. Let $\pi : G \to G/H$ be $h \to [h]_H$. Then $K \to \pi(K)$ is a 1-1 correspondence between the subgroups of G that contains H to subgroups of G/H. If K' is a normal subgroup of G/H, then $\pi^{-1}(K')$ is a normal subgroup of G.*

Proof. Let K be a subgroup of G that contains H. Clearly $\pi^{-1}(\pi(K)) = K$. So π is injective. Let K be a subgroup of G/H. It's easy to see that $\pi^{-1}(K)$ is a subgroup of G that contains H. So π is surjective. So π is a 1-1 correspondence. Let K' be a normal subgroup of G/H. $\forall g \in G : g\pi^{-1}(K')g^{-1} = \pi^{-1}(\pi(g\pi^{-1}(K')g^{-1})) = \pi^{-1}([g]_H K'[g]_H^{-1})) = \pi^{-1}(K')$. So $\pi^{-1}(K')$ is a normal subgroup of G. □

Note Cosets and quotient groups can be defined in another way:

Let $\sim$ be an equivalent relation in monoid M. Define $\sim$ to be a congruence iff it satisfies that $a \sim b \wedge c \sim d \Rightarrow ab \sim cd$. This ensures the composition $[a] \cdot [b] = [ab]$ well-defined. Let $[M] = \{[m] | m \in M\}$. Then $([M], \cdot, [1])$ forms a monoid.

If M is a group, $([M], \cdot, [1])$ is also a group. Then $[1]$ is a normal subgroup of M and $[a]$s are cosets of $[1]$. $([M], \cdot, [1])$ is just the quotient group $M/[1]$.

Definition 1.2.12. *Let H and T be subgroups of group G. We define an equivalence relation in G as*

$$g_1 \sim g_2 \iff \exists h \in H, t \in T : g_1 = hg_2t \tag{1.8}$$

Each equivalent classes are called ***(H, T)-double cosets****, denoted by $[G]_{H,T}$. The coset containing g is denoted by $[g]_{H,T}$.*

1.3 Some Concepts

Definition 1.3.1. *The* ***center*** *of a group is the set of elements that commutes with every elements in G, denoted by $Z(G)$. That is*

$$Z(G) = \{x \in G | \forall g \in G : gx = xg\} \tag{1.9}$$

Definition 1.3.2. *The **centralizer** of a set H in group G is the set of elements that commutes with every elements in H, denoted by $C_G(H)$. That is*

$$C_G(H) = \{x \in G | \forall g \in H : gx = xg\} \tag{1.10}$$

Definition 1.3.3. *The **normalizer** of a set H in group G, denoted by $N_G(H)$, is defined by*

$$N_G(H) = \{z \in G | zH = Hz\} \tag{1.11}$$

Normally we abbreviate $C_G(\{x\})$ for $C_G(x)$

Lemma 1.3.4. *$Z(G)$ is a normal subgroup of G, and $C_G(H)$ and $N_G(H)$ is a subgroup of G.*

1.4 Commutator

Definition 1.4.1. *Let G be a group. The* **commutator** *of $g_1, g_2 \in G$ is $[g_1, g_2] = g_1 g_2 g_1^{-1} g_2^{-1}$.*

Definition 1.4.2. *Let G be a group. The* **commutator subgroup** *of G is $\langle \{[g_1, g_2] | g_1, g_2 \in G\} \rangle$.*

Lemma 1.4.3. *Let G be a group, and H be the commutator subgroup of G. Then H is a normal subgroup.*

Proof. Let $S = \{[g_1, g_2] | g_1, g_2 \in G\}$. Since $t[g_1, g_2]t^{-1} = [tg_1t^{-1}, tg_2t^{-1}]$, it's easy to see that $N_G(S) = G$. Then $N_G(H) = G$. □

Lemma 1.4.4. *Let G be a group, and H be the commutator subgroup of G. Then G/H is abelian.*

Proof. $[a] \cdot [b] \cdot [a^{-1}] \cdot [b^{-1}] = [aba^{-1}b^{-1}] = 1$. □

Lemma 1.4.5. *Let G be a group, H be the commutator subgroup of G, and K is a normal subgroup of G. G/K is abelian iff $H \subseteq K$.*

Proof. G/K is abelian $\Leftrightarrow \forall a, b : [aba^{-1}b^{-1}]_K = 1 \Leftrightarrow \forall a, b : aba^{-1}b^{-1} \in K \Leftrightarrow H \subseteq K$. □

1.5 Homomorphism and Isomorphism

Definition 1.5.1. *Let G_1 and G_2 be two groups. We define a map f from G_1 to G_2 to be a* **homomorphism** *if*

$$\forall g, h \in G_1 : f(g) \circ f(h) = f(g \circ h) \tag{1.12}$$

and $f(e) = e$.

Lemma 1.5.2. *Let f be a homomorphism. $f(g)^{-1} = f(g^{-1})$*

Definition 1.5.3. *A homomorphism is called a(n)*

1. **monomorphism** *if it's injective*

2. **epimorphism** *if it's surjective*

3. **isomorphism** *if it's bijective, denoted by* $\cong$

Definition 1.5.4. *A homomorphism from G to itself is called an* **endomorphism**. *An isomorphism from G to itself is called an* **automorphism**.

Lemma 1.5.5. *All automorphisms of G form a group under function composition. This is called $Aut(G)$.*

Definition 1.5.6. *Let f be a homomorphism from G_1 to G_2, its* **kernel** *is defined as* $\ker(f) = f^{-1}(e)$ *while its* **image** *is defined as* $\text{im}(f) = f(G_1)$.

Lemma 1.5.7. $\ker(f)$ *is a normal subgroup of* G_1 *and* $\text{im}(f)$ *is a subgroup of* G_2. $G_1/\ker(f) \cong \text{im}(f)$.

Definition 1.5.8. *Let G be a group. We define the group of* **inner automorphisms** $Inn(G)$ *to be the collection of maps I_a, defined by $I_a(x) = axa^{-1}$.*

Lemma 1.5.9. *The map $I : G \mapsto Inn(G)$ defined by $I(a) = I_a$ is a homomorphism with kernel $C(G)$. Thus $Inn(G) \cong G/C(G)$.*

Lemma 1.5.10. $Inn(G)$ *is a normal subgroup of* $Aut(G)$.

Proof. $f^{-1}(af(x)a^{-1}) = f^{-1}(a)x(f^{-1}(a))^{-1}$ □

Definition 1.5.11. $Aut(G)/Inn(G)$ *is called the group of* **outer automorphisms**.

Lemma 1.5.12. *Let H be a subset of G. Let I be the homomorphism $N_G(H) \mapsto Aut(H)$ by $I(g)(h) = ghg^{-1}$. Then the kernel of I is $C_G(H)$.*

Definition 1.5.13. *Let G_1 and G_2 be two groups. We define a map f from G_1 to G_2 to be an* **anti-homomorphism** *if*

$$\forall g, h \in G_1 : f(g) \circ f(h) = f(h \circ g) \tag{1.13}$$

and $f(e) = e$.

Lemma 1.5.14. *If f is a homomorphism, $g \mapsto f(g)^{-1}$ is an* ***anti-homomorphism***

Definition 1.5.15. *An* ***anti-isomorphism*** *is an anti-homomorphism that is bijective.*

1.6 Isomorphism Theorems

Theorem 1.6.1. *Let K be a normal subgroup of H, which is a subgroup of G. Then H/K is a subgroup of G/K. Let f be a map from the subgroups of G that contains H to the subgroups of G/K, defined by $f(T) = T/K$. Then f is bijective.*

Theorem 1.6.2. *Let K be a normal subgroup of H, which is a subgroup of G. Then H/K is a normal subgroup iff H is a normal subgroup of G. In this case, $G/H \cong (G/K)/(H/K)$.*

Proof. Obviously H/K is a subgroup of G/K. Then it's a normal subgroup iff

$$[g]_K(H/K)[g]_K^{-1} = \{[g]_K[h]_K[g^{-1}]_K | h \in H\} = \{[ghg^{-1}]_K | h \in H\} = H/K \tag{1.14}$$

It's easy to prove that this is equivalent to

$$gHg^{-1} = H \tag{1.15}$$

Finally we give an isomorphism map

$$f([g]_H) = [[g]_K]_{H/K} \tag{1.16}$$

□

Theorem 1.6.3. *Let H and K be subgroups of G, K normal in G. Prove that HK is a subgroup of G containing K as normal subgroup, $H \cap K$ is normal in H, and $HK/K \cong H/(H \cap K)$.*

Proof. The proof is straightforward. the isomorphism map is

$$f([hk]_K) = [h]_{H\cap K} \tag{1.17}$$

□

1.7 Direct product and Semi-direct Product

Definition 1.7.1. *The* **direct product** *of two groups G_1 and G_2 is a group denoted as $G_1 \times G_2$, with the set $G_1 \times G_2$ (treated as Cartesian product of sets), and multiplication rule as*

$$(g_1, g_2) \circ (g_1', g_2') = (g_1 \circ g_1', g_2 \circ g_2') \tag{1.18}$$

Definition 1.7.2. *The* **semi-direct product** *of two groups G_1 and G_2 is a group denoted as $G_1 \rtimes G_2$, with the set $G_1 \times G_2$ and multiplication rule as*

$$(g_1, g_2) \circ (g_1', g_2') = (g_1 \circ \phi_{g_2}(g_1'), g_2 \circ g_2') \tag{1.19}$$

where ϕ_g is a homomorphism from G_2 to $\mathrm{Aut}(G_1)$.

Lemma 1.7.3. *Let H be a normal subgroup of G, and for each $[g]$. Suppose there exist a homomorphism f from G/H to G such that $f([g]) \in [g]$ for every $[g] \in G/H$.*

We define the multiplication rule of semi-direct product group $H \rtimes G/H$ as

$$(h, [g]) \circ (h', [g]') = (h \circ f([g]) \circ h' \circ f([g])^{-1}, [g] \circ [g]') \tag{1.20}$$

The map g from $H \rtimes G/H$ to G defined by

$$g(h, [g]) = h \circ f([g]) \tag{1.21}$$

is an isomorphism.

In general, we have the theorem

Theorem 1.7.4 (Schur,Zassenhaus)**.** *Let H be a normal subgroup of a finite group G. If $|H|$ and $|G/H|$ are relatively prime, then $G \cong H \rtimes G/H$ for some ϕ.*

1.8 Group acting on sets

Definition 1.8.1. *All bijective maps from a set X to itself form a group under map composition, this is called the* ***permutation group*** *of X, denoted by S_X. The unit element is just the identity map. Any subgroup of this group is called a* ***group of transformation*** *(on X).*

Theorem 1.8.2 (Cayley)**.** *Any group is isomorphic to a group of transformation*

Proof. The isomorphism from G to group of transformation on G is just $g \to f_g$ where f_g is a map defined as $f_g g' = g \circ g'$. □

Definition 1.8.3. *An* **action** *of a group G on X is a triple (G, X, P), where P a homomorphism $G \mapsto S_X$. We usually use $\circ$ for the map P, writing $P(g)(x)$ as $g \circ x$. With an action $(G, X, \circ)$, we also call X a G-***set***.*

Definition 1.8.4. *We say the action of G on X is* **faithful** *if the homomorphism $G \mapsto S_X$ is injective.*

Definition 1.8.5. *If we define the equivalent relation over X as*

$$X \sim Y \iff \exists g : g \circ x = y \tag{1.22}$$

The equivalent classes are called ***orbits****, denoted by O_i, where i is the index to distinguish different orbits. The action is called* ***transitive*** *if there is only one orbit.*

Obviously, if $|X|$ is finite, $|X| = \sum_i |O_i|$.

Definition 1.8.6. *For a point $x \in O_i$, the elements g of G such that $g \circ x = x$ is called the* ***stabilizer*** *of x, denoted by S_x.*

Lemma 1.8.7. *S_x is a subgroup of G.*

Lemma 1.8.8. *If $h \circ x = y$, then $S_y = h \circ S_x \circ h^{-1}$. Thus if $x, y \in O_i$, $|S_x| = |S_y|$.*

Lemma 1.8.9. *There is a 1-1 map between G/S_x and O_i defined by*

$$f([g]) = g \circ x \tag{1.23}$$

Corollary 1.8.10. *If $|G|$ is finite, we have the* ***counting formula****: $|G/S_x| = |O_i|$ and $|G| = |O_i||S_x|$.*

Example 1.8.11. *We define the* **conjugation action** *of a group G on itself as $g \circ g' = gg'g^{-1}$. The orbits are called conjugacy class, and two elements in an orbit are called conjugate to each other.*

Let g be an element of G. If $g \in Z(G)$, it forms a conjugacy class itself. If $g \notin Z(G)$, its stabilizer is $C(g)$. Let $\{C_i\}$ be the conjugacy classes of G. Then the counting formula becomes the **class equation***:*

$$|G| = |C(G)| + \sum_{|C_i|>1} |C_i| = |Z(G)| + \sum_{|C_i|>1} |G/C(x_i)| \tag{1.24}$$

where $x_i \in C_i$.

Definition 1.8.12. *Let X and Y be G-sets. A map $f : X \mapsto Y$ is a* **homomorphism** *if $\forall g \in G, x \in X : g \circ f(x) = f(g \circ x)$. If f is bijective, then it's called an* **isomorphism**.

Example 1.8.13. *Let H be a subgroup of G. G acts on $[G]_H$ by $g \circ [a]_H = [ga]_H$.*

Lemma 1.8.14. *Let $(G, X, \circ)$ be a transitive action and $x \in X$. There's a G-set isomorphism $f : X \mapsto [G]_{S_x}$ defined by $f(g \circ x) = [g]_{S_x}$.*

Definition 1.8.15. *Let X be a transitive G-set. The* **rank** *of X is the number of S_x-orbits of X.*

Lemma 1.8.16. *Let X be a transitive G-set and $x \in X$. The rank of X is the number of (S_x, S_x)-double cosets in G.*

Proof. The isomorphism $f : X \mapsto [G]_{S_x}$ induce the 1-1 map between the S_x-orbits and the (S_x, S_x)-double cosets. □

1.9 Examples

Example 1.9.1. ***Cyclic group*** *C_n is the group with set $\{e, a, a^2, \ldots, a^{n-1}\}$, where $a^n = e$. It describes the discreet rotation in a plane. C_n is an abelian group.*

Example 1.9.2. ***Dihedral group*** *D_n is the group with set $\{e, a, a^2, \ldots, a^{n-1}, b, ab, a^2b, \ldots, a^{n-1}b\}$, where $a^n = b^2 = e$ and $ba = a^{-1}b$. It describes the discreet rotation in a plane together with mirror reflection. D_n is a non-abelian group when $n \geq 2$.*

Example 1.9.3. *Integers form a group under addition, called $\mathbb{Z}$.*

Example 1.9.4. *$\{0, \ldots, n-1\}$ form a group under addition mod n, called $\mathbb{Z}_n$. $\mathbb{Z}_n$ is isomorphic to C_n.*

Example 1.9.5. *$\mathbb{Z}_2$ is isomorphic to the group defined by the set $\{-1, 1\}$ under number multiplication. Sometimes we also call this group the* ***group of parity****.*

Example 1.9.6. *Units of quaternion $\{\pm 1, \pm i, \pm j, \pm k\}$ form a group, called the* ***quaternion group****. This is a non-Abelian group. The multiplication rule is*

$$i^2 = j^2 = k^2 = -1,\ ij = -ji = k,\ jk = -kj = i,\ ki = -ik = j \tag{1.25}$$

Example 1.9.7. *The $N \times N$ invertible matrices over a field $\mathbb{F}$ form a group under matrix multiplication. This is called* ***general linear group****, denoted by $GL(N, \mathbb{F})$. All elements in $GL(N, \mathbb{F})$ of determinate 1 form a group called* ***special linear group****, denoted by $SL(N, \mathbb{F})$.*

Example 1.9.8. *Let H be an $N \times N$ matrix over $\mathbb{F}$, and f be an anti-isomorphism from $GL(N, \mathbb{F})$ to itself. All matrices T of $GL(N, \mathbb{F})$ such that*

$$f(T)HT = H \tag{1.26}$$

form a group.

Definition 1.9.9. *A group is called* **simple** *if it has no non-void proper normal subgroup.*

Example 1.9.10. *All finite simple groups have been classified by mathematicians into four categories:*

1. *Cyclic group of prime order*
2. *Alternating group of degree* ≥ 5
3. *Simple group of Lie type*
4. *The 26 sporadic simple groups*

1.10 Permutation Group

As have defined, the permutation group of a set X is all bijective maps from X to itself under map composition.

Lemma 1.10.1. *If* $|X| = N$ *is finite, the permutation group of* X *is isomorphic to the permutation group of* $\{1, 2, \ldots, N\}$.

So in order to study the general permutation group, we only need to study S_N.

Definition 1.10.2. *For an element* f *of* S_N*, we may express* f *as*

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & N \\ f(1) & f(2) & f(3) & \cdots & f(N) \end{pmatrix} \tag{1.27}$$

Note that we don't require elements in the first row to be of ascending order.

Lemma 1.10.3.

$$\begin{pmatrix} 1 & 2 & \cdots & N \\ f(1) & f(2) & \cdots & f(N) \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & \cdots & N \\ g(1) & g(2) & \cdots & g(N) \end{pmatrix} = \begin{pmatrix} 1 & 2 & \cdots & N \\ f(g(1)) & f(g(2)) & \cdots & f(g(N)) \end{pmatrix} \tag{1.28}$$

$$\begin{pmatrix} 1 & 2 & \cdots & N \\ f(1) & f(2) & \cdots & f(N) \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & \cdots & N \\ f^{-1}(1) & f^{-1}(2) & \cdots & f^{-1}(N) \end{pmatrix} = \begin{pmatrix} f(1) & f(2) & \cdots & f(N) \\ 1 & 2 & \cdots & N \end{pmatrix} \tag{1.29}$$

1.10.1 Cycle Decomposition

Definition 1.10.4. *An element of the type*

$$\begin{pmatrix} i_1 & i_2 & \cdots & i_m & a & b & \cdots \\ i_2 & i_3 & \cdots & i_1 & a & b & \cdots \end{pmatrix} \tag{1.30}$$

is called an ***m-cycle****, denoted by* $C = (i_1, i_2, \ldots, i_m)$*. It's length is defined as* $|C| = m$*. A cycle of length 2 is called a* ***transposition****.*

Lemma 1.10.5. $(i_1, \ldots, i_n) = (i_1, i_n) \circ \cdots \circ (i_1, i_2)$.

Definition 1.10.6. *We say two cycles $(i_1, \ldots, i_m)$ and $(j_1, \ldots, j_t)$ are disjoint if $\{i_1, \ldots, i_m\}$ and $\{j_1, \ldots, j_t\}$ are disjoint.*

Lemma 1.10.7. *Two disjoint cycles commutes.*

Lemma 1.10.8. *Each $f \in S_N$ is a product of disjoint cycles. The product is unique for each element if the omit the difference on the order of the production.*

Proof. For each $f \in S_N$, let $\{O_i\}$ be the orbits of $\langle f \rangle$. If $|O_i| = m$ and $a \in O_i$. Then $O_i = \{f^n(a) | n = 0, \ldots, m-1\}$ and $f^{(m)}(a) = a$. We define a cycle for each O_i as $C_i = (a, f(a), \ldots, f^{(m-1)}(a))$. C_is are mutually disjoint, and $f = \prod_i C_i$. □

Definition 1.10.9. *For $g \in S_N$, we have cycle decomposition $g = C_1 \cdots C_p$, rearranged so that $|C_1| < \cdots < |C_p|$. Then we define $(|C_1|, \ldots, |C_p|)$ as the cycle type of g.*

Theorem 1.10.10. *The conjugacy class of S_N are elements of the same cycle type.*

1.10.2 Sign Function

Definition 1.10.11. *Let f be a permutation on $\{1, \ldots, N\}$ with cycle type $(|C_1|, \ldots, |C_p|)$. We define the* **sign** *of f as*

$$\operatorname{sgn}(f) = \prod_i (-1)^{|C_i|+1} = (-1)^{N+p} \tag{1.31}$$

Especially $\operatorname{sgn}(e) = 1$.

Lemma 1.10.12. $\operatorname{sgn}((ab) \circ g) = -\operatorname{sgn}(g)$

Proof.

$$\begin{aligned} (ab)(a, c_1, \ldots, c_n, b, d_1, \ldots, d_m) &= (a, c_1, \ldots, c_n)(b, d_1, \ldots, d_m) && (1.32) \\ (ab)(a, c_1, \ldots, c_n)(b, d_1, \ldots, d_m) &= (a, c_1, \ldots, c_n, b, d_1, \ldots, d_m) && (1.33) \end{aligned}$$

□

Lemma 1.10.13. *Each element of S_N can be decomposed into product of transpositions.*

Proof. Each element can be decomposed into cycles and each cycles can be decomposed into transpositions. □

Lemma 1.10.14. *Suppose we can write f as*

$$f = \prod_{i=1}^{m} S_i \tag{1.34}$$

where S_i are transpositions.

Then $\operatorname{sgn}(f) = (-1)^m$. *This means that each element can only be decomposed into a product of even number of transpositions if is sign is 1, and odd if -1.*

Proof.

$$\prod_{i=m}^{1} S_i f = e \tag{1.35}$$

Then

$$\mathrm{sgn}\Big(\prod_{i=m}^{1} S_i f\Big) = (-1)^m \mathrm{sgn}(f) = 1 \tag{1.36}$$

□

Lemma 1.10.15. *sgn is a homomorphism from S_N to $\mathbb{Z}_2$.*

Proof. To prove $\mathrm{sgn}(f \circ g) = \mathrm{sgn}(f) \cdot \mathrm{sgn}(g)$, decompose f into product of transpositions. □

1.11 Alternating Group

Definition 1.11.1. *The kernel of sgn forms a subgroup of S_N, called the **alternating group**, denoted by A_N.*

Theorem 1.11.2. *Let $g \in A_N \subseteq S_N$. $g \in C_A$ is a conjugacy class of A_N, and $g \in C_S$ is a conjugacy class of S_N. It's easy to see that $C_A \subseteq C_S \subseteq A_N$ and $C_{A_N}(g) = C_{S_N}(g) \cap A_N$. If $C_{S_N}(g) \subseteq A_N$, then $|C_A| = |C_S|/2$. Otherwise, $|C_A| = |C_S|$.*

Proof.

$$[C_{S_N}(g) : C_{A_N}(g)] = \frac{|C_{S_N}(g)|}{|C_{A_N}(g)|} = \frac{|S_N|/|C_S|}{|A_N|/|C_A|} = 2|C_A|/|C_S| = 1 \text{ or } 2 \tag{1.37}$$

$$|C_A| = |C_S|/2 \Leftrightarrow [C_{S_N}(g) : C_{A_N}(g)] = 1 \Leftrightarrow C_{S_N}(g) = C_{A_N}(g) \Leftrightarrow C_{S_N}(g) \subseteq A_N \tag{1.38}$$

□

Theorem 1.11.3. *Let $g \in A_N \subseteq S_N$. We have $C_{S_N}(g) \subseteq A_N$ iff the cycle decomposition of g contains cycles of distinct odd length.*

Proof. Let $g = \prod_i c_i$ is the cycle decomposition. If $\exists c_i$ of even length, then $c_i \in C_{S_N}(g) - A_N$. If $\exists c_i, c_j$ of same odd length. Let $c_i = (a_1, \ldots, a_n)$ and $c_j = (b_1, \ldots, b_n)$. Then $(a_1 b_1) \cdots (a_n, b_n) \in C_{S_N}(g) - A_N$. If $\{c_i\}$ are cycles of distinct odd length. Then $h \in C_{S_N}(g) \Rightarrow h = \prod_i c_i^{n_i} \Rightarrow h \in A_N$. □

Theorem 1.11.4. *Let C be a conjugacy class of S_N and $C \in A_N$. If the cycle decomposition of C contains cycles of distinct odd length, then C splits into two conjugacy class of A_N of the same size. Otherwise, C is a conjugacy class of A_N.*

Lemma 1.11.5. *Each element of A_N can be decomposed into product of 3-cycles.*

Proof. $(a, b) = (1, a)(1, b)(1, a)$ and $(1, a)(1, b) = (1, b, a)$. □

1.11.1 Simplicity of A_n

Lemma 1.11.6. *A_4 is not simple*

Proof. A normal subgroup is $\{(1,2)(3,4),(1,3)(2,4),(1,4)(2,3),(1)(2)(3)(4)\}$. □

Lemma 1.11.7. *A_5 is simple.*

Proof. The conjugacy classes of A_5 are: (5) with 12 elements, (5) with 12 elements, $(3,1,1)$ with 20 elements, $(2,2,1)$ with 15 elements and $(1,1,1,1,1)$ with 1 element.

Any normal subgroup of A_5 must be a union if conjugacy classes. □

Lemma 1.11.8. *Let H be a normal subgroup of $A_n (n \geq 5)$. If H contains a 3-cycle, then $H = A_n$.*

Proof. Any two 3-cycles are conjugated in $A_n (n \geq 5)$, since the cycle decomposition of a 3-cycle is $(1,\dots,1,3)$. □

Lemma 1.11.9. *Let H be a normal subgroup of G, and K be a simple subgroup of G. Then $K \subseteq H$ or $H \cap K = 1$.*

Proof. $H \cap K$ is a normal subgroup of K. □

Lemma 1.11.10. *$A_n (n \geq 5)$ is simple.*

Proof. Suppose $n > 5$. Let H be a nontrival normal subgroup of A_n. Let $\alpha \in H$ be an element that move i to j. Let β be a 3-cycle that fixes i and moves j. It's easy to see that $\alpha\beta \neq \beta\alpha$. Let $a = \beta\alpha\beta^{-1}\alpha^{-1}$. Clearly $a = (\beta\alpha\beta^{-1})\alpha^{-1} \in H$, and $a = \beta(\alpha\beta^{-1}\alpha^{-1})$ is a product of 2 3-cycles. So a moves at most 6 elements.

If a moves 6 elements (in this case $n \geq 6$), a has the cycle type $(3,3,1,\dots)$. Since elements with cycle type $(3,3,1,\dots)$ form a unique conjugacy class, $(123)(456)$ and $(654)(123) \in H$. So $(132) \in H$. So $H = A_n$.

Otherwise a moves at most 5 elements. Let A_5 be the subgroup of A_n that moves these 5 elements. Then $H \cap A_5 \neq 1$. So $A_5 \subseteq H$. So H contains a 3-cycle. So $H = A_n$. □

1.12 Sylow's Theorems

Definition 1.12.1. *Let p be a prime number. By a* **p-group***, we mean a group of order p^n.*

Let G be a finite group. We call a subgroup of G that is a p-group a **p-subgroup***.*

Let H be a p-subgroup of G and $|H| = p^m$. We call H **p-Sylow subgroup** *if p^m is the highest power of p that divides $|G|$.*

Lemma 1.12.2. *Let G be a finite abelian group, and let p be a prime number dividing $|G|$. Then G has an element of order p.*

Proof. We prove this by induction on $|G|$. The lemma certainly holds for $|G| = 1$.

When $|G| > 1$, we choose $g \in G$ of order $m > 1$. If $p|m$, then $g^{m/p}$ is of order p. If $p \not| m$, $p \big| |G/(g)|$. Since $|G/(g)| < |G|$, we have an element $(h) \in G/(g)$ of order p. Let $h \in G$ be of order n. Then $(h)^n = (1)$. So $p|n$. Then $h^{n/p}$ is of order p. □

Theorem 1.12.3 (Sylow I)**.** *If p is a prime number and $p^k \big| |G|$. Then G contains a subgroup of order p^k.*

Proof. We prove this by induction on $|G|$. The theorem certainly holds for $|G| = 1$.

When $|G| > 1$, we have the class equation

$$|G| = |Z(G)| + \sum_i [G : C(x_i)] \tag{1.39}$$

If $p \not| |Z(G)|$, $\exists i : p \not| [G : C(x_i)]$. So $p^k | C(x_i)$ and $|C(x_i)| < |G|$. So $C(x_i)$ contains a subgroup of order p^k. If $p \big| |Z(G)|$, from the lemma, $\exists g \in Z(G)$ of order p. So $p^{k-1} \big| |G/(g)|$. Since $|G/(g)| < |G|$ and (g) is normal, $\exists H/(g)$ of order p^{k-1}, and H is of order p^k. □

Lemma 1.12.4. *Let P be a Sylow p-subgroup of G, and H a subgroup of order p^k contained in $N_G(P)$. Then $H \subseteq P$.*

Proof. Since P is normal subgroup of $N_G(P)$, HP is a subgroup of G and $HP/P \simeq H/(H \cap P)$. So $|HP/P| = |H/(H \cap P)| = p^s$. So $|HP| = p^s |P|$. Since P is a Sylow p-subgroup, $|HP| = |P|$. So $HP = P$. So $H \subseteq P$. □

Lemma 1.12.5. *Let H be a p-group acting on a finite set S. Then the number of fixed points of $H \equiv |S| \mod p$.*

Theorem 1.12.6 (Sylow II)**.** *1. Any two Sylow p-subgroups of G are conjugate in G*

2. The number of Sylow p-subgroups divides the index of any Sylow p-subgroups, and $\equiv 1 \mod p$.

3. Any p-subgroup is contained in a Sylow p-subgroup.

Proof. Let Π be the set of all Sylow p-subgroups. For each p-subgroup $P \in \Pi$, P acts on Π by conjugation. Let P' be a fixed point of the action. Then $P \subseteq N_G(P') \Rightarrow P = P'$. So P is the only fixed point. Let O be an orbit in Π. From (1.12.5), $|O| \equiv 1 \mod p$ if $P \in O$, and $|O| \equiv 0 \mod p$ if $P \notin O$. Since this holds for any $P \in \Pi$, Π is the only orbit. So $|\Pi| \equiv 1 \mod p$. Since G acts transively on $|\Pi|$ by conjugation, we have $|\Pi| = [G : N_G(P)]$. So $|\Pi| \big| [G : P]$.

Let H be a p-subgroup of order $p^k (k > 0)$. H acts on Π by conjugation. Since $|\Pi| \equiv 1 \mod p$, H-action has at least one fixed point, say P_0. Then $H \subseteq N_G(P_0)$. So by the lemma (1.12.4), $H \subseteq P_0$. □

Corollary 1.12.7. *Let G be a group and N a normal subgroup of G. If P is a Sylow p-subgroup of N then $G = N_G(P)N$.*

Proof. $\forall g \in G$, gPg^{-1} is a Sylow p-subgroup of N. So by Sylow II, $\exists n \in N$ such that $gPg^{-1} = nPn^{-1}$. So $g^{-1}n \in N_G(P)$. □

1.13 Solvability and Nilpotenty

Definition 1.13.1. *Let G be a finite group. G is said to be* **solvable** *if there exist a series $\{G_0, \ldots, G_n\}$ of normal subgroups of G such that*

$$1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G \tag{1.40}$$

and G_{i+1}/G_i is abelian.

Theorem 1.13.2. *Let H be a normal subgroup of G. G is solvable iff H and G/H are solvable.*

Theorem 1.13.3. *Let p be a prime number. p-group is solvable.*

Proof. Let G be a p-group of order $p^k (k > 1)$. We prove by induction on k. If $k = 1$, G is cyclic and thus solvable. If $k > 1$, we have class equation

$$|G| = |Z(G)| + \sum_i [G : C(x_i)] \tag{1.41}$$

Clearly $p \big| |Z(G)|$. So $C(G)$ is non-trivial. If $Z(G) = G$, clearly G is solvable. Otherwise $Z(G)$ is a normal subgroup of G and by induction $Z(G)$ and $G/Z(G)$ are solvable. So G is solvable. □

Theorem 1.13.4. *Let p and q be distinct prime numbers. A group of order pq is solvable.*

Proof. Let G be a group of order pq. Let's assume $p < q$. Let N_q be number of q-Sylow subgroups. By Sylow theorem, we have $N_q | p$ and $N_q \equiv 1 \mod q$. So $N_q = 1$. So there's only one q-Sylow subgroup and it's normal and solvable. Let it be H. G/H is cyclic and thus solvable. So G is solvable. □

Definition 1.13.5. *Let G be a finite group. G is said to be* **nilpotent** *if there exist a series $\{G_0, \ldots, G_n\}$ of normal subgroups of G such that*

$$1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G \tag{1.42}$$

and $G_{i+1}/G_i = Z(G/G_i)$.

Theorem 1.13.6. *A nilpotent group is solvable.*

Chapter 2

Mathieu Groups

2.1 Block System

Definition 2.1.1. *Let G be a group that acts on a set S transitively. A* **block system** *is a partition Π of S such that $\forall B \in \Pi \forall g \in G : gB \in \Pi$. Each $B \in S$ is called a* **block** *if it's in some block system.*

A block system is a coarse-grained action.

Lemma 2.1.2. *Let G be a group that acts on a set S transitively. Let Π be a block system of S. For each $B \in \Pi$, $\Pi = \{gB | g \in G\}$. So Π is uniquely determined by one of its element.*

Lemma 2.1.3. *Let G be a group that acts on a set S transitively. $B \subseteq S$ is a block if $\forall g \in G : gB = B \vee gB \cap B = \emptyset$.*

Lemma 2.1.4. *Non-empty intersection of blocks is a block.*

Definition 2.1.5. *Let G be a group that acts on X transitively. Let Π be a block system of S. For each $B \in \Pi$, the* **stabilizer** *of B is defined as $S_B = \{g \in G | gB = B\}$. Clearly $x \in B \Rightarrow S_x$ is a subgroup of S_B.*

There's an isomorphism between the action on the left cosets and the action on the block system.

Definition 2.1.6. *A transitive action is called* **primitive** *iff it contains no non-trivial block system*

Definition 2.1.7. *Let G be a group that acts on X transitively. The action is called* **maximal** *iff each S_x is maximal.*

Lemma 2.1.8. *Let G be a group that acts on a set X transitively. For each $x \in X$, there's 1-1 correspondence between non-trivial subgroup containing S_x (H such that $G \supsetneq H \supsetneq S_x$) and a non-trivial block containing x (a block that's not $\{x\}$ or S).*

Proof. For each H such that $G \supsetneq H \supsetneq S_x$, we define $f(H)$ by $\{Hx\}$. It's easy to see that f is injective. For each non-trivial block $B \ni x$, let $H_B = \{g \in G | gx \in B\}$. It's easy to see that H_B is a non-trivial subgroup containing S_x and $f(H_B) = B$. So f is surjective. □

Corollary 2.1.9. *Let $(G, X, \circ)$ be a transitive action. The action is primitive iff it's maximal.*

Lemma 2.1.10. *Let $(G, X, \circ)$ be a primitive action. Let $H \neq 1$ be a normal subgroup of G. Then H acts transitively on X.*

Proof. For each x, $Hx = HS_x x = Gx = X$. □

2.2 Multiple transitivity

Definition 2.2.1. *Let $(G, S, \circ)$ be an action. Let $\Delta(S^n) = \{(s_1, \ldots, s_n) | s_i \in S, s_1 \neq \cdots \neq s_n\}$. We have a natural action $(G, \Delta(S^n), \circ)$ defined by $g \circ (s_1, \cdots, s_n) = (g \circ s_1, \cdots, g \circ s_n)$. The action $(G, S, \circ)$ is called* **n-transitive** *if the action $(G, \Delta(S^n), \circ)$ is transitive.*

Lemma 2.2.2. *Let $(G, S, \circ)$ be an action. If the action is k-transitive, then the action is n-transitive for any $n \leq k$.*

Lemma 2.2.3. *Let $(G, S, \circ)$ be an action. Then the action is k-transitive iff S_x acts on $(X - \{x\})$ $(k-1)$-transitively for each $x \in X$.*

Lemma 2.2.4. *A 2-transitive action is primitive.*

Proof. There's no non-trivial block. □

Definition 2.2.5. *Let $(G, S, \circ)$ be an action. $(G, S, \circ)$ is called* **sharply n-transitive** *if the action $(G, \Delta(S^n), \circ)$ satisfied that $\forall (s_1, \ldots, s_n) \in \Delta(S^n) : S_{(s_1, \ldots, s_n)} = 1$.*

Lemma 2.2.6. *Let $(G, S, \circ)$ be an action. Then the action is sharply k-transitive iff S_x acts on $(X - \{x\})$ sharply $(k-1)$-transitively for each $x \in X$.*

Lemma 2.2.7. *S_n acts sharply n-transitively on $\{1, \ldots, n\}$ for every n. A_n acts sharply $(n-2)$-transitively on $\{1, \ldots, n\}$ for every $n \geq 3$.*

Definition 2.2.8. *A sharply 1-transitive action is called* **regular**.

Lemma 2.2.9. *A sharply n-transitively is faithful.*

2.3 Affine Geometry

Definition 2.3.1. *A set A is an n-dimensional* **affine space** *if there's a map $\rightarrow$: $A \times A \mapsto K^n$ (n-dimension linear space over the field K) such that*

1. *For each $x \in A$, the partial map $y \mapsto \overrightarrow{xy}$ is a bijection from A to K^n.*
2. *For each $x, y, z \in A$, $\overrightarrow{xy} + \overrightarrow{yz} = \overrightarrow{xz}$.*

Definition 2.3.2. *Let V be an n-dimensional linear space. For each m-dimensional subspace $S \subseteq V$ and each $v \in V$, $S + v$ is called an m-dimensional* **affine subspace** *of V.*

Clearly an m-dimensional affine subspace of V is an affine space by defining $\overrightarrow{xy} = y - x$.

Definition 2.3.3. *Let U and V be n-dimensional linear spaces. A bijective map $f : U \mapsto V$ is an* **affine isomorphism** *iff $\forall S \subseteq U, f(S)$ an affine subspace of $V \Leftrightarrow S$ is an affine subspace of U.*

Definition 2.3.4. *Let V be a linear space. The affine automorphisms of V is denoted by $Aut(V)$.*

Definition 2.3.5. *Let V and V' be vector spaces over K. A function $f : V \mapsto V'$ is a* **semilinear transformation** *if there's $\sigma \in Aut(K)$ such that $\forall x, y \in V, \forall \lambda \in K$*

$$f(x+y) = f(x) + f(y) \tag{2.1}$$
$$f(\lambda x) = \sigma(\lambda)x \tag{2.2}$$

A semilinear transformation is nonsingular if it is a bijection. All semilinear transformations on a linear space V form a group denoted by $\Gamma L(V)$.

To be continued.

Chapter 3

Linear Representation of Finite Group

Definition 3.0.1. *A **linear representation** of a group G is a homomorphism T from G to general linear group of V. For our purpose, we require V to be a finite dimensional complex linear space.*

Example 3.0.2. *Obviously $T(g) = id$ is a representation, called the **identity representation**.*

Definition 3.0.3. *Two linear representations are said **equivalent** if they are related by a similar transformation, that is*

$$T_1 \sim T_2 \iff T_1 = ST_2S^{-1} \tag{3.1}$$

Lemma 3.0.4. *Each linear representations is a unitary representations relative to some inner product.*

Proof. From an arbitrary inner product H_0 on V, we can define a new inner product

$$H(u, v) = \sum_{g \in G} H_0(T(g)u, T(g)v) \tag{3.2}$$

It's easy to see that H is an inner product and $\forall g \in G : H(u, v) = H(T(g)u, T(g)v)$.

Thus $T(g)$s are isometries with respect to H, and thus unitary. This means we can always find an inner product such that $T(g)$s are unitary. □

We'll use this inner product from now on.

3.1 Reducibility

Definition 3.1.1. *A set of operators $T_i : V \mapsto V$ is said to be* **reducible** *if it has a non-trival proper invariant subspace of V. That is*

$$\exists 0 \neq V_0 \subsetneq V \ \forall i : T_iV_0 \subset V_0 \tag{3.3}$$

Lemma 3.1.2. *Let T be a non-singular operator. Then $TV_0 \subset V_0 \iff TV_0 = V_0$.*

Definition 3.1.3. *A set of unitary operators T_i is called* **completely reducible** *if we can divide V into $V_1 \oplus V_2$ such that*

$$\forall i : T_i V_1 \subset V_1 \wedge T_i V_2 \subset V_2 \tag{3.4}$$

From the lemma above, that means

$$\forall i : T_i V_1 = V_1 \wedge T_i V_2 = V_2 \tag{3.5}$$

Theorem 3.1.4. *If a set of unitary operators is reducible, then it is completely reducible.*

Proof. If T_i is reducible with a proper invariant subspace V_0, then

$$V = V_0 \oplus V_0^{\perp} \tag{3.6}$$

Since T_i is an isometry,

$$\forall i : T_i V_0^{\perp} \perp T_i V_0 = V_0 \tag{3.7}$$

Thus for all i, $T_i V_0^{\perp} \subset V_0^{\perp}$, and thus $T_i V_0^{\perp} = V_0^{\perp}$.
Thus T_i is completely reducible. □

Definition 3.1.5. *A representation of a group G is (completely) reducible iff the set $\{T(g)|g \in G\}$ is (completely) reducible.*

Lemma 3.1.6. *A representation of a group G is completely reducible if its reducible.*

For a set of unitary operators T_i on V. If T_i is reducible, we can reduce it into $V = V_1 \oplus V_2$. Then we consider $T_i|_{V_1}$ and $T_i|_{V_2}$. If $T_i|_{V_1}$ is reducible, we can reduce it into $V_1 = V_{1,1} \oplus V_{1,2}$ …We continue this procedure until we decompose V into $V_1 \oplus \cdots \oplus V_n$ such that $T_i|_{V_j}$ is irreducible. This is called the reduction of a set of unitary operators. As we have shown, we can choose V_1 …V_n so they are mutually orthogonal. (This can be strictly proved by induction on the dimension of V)

Lemma 3.1.7. *If $T(g)$ is irreducible, then so is $T^{\dagger}(g)$.*

Proof. $T^{\dagger}(g)$ is also unitary. If it's reducible, then it's completely reducible, which leads to the reducibility of $T(g)$. □

3.2 Schur's Lemma

Lemma 3.2.1 (Schur)**.** *If $T(g)$ is an irreducible representation of group G over linear space V. P is any linear transformation over V and*

$$\forall g : T(g)P = PT(g) \tag{3.8}$$

then $P = \lambda I$.

Proof. Define $P_\lambda = P - \lambda I$. Since $\det P_\lambda = \det(P - \lambda I)$ always has a root in $\mathbb{C}$, we can choose λ so that P_λ is singular.

Obviously we also have

$$\forall g : T(g)P_\lambda = P_\lambda T(g) \tag{3.9}$$

Thus

$$\forall g : T(g)P_\lambda V = P_\lambda T(g)V = P_\lambda V \tag{3.10}$$

Thus $P_\lambda V$ is an invariant subspace.

Since $T(g)$ is irreducible, $P_\lambda V = V$ or $\emptyset$.

Since P_λ is singular, $P_\lambda V = \emptyset$. Thus $P_\lambda = 0$, $P = \lambda I$ □

Corollary 3.2.2. *Abelian groups only have 1-D irreducible representations.*

Lemma 3.2.3 (Schur)**.** *If $T(g)$ and $T'(g)$ are two inequivalent irreducible representations of group G over linear space V and V'. P is any linear transformation from V' to V and*

$$\forall g : T(g)P = PT'(g) \tag{3.11}$$

then $P = 0$.

Proof. Choose any inner products over V and V'. Assume $P \neq 0$, thus $P^\dagger \neq 0$.

$$\forall g : T(g)PV' = PT'(g)V' = PV' \tag{3.12}$$

And

$$\forall g : P^\dagger T^\dagger(g) = T'^\dagger(g)P^\dagger \tag{3.13}$$

thus

$$\forall g : T'^\dagger(g)P^\dagger V = P^\dagger T^\dagger(g)V = P^\dagger V \tag{3.14}$$

Since $T(g)$ and $T'^\dagger(g)$ are both irreducible, if $P \neq 0$, $PV' = V$ and $P^\dagger V = V'$.

This means that P is invertible, thus

$$\forall g : P^{-1}T(g)P = T'(g) \tag{3.15}$$

and $T(g)$ and $T'(g)$ are equivalent. This is a contradiction.

Thus $P = 0$. □

Theorem 3.2.4 (Wigner,Eckart)**.** *If $D(g)$ is a unitary group representation over a complex linear space.*

We have an orthonormal basis $|a, j, x\rangle$ such that

$$\langle a, j, x|D(g)|b, k, y\rangle = \delta_{ab}\delta_{xy}[D^a(g)]_{jk} \tag{3.16}$$

where a labels different irreducible representations, j labels the representation indices, and x labels equivalent representations.

If D is a symmetry for the operator O, that is

$$D(g)OD(g)^\dagger = O \Rightarrow [O, D(g)] = 0 \tag{3.17}$$

Then

$$\langle a, j, x|O|b, k, y\rangle = O(a)_{xy}\delta_{ab}\delta_{jk} \tag{3.18}$$

Proof.

$$\begin{aligned} 0 &= \langle a,j,x|[O,D(g)]|b,k,y\rangle && (3.19)\\ &= \langle a,j,x|O|c,l,z\rangle\langle c,l,z|D(g)|b,k,y\rangle - \langle a,j,x|D(g)|c,l,z\rangle\langle c,l,z|O|b,k,y\rangle && (3.20)\\ &= \langle a,j,x|O|b,l,y\rangle[D^a(g)]_{lk} - [D^a(g)]_{jl}\langle a,l,x|O|b,k,y\rangle && (3.21)\end{aligned}$$

Use Schur's lemma. □

When considering the set of all inequivalent irreducible representations, we use a superscript to distinguish among them, such as T^a

Lemma 3.2.5. *In matrix form, we have the* ***orthogonality relation***

$$\begin{aligned} \frac{1}{|G|}\sum_g T^{a\dagger}_{si}(g)\delta_{il}\delta_{jm}T^b_{jt}(g) &= \frac{\delta_{lm}}{d_a}\delta_{ab}\delta_{st} && (3.22)\\ \frac{d_a}{|G|}\sum_g T^{a*}_{ls}(g)T^b_{mt}(g) &= \delta_{ab}\delta_{lm}\delta_{st} && (3.23)\end{aligned}$$

Proof. For two irreducible representations T^a and T^b and any map D from V^b to V^a, since

$$\begin{aligned} \big(\sum_g T^{a\dagger}(g)DT^b(g)\big)T^b(g') &= \sum_g T^{a\dagger}(g)DT^b(g\circ g') && (3.24)\\ &= \sum_g T^{a\dagger}(g\circ g'^{-1})DT^b(g) && (3.25)\\ &= T^a(g')\sum_g T^{a\dagger}(g)DT^b(g) && (3.26)\end{aligned}$$

From Schur's lemma, we have

$$\frac{1}{|G|}\sum_g T^{a\dagger}(g)DT^b(g) = \lambda\delta_{ab}I \tag{3.27}$$

By taking trace on both sides, we know if $a=b$, $\lambda = \frac{\mathrm{Tr}[D]}{d_a}$, where d_a is the dimension of T^a.
In matrix form, choose D_{ij} to be $\delta_{il}\delta_{jm}$. We have the orthogonality relation. □

3.3 Regular Representation

Definition 3.3.1. *We define the* **group space** *as a vector space of $|G|$ dimension, where each basis vector corresponds to an element of G. That is, we can express a basis as $\vec{g}$.*

Example 3.3.2. *Then we have two natural representation of G on the group space called* ***left/right regular representation****. The left regular representation is defined by*

$$L(g')c_g\vec{g} = c_g\overrightarrow{g'\circ g} \tag{3.28}$$

and the right regular representation is defined by

$$R(g')c_g\overrightarrow{g} = c_g\overrightarrow{g \circ g'^{-1}} \tag{3.29}$$

We define the inner product in the group space as

$$(\overrightarrow{h}, \overrightarrow{g}) = \delta_{gh} \tag{3.30}$$

Both regular representations are unitary under this inner product.

We define $\overrightarrow{T^a_{ij}}$ *as*

$$\overrightarrow{T^a_{ij}} = \sum_g T^a_{ij}(g)\overrightarrow{g} \tag{3.31}$$

Then

$$\left(\overrightarrow{T^b_{kl}}, \overrightarrow{T^a_{ij}}\right) = \sum_g T^{b*}_{kl}(g)T^a_{ij}(g) = \frac{|G|}{d_a}\delta_{ab}\delta_{ik}\delta_{jl} \tag{3.32}$$

So $\overrightarrow{T^a_{ij}}s$ *are orthogonal for different* (a, i, j).

We have

$$\begin{aligned} R(g)\overrightarrow{T^a_{ij}} &= \sum_h T^a_{ij}(h)\overrightarrow{h \circ g^{-1}} && (3.33)\\ &= \sum_h T^a_{ij}(h \circ g)\overrightarrow{h} && (3.34)\\ &= T^a_{kj}(g)\overrightarrow{T^a_{ik}} && (3.35) \end{aligned}$$

So that $\overrightarrow{T^a_{ij}}s$ *(a and i fixed) form an invariant subspace, in which* $R(g)$ *transforms like* T^a.

Similarly

$$L(g)\overrightarrow{T^a_{ij}} = T^{a\dagger}_{ik}(g)\overrightarrow{T^a_{kj}} \tag{3.36}$$

Next we prove that $\overrightarrow{T^a_{ij}}s$ *are complete.*

For an arbitrary vector $\overrightarrow{v}$, *we have* $\overrightarrow{v} = \sum \overrightarrow{v_a}$ *such that each* $\overrightarrow{v_a}$ *is in* V_a, *an irreducible subspace of* $R(g)$. *Thus* $R|_{V_a}$ *is similar to some irreducible representation, say* T^a. *Then we can find a basis* $\overrightarrow{e_i}$ *on* V_i *such that*

$$R(g)\overrightarrow{e_j} = T^a_{ij}(g)\overrightarrow{e_i} \tag{3.37}$$

We may expand $\overrightarrow{e_j}$ *as* $\sum_h e_{jh}\overrightarrow{h}$ *where* $h \in G$, *we have*

$$\sum_h e_{jh}\overrightarrow{h \circ g^{-1}} = \sum_h T^a_{ij}(g)e_{jh}\overrightarrow{h} \tag{3.38}$$

Compare the coefficient on both sides, we have

$$\begin{aligned} \forall h, g &: e_{j(h\circ g)} = T^a_{ij}(g)e_{ih} && (3.39)\\ \forall g &: e_{jg} = T^a_{ij}(g)e_{ie} && (3.40) \end{aligned}$$

Thus

$$\vec{e_j} = \sum_h e_{jg}\vec{g} = \sum_h T^a_{ij}(g)e_{ie}\vec{g} = e_{ie}\overrightarrow{T^a_{ij}} \tag{3.41}$$

Thus

$$\vec{v}_a = v_j\vec{e_j} = v_j e_{ie}\overrightarrow{T^a_{ij}} \tag{3.42}$$

Such each $\vec{v_a}$ can be expand by $\overrightarrow{T^a_{ij}}$s. Such each $\vec{v}$ can be expand by $\overrightarrow{T^a_{ij}}$s.

Thus $\overrightarrow{T^a_{ij}}$s form a orthogonal complete basis. And clearly the right regular representation can be reduced into

$$R = \bigoplus_a (T^a)^{\oplus d_a} \tag{3.43}$$

Counting the dimension of both sides, we have

Theorem 3.3.3 (Burnside)**.** $|G| = \sum_a d_a^2$

3.4 Characters

Definition 3.4.1. ***Characters*** *of a group representation T are defined as*

$$\chi(g) = \mathrm{Tr}[T(g)] \tag{3.44}$$

Lemma 3.4.2. *If g is conjugate to g', then $\chi(g) = \chi(g')$. Thus $\chi(g)$ is a function of conjugate class, thus we sometime write $\chi(C_i)$ where C_i is the i-th conjugate class.*

As before, we define χ^a for each inequivalent irreducible representation T^a.

Lemma 3.4.3. *We have the orthogonality relation for characters*

$$\frac{1}{|G|}\sum_g \chi^{a*}(g)\chi^b(g) = \delta_{ab} \tag{3.45}$$

or

$$\sum_i |C_i|\chi^{a*}(C_i)\chi^b(C_i) = |G|\delta_{ab} \tag{3.46}$$

Proof. Taking traces on both sides of Eqn. 3.23. □

Definition 3.4.4. *We define the* **class space** *as the subspace of group space that contains all vector $|v\rangle$ such that*

$$\forall g : R(g)L(g)\vec{v} = \vec{v} \tag{3.47}$$

Lemma 3.4.5. *For each character χ we define the corresponding vector in the group space as*

$$\vec{\chi} = \chi(g)\vec{g} \tag{3.48}$$

$\vec{\chi}$ is contained in the class space.

Lemma 3.4.6. *$\overrightarrow{\chi^a}$s for characters of irreducible representations form an orthogonal complete basis*

Proof. We have

$$(\overrightarrow{\chi^a}, \overrightarrow{\chi^b}) = \sum_g \chi^{a*}(g)\chi^b(g) = |G|\delta_{ab} \tag{3.49}$$

Thus $\overrightarrow{\chi^a}$s are orthogonal to each other.
For each $\vec{v}$ is the class space, we can expand $\vec{v}$ over $\overrightarrow{T^a_{ij}}$ as

$$\vec{v} = \sum_a v^a_{ji}\overrightarrow{T^a_{ij}} \tag{3.50}$$

We have

$$\begin{aligned} R(g)L(g)\vec{v} &= \sum_a R(g)L(g)v^a_{ji}\overrightarrow{T^a_{ij}} && (3.51)\\ &= \sum_a T^a_{lj}(g)T^{a\dagger}_{ik}(g)v^a_{ji}\overrightarrow{T^a_{kl}} && (3.52)\\ &= \vec{v} = \sum_a v^a_{lk}\overrightarrow{T^a_{kl}} && (3.53) \end{aligned}$$

Thus

$$\begin{aligned} T^a_{lj}(g)T^{a\dagger}_{ik}(g)v^a_{ji} &= v^a_{lk} && (3.54)\\ T^a_{lj}(g)v^a_{ji} &= T^a_{ki}(g)v^a_{lk} && (3.55) \end{aligned}$$

From Schur's lemma, we have

$$v^a_{ij} = v^a\delta_{ij} \tag{3.56}$$

Thus

$$\vec{v} = \sum_a v^a\delta_{ij}\overrightarrow{T^a_{ij}} = \sum_a v^a\overrightarrow{\chi^a} \tag{3.57}$$

Thus $\overrightarrow{\chi^a}$s form an orthogonal complete basis over the class space. □

Lemma 3.4.7. *If the representation T can be reduced into $T^a \oplus \cdots \oplus T^z$, then its character $\chi(g) = \chi^a(g) + \cdots + \chi^z(g)$. Thus $\overrightarrow{\chi} = \overrightarrow{\chi^a} + \cdots + \overrightarrow{\chi^z}$. The expansion coefficients of $\overrightarrow{\chi}$ over $\overrightarrow{\chi^a}$s are integers and just means the recurrence of different irreducible representations where T is reduced.*

Proof.

$$\begin{aligned} \chi(g) &= \mathrm{Tr}[T(g)] && (3.58)\\ &= \mathrm{Tr}\left[\begin{pmatrix} T^a(g) & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & T^z(g) \end{pmatrix}\right] && (3.59)\\ &= \mathrm{Tr}[T^a(g)] + \cdots + \mathrm{Tr}[T^z(g)] && (3.60)\\ &= \chi^a(g) + \cdots + \chi^z(g) && (3.61) \end{aligned}$$

□

Lemma 3.4.8. *For each conjugate class C_i of G, we construct a vector*

$$\overrightarrow{C_i} = \sum_{g \in C_i} \overrightarrow{g} \tag{3.62}$$

$\overrightarrow{C_i}s$ is an orthogonal complete basis of the class space.

Corollary 3.4.9. *The dimension of the class space is the number of inequivalent irreducible representations, and is also the number of conjugate classes.*

Lemma 3.4.10. *We have the second orthogonality relation*

$$\sum_a |C_i| \chi^{a*}(C_i) \chi^a(C_j) = |G| \delta_{ij} \tag{3.63}$$

Proof. We define a matrix Γ as

$$\Gamma_{ij} = \sqrt{\frac{|C_j|}{|G|}} \chi^i(C_j) \tag{3.64}$$

From the arguments above we know that Γ is a square matrix. And the orthogonality relation tell us that $\Gamma\Gamma^\dagger = I$. Thus $\Gamma^\dagger\Gamma = I$. □

3.5 Group Algebra

Definition 3.5.1. *We define the multiplication over the group space as*

$$\overrightarrow{x} \cdot \overrightarrow{y} = \Big(\sum_g x_g \overrightarrow{g} \Big) \cdot \Big(\sum_h y_h \overrightarrow{h} \Big) = \sum_g \sum_h x_g y_h \overrightarrow{gh} \tag{3.65}$$

*Thus the group space forms an associative algebra called the **group algebra**.*

Obviously

$$\overrightarrow{e} \cdot \overrightarrow{v} = \overrightarrow{v} \tag{3.66}$$
$$\overrightarrow{g} \cdot \overrightarrow{g^{-1}} = \overrightarrow{e} \tag{3.67}$$
$$L(g)\overrightarrow{v} = \overrightarrow{g} \cdot \overrightarrow{v} \tag{3.68}$$
$$R(g)\overrightarrow{v} = \overrightarrow{v} \cdot \overrightarrow{g^{-1}} \tag{3.69}$$

Lemma 3.5.2. *A vector $\overrightarrow{v}$ belongs to the class space iff $\forall g \in G : \overrightarrow{g} \cdot \overrightarrow{v} \cdot \overrightarrow{g^{-1}} = \overrightarrow{v}$.*

Lemma 3.5.3.

$$\overrightarrow{C_i} \cdot \overrightarrow{C_j} = f_{ijk} \overrightarrow{C_k} \tag{3.70}$$

where f_{ijk} is an integer.

Proof. Clearly $\vec{g}\cdot\vec{C_i}\cdot\overrightarrow{g^{-1}}=\vec{C_i}$.

Since

$$\vec{g}\cdot\vec{C_i}\cdot\vec{C_j}\cdot\overrightarrow{g^{-1}}=\vec{g}\cdot\vec{C_i}\cdot\overrightarrow{g^{-1}}\cdot\vec{g}\cdot\vec{C_j}\cdot\overrightarrow{g^{-1}}=\vec{C_i}\cdot\vec{C_j} \tag{3.71}$$

$\vec{C_i}\cdot\vec{C_j}$ belongs to the class space. It can be expressed as

$$\vec{C_i}\cdot\vec{C_j}=f_{ijk}\vec{C_k} \tag{3.72}$$

Obviously $\vec{C_i}\cdot\vec{C_j}$ has integers coefficients expanding on $\vec{g}$ basis. Then clearly f_{ijk} is an integer. □

Definition 3.5.4. *For each representation $T: G\mapsto GL(V)$, we define a map T from the group algebra to $hom(V)$ by*

$$T(\vec{v})=\sum_g v_g T(g) \tag{3.73}$$

where $\vec{v}=v_g\vec{g}$.

Lemma 3.5.5. *The T defined above is an algebra homomorphism, sometimes called the **representation of the group algebra**.*

Proof.

$$\begin{aligned} T(\vec{v})T(\vec{v'}) &= \sum_{gg'} v_g T(g) v'_{g'} T(g') && (3.74)\\ &= \sum_{gg'} v_g v'_{g'} T(gg') && (3.75)\\ &= \sum_{gg'} T(v_g v'_{g'}\overrightarrow{gg'}) && (3.76)\\ &= T(\vec{v}\cdot\vec{v'}) && (3.77) \end{aligned}$$

□

Lemma 3.5.6. *$T(\vec{C_i})=\frac{|C_i|}{d}\chi(C_i)I$, where d is the dimension of the representation space.*

Proof.

$$\begin{aligned} T(g)T(\vec{C_i})T(g^{-1}) &= T(\vec{g})T(\vec{C_i})T(\overrightarrow{g^{-1}}) && (3.78)\\ &= T(\vec{g}\cdot\vec{C_i}\cdot\overrightarrow{g^{-1}}) && (3.79)\\ &= T(\vec{C_i}) && (3.80) \end{aligned}$$

Thus $T(g)T(\vec{C_i})=T(\vec{C_i})T(g)$. From Schur's lemma, $T(\vec{C_i})=\lambda I$. By taking traces, $\lambda=\frac{|C_i|}{d}\chi(C_i)$. □

Lemma 3.5.7. *For a group representation T^a,*

$$\frac{|C_i|}{d_a}\chi^a(C_i)\frac{|C_j|}{d_a}\chi^a(C_j)=f_{ijk}\frac{|C_k|}{d_a}\chi^a(C_k) \tag{3.81}$$

where f_{ijk} is defined in Eqn. 3.72.

Proof.

$$T^a(\vec{C_i}\cdot\vec{C_j})=T^a(\vec{C_i})T^a(\vec{C_j})=f_{ijk}T^a(\vec{C_k}) \tag{3.82}$$

□

3.6 $d_a \big| |G|$

Definition 3.6.1. *An element $a \in \mathbb{F}$ is an **algebraic integer** if its the root of some monic polynomials in $\mathbb{F}[x]$ with integral coefficient.*

Theorem 3.6.2. *The set of all algebraic integers (relative to $\mathbb{F}$) forms a ring.*

Proof. If a is an algebraic integer and $a^n + \sum_{i=0}^{n-1} z_i a^i = 0$, clearly $\{1, \ldots, a^{n-1}\}$ generates $\mathbb{Z}[a]$.

If a and b are algebraic integers, $\mathbb{Z}[a]$ and $\mathbb{Z}[b]$ are finitely generated. Then clearly $\mathbb{Z}[a, b]$ is finitely generated. Since $\mathbb{Z}[a, b]$ is a Noether module, it's submodules $\mathbb{Z}[a + b]$ and $\mathbb{Z}[ab]$ are finitely generated. Suppose $\mathbb{Z}[a + b]$ is generated by $\{f_1(a + b), \ldots, f_n(a + b)\}$ and their maximal degree is d. Then $(a + b)^{(d+1)} = z_i f_i(a + b)$. Thus $a + b$ is an algebraic integer. Similarly ab is an algebraic integer. □

Theorem 3.6.3. *The algebraic integer (relative to $\mathbb{C}$) that is rational is an integer.*

Theorem 3.6.4. *The eigenvalues of an integer matrix are algebraic integers.*

Theorem 3.6.5. $d_a \big| |G|$

Proof. Clearly, the character $\chi^a(g)$ (of irreducible representation $T^a(g)$) is the sum of some eigenvalues of $L(g)$, which is a integer matrix under the basis $|g\rangle$. Thus $\chi^a(g)$ is an algebraic integer.

Equation (3.81) can be viewed as an eigenvalue equation of the matrix $(f_i)_{jk}$. Thus the eigenvalue $\frac{|C_i|}{d_a}\chi^a(C_i)$ is an algebraic integer.

Obviously the complex conjugation of an algebraic integer is an algebraic integer.

From (3.63) we have

$$\sum_a \frac{|C_i|}{d_a}\chi^{a*}(C_i)\chi^a(C_i) = \frac{|G|}{d_a} \tag{3.83}$$

The LHS is an algebraic integer, thus $\frac{|G|}{d_a}$ is also an algebraic integer. But $\frac{|G|}{d_a}$ is rational. So it is an integer. □

3.7 Character Table

The characters of irreducible representations have many advantages over the representations themselves. Firstly the characters are very concise. Secondly they're fixed while the representations can vary by a similar transformation. Thirdly, they provide us much information to reduce an arbitrary representation.

Thus for groups, people usually list $\chi^a(C_i)$s of all inequivalent irreducible representations a over all conjugacy classes C_i in the form a **character tables**, such as Tab. 3.1.

For most situations, the character table is uniquely determined by the equations for the characters that we have derived, which includes

1. The number of the inequivalent irreducible representations is the number of conjugacy classes.
2. The Burnside theorem $|G| = \sum_a d_a^2$.

	C_1	$\cdots$	C_n
χ^1	$\chi^1(C_1)$	$\cdots$	$\chi^1(C_n)$
$\cdots$	$\cdots$	$\ddots$	$\cdots$
χ^n	$\chi^n(C_1)$	$\cdots$	$\chi^n(C_n)$

Table 3.1: A character table.

3. $d_a \big| |G|$

4. The orthogonality relations:

$$\sum_i |C_i| \chi^{a*}(C_i)\chi^b(C_i) = |G|\delta_{ab} \tag{3.84}$$

$$\sum_a |C_i| \chi^{a*}(C_i)\chi^a(C_j) = |G|\delta_{ij} \tag{3.85}$$

5.

$$\frac{|C_i|}{d_a}\chi^a(C_i)\frac{|C_j|}{d_a}\chi^a(C_j) = f_{ijk}\frac{|C_k|}{d_a}\chi^a(C_k) \tag{3.86}$$

Note that for the identity representation, we can fill in $\chi(C_i) = 1$ without hesitation. We also have $\chi^a(e) = d_a$. We may take these to results into (3.84) and (3.85) and get for non-identity irreducible representation

$$\sum_i |C_i| \chi^a(C_i) = 0 \tag{3.87}$$

and for $C_i \neq \{e\}$

$$\sum_a d_a \chi^a(C_i) = 0 \tag{3.88}$$

We may also make use of the fact that for 1-D representations T^a, $\chi^a = T^a$.

3.8 Direct Product Representations

Definition 3.8.1. *Let $T(g)$ and $T'(g)$ be two representations of group G that act on V and V' respectively. $T''(g) = T(g) \otimes T'(g)$ is called the **direct product representation** of $T(g)$ and $T'(g)$.*

Lemma 3.8.2. *The characters of $T''(g) = T(g) \otimes T'(g)$ are $\chi''(g) = \chi(g)\chi'(g)$.*

Proof.

$$\chi''(g) = \mathrm{Tr}[T''(g)] = \mathrm{Tr}[T(g) \otimes T'(g)] = \mathrm{Tr}[T(g)]\mathrm{Tr}[T'(g)] = \chi(g)\chi'(g) \tag{3.89}$$

□

Definition 3.8.3. *If $T^a(g)$ and $T^b(g)$ are irreducible representations, normally $T^n(g) = T^a(g) \otimes T^b(g)$ is reducible, and can be reduced into $\bigoplus_c (T^c)^{\oplus n_{abc}}$, which is called the* ***Clebsch-Gordan series****. n_{abc} is can be calculated by*

$$n_{abc} = \frac{1}{|G|} \langle \chi^c | \chi^n \rangle \tag{3.90}$$

where $\chi^n(g) = \chi^a(g)\chi^b(g)$.

Chapter 4

Ring

4.1 Basics

Definition 4.1.1. *A* **ring** $(R, \cdot, +)$ *is a set* R *together with binary operators* $\cdot$ *and* $+$ *such that*

1. $(R, +)$ *is a abelian group with unit* 0*, called the* **additive group**.
2. $(R, \cdot)$ *is a monoid with unit* 1*, called the* **multiplicative monoid**.
3. $a(b + c) = ab + ac$ *and* $(a + b)c = ac + bc$ *hold* $\forall a, b, c \in R$.

Definition 4.1.2. *Let* $(R, \cdot, +)$ *be a ring. We define its* **opposite ring** $(R, \times, +)$*, denoted by* R^{op}*, to be the ring with the same underlying set and addition operation, and a new multiplication defined by* $a \times b = b \cdot a$.

Definition 4.1.3. *Let* $(R, \cdot, +)$ *be a ring,* $(S, \cdot, +)$ *is a* **subring** *of* $(R, \cdot, +)$ *if* $(S, +)$ *is a subgroup of* $(R, +)$*, and* $(S, \cdot)$ *is a submonoid of* $(R, \cdot)$.

Example 4.1.4. $\mathbb{Z}$*,* $\mathbb{Q}$*,* $\mathbb{R}$ *and* $\mathbb{C}$ *with the usual addition and multiplication are rings.*

Example 4.1.5. $\{m + n\sqrt{a} | m, n \in \mathbb{Z}\}(a \in \mathbb{Z})$ *is a subring of* $\mathbb{C}$ *called the* **Gaussian integers**.

Definition 4.1.6. *A ring* $(R, \cdot, +)$ *is a* **commutative ring** *if* $(R, \cdot)$ *is a commutative monoid.*

Definition 4.1.7. *A commutative ring* $(R, \cdot, +)$ *is an* **integral domain** *if* $(R - 0, \cdot)$ *is a submonoid of* $(R, \cdot)$.

Definition 4.1.8. *Let* R *be a ring.* $a \in R$ *is a* **left (right) zero divisor** *if* $\exists b \in R : ab = 0 (ba = 0)$.

Lemma 4.1.9. *A commutative ring* $(R, \cdot, +)$ *is an integral domain iff there's no non-zero zero divisors.*

Lemma 4.1.10. *A commutative ring* $(R, \cdot, +)$ *is an integral domain iff the cancellation law holds:* $ab = ac \wedge a \neq 0 \Rightarrow b = c$.

Definition 4.1.11. *A ring* $(R, \cdot, +)$ *is a* **division ring** *if* $(R - 0, \cdot)$ *is a subgroup of* $(R, \cdot)$.

Lemma 4.1.12. *A finite integral domain is a division ring.*

Definition 4.1.13. *A commutative division ring is called a* **field**.

Definition 4.1.14. *Let $(R, \cdot, +)$ be a ring. The invertible elements of the monoid $(R, \cdot)$ are called the* **units** *of R, which form a group $R^\times$.*

Lemma 4.1.15. *In a ring R, if $1 - ab$ is invertible, then so is $1 - ba$.*

Proof. $(1 - ba)^{-1} = 1 + b(1 - ab)^{-1}a$. □

Lemma 4.1.16 (Hua)**.** *In a ring R, if a, b and $ab - 1$ is invertible, then so is $a - b^{-1}$ and $(a - b^{-1})^{-1} - a^{-1}$.*

Proof. $(a - b^{-1})^{-1} = b(ab - 1)^{-1}$, $((a - b^{-1})^{-1} - a^{-1})^{-1} = aba - a$. □

Example 4.1.17. *$n \times n$ matrices with entries in a ring K form a ring $M_n(K)$ under matrix addition and matrix multiplication.*

Lemma 4.1.18. *Let R be a commutative ring. A matrix $A \in M_n(R)$ is invertible iff its determinant is invertible in R.*

Proof. $adj(A) \cdot A = A \cdot adj(A) = det(A)$ □

Example 4.1.19. *The* **quaternions** $\mathbb{H}$ *is a subring of $M_2(\mathbb{C})$ defined by* $\{\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} | a, b \in \mathbb{C}\}$.

Lemma 4.1.20. $\mathbb{H}$ *is a division ring.*

Proof. $det \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} = |a|^2 + |b|^2$. □

Lemma 4.1.21. $\mathbb{H}$ *is a real linear space with basis* $1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ *and* $k = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$.

4.2 Centralizer

Definition 4.2.1. *The* ***center*** *of a ring is the set of elements that commutes with every elements in R, denoted by $Z(R)$. That is*

$$Z(R) = \{x \in R | \forall r \in R : rx = xr\} \tag{4.1}$$

Definition 4.2.2. *The* ***centralizer*** *of a set S in group R is the set of elements that commutes with every elements in S, denoted by $C_R(S)$. That is*

$$C_R(S) = \{x \in R | \forall s \in S : sx = xs\} \tag{4.2}$$

Lemma 4.2.3. *Let S be a subset of a ring R then $C_R(S)$ is a subring of R.*

Lemma 4.2.4. *In a division ring, if $ab \neq ba$, we have the identity*

$$a = (b^{-1} - (a-1)^{-1}b^{-1}(a-1))(a^{-1}b^{-1}a - (a-1)^{-1}b^{-1}(a-1))^{-1} \tag{4.3}$$

Theorem 4.2.5 (Cartan,Brauer,Hua)**.** *A division ring (but not a field) K is generated by a non-central element and its conjugates.*

Proof. Let L be the set of all conjugates of a non-central element. Let K' be the subdivision-ring generated by L. It's easy to see that K' is normal. For each $a \in R$, if there exist $b \in K'$ not commutes with a, then $a = (b^{-1} - (a-1)^{-1}b^{-1}(a-1))(a^{-1}b^{-1}a - (a-1)^{-1}b^{-1}(a-1))^{-1} \in K'$. So $K - K'$ and K' are commutative elementwise.

If $K \neq K'$, let $a \in K - K'$ and $b, b' \in K'$ such that $bb' \neq b'b$. b and b' exist since otherwise K' is in the center of K. It's easy to see that $ab \in K - K'$. Thus $(ab)b' = b'(ab) = ab'b$. Thus $bb' = b'b$, a contradiction. □

Corollary 4.2.6. *Every proper normal subdivision-ring of a division ring is contained in its center.*

4.3 Ideals

Definition 4.3.1. *Let R be a ring. A subset $I \subseteq R$ is a* **(two-sided) ideal** *if I is an additive subgroup of R and $\forall g \in G : gI = Ig \subseteq I$.*

Lemma 4.3.2. *The intersection of ideals is an ideal.*

Definition 4.3.3. *Let R be a ring and $S \subseteq R$. The ideal* **generated by** *S, denoted by $\langle S \rangle$, is the intersection of all the ideals that contain S.*

Lemma 4.3.4. *Let R be a ring and $S \subseteq R$. The ideal generated by S is $\{\sum_{i=0}^{n} l_i s_i r_i | n \in \mathbb{N}, l_i, r_i \in R, s_i \in S\}$*

Definition 4.3.5. *A* **principle ideal** *is an ideal generated by one element.*

Definition 4.3.6. *An integral domain is a* **principle integral domain (PID)** *if every ideal is principle.*

Example 4.3.7. *$\mathbb{Z}$ is a PID.*

Definition 4.3.8. *In a commutative ring, a* **prime ideal** *I is an ideal such that $ab \in I \Rightarrow a \in I \vee b \in I$.*

Definition 4.3.9. *A* **maximal ideal** *I is an ideal of R such that there's no ideal M that satisfies $R \supsetneq M \supsetneq I$.*

Lemma 4.3.10. *In a commutative ring, a maximal ideal is a prime ideal.*

Proof. Let I be a maximal ideal of R such that I is not prime. Then there're a, b such that $ab \in I$, $a, b \notin I$. Then $\langle a, I \rangle = \langle b, I \rangle = R$. Then $\exists s \in R, t \in R, x \in I, y \in T$ such that $as + x = bt + y = 1$. Then $abst + (xbt + yas + xy) = 1$. Then $\langle ab, I \rangle = R$, a contradiction. □

Lemma 4.3.11. *In a PID, a prime ideal is a maximal ideal.*

4.4 Quotient Ring

Definition 4.4.1. *Let R be a ring with an ideal I. The additive quotient group R/I is a ring with the multiplication $[a] \cdot [b] = [ab]$, called the* **quotient ring**.

Example 4.4.2. *$(m) = m\mathbb{Z}$ is an ideal in the ring $\mathbb{Z}$. We define the quotient ring $\mathbb{Z}_m = \mathbb{Z}/(m)$.*

Lemma 4.4.3. *If p is a prime number, $\mathbb{Z}_p$ is a field, also denoted by F_p.*

Lemma 4.4.4. *Let R be a ring with an ideal I. I is prime iff R/I is an integral domain.*

Lemma 4.4.5. *Let R be a ring with an ideal I. I is maximal iff R/I is a field.*

4.5 Homomorphism and Isomorphism

Definition 4.5.1. *Let R_1 and R_2 be two rings. We define a map $f : R_1 \mapsto R_2$ to be a* **homomorphism** *if it's a homomorphism of both the addition group and the multiplication monoid.*

As with groups, we can define similar concepts of **monomorphism, epimorphism, isomorphism, endomorphism, automorphism, kernel, image, inner automorphism ...**

Lemma 4.5.2. *All automorphisms of a ring R form a group under function composition. This is called $Aut(R)$.*

Lemma 4.5.3. *Let $f : R_1 \mapsto R_2$ be a ring homomorphism. $\ker(f)$ is an ideal of R_1 and $\mathrm{im}(f)$ is a subring of R_2. $R_1/\ker(f) \cong \mathrm{im}(f)$.*

Definition 4.5.4. *Let R_1 and R_2 be two rings. We define a map $f : R_1 \mapsto R_2$ to be a n* **anti-homomorphism** *if it's a homomorphism of the addition group and an anti-homomorphism of the multiplication monoid.*

Lemma 4.5.5. *The composite of a homomorphism and an anti-homomorphism is an anti-homomorphism. The composite of two anti-homomorphisms is a homomorphism*

Lemma 4.5.6. *The identity map $R \mapsto R^{op}$ is an anti-homomorphism.*

4.5.1 Jordan homomorphism

Definition 4.5.7. *A* **Jordan homomorphism** *$\eta : R \mapsto R'$ is an additive group homomorphism that satisfies $\eta(1) = 1$ and $\eta(aba) = \eta(a)\eta(b)\eta(a)$.*

Lemma 4.5.8. *Let $\eta : R \mapsto R'$ be a Jordan homomorphism, then*

$$\eta(a^k) = \eta(a)^k, k \in \mathbb{N} \tag{4.4}$$

$$\eta(abc + cba) = \eta(a)\eta(b)\eta(c) + \eta(c)\eta(b)\eta(a) \tag{4.5}$$

$$\eta(ab + ba) = \eta(a)\eta(b) + \eta(b)\eta(a) \tag{4.6}$$

Lemma 4.5.9 (Hua)**.** *Let $\eta : R \mapsto R'$ be an additive group homomorphism that satisfies*

1. $\eta(1) = 1$
2. *For each $a, b \in R$, either $\eta(ab) = \eta(a)\eta(b)$ or $\eta(ab) = \eta(b)\eta(a)$*

Then η is a ring homomorphism or a ring anti-homomorphism.

Proof. For each $a \in R$, let $A_1 = \{r \in R | \eta(ar) = \eta(a)\eta(r)\}$ and $A_2 = \{r \in R | \eta(ar) = \eta(r)\eta(a)\}$. If $A_1 \neq R$ and $A_2 \neq R$, then let $r_1 \in R - A_1$ and $r_2 \in R - A_2$. Then $\eta(ar_1) = \eta(r_1)\eta(a) \neq \eta(a)\eta(r_1)$, and $\eta(ar_2) = \eta(a)\eta(r_2) \neq \eta(r_2)\eta(a)$. If $\eta(a(r_1 + r_2)) = \eta(a)\eta(r_1 + r_2)$, then $\eta(r_1)\eta(a) = \eta(a)\eta(r_1)$, a contradiction. If $\eta(a(r_1+r_2)) = \eta(r_1+r_2)\eta(a)$, there's a similar contradiction. So $A_1 = R$ or $A_2 = R$.

Let $S_1 = \{a \in R | \forall r \in R : \eta(ar) = \eta(a)\eta(r)\}$ and $S_2 = \{a \in R | \forall r \in R : \eta(ar) = \eta(r)\eta(a)\}$. If $S_1 \neq R$ and $S_2 \neq R$, then let $r_1 \in R - S_1$ and $r_2 \in R - S_2$. Then exists $a \in R$ such that $\eta(r_1 a) = \eta(a)\eta(r_1) \neq \eta(r_1)\eta(a)$. So $\eta(r_2 a) = \eta(a)\eta(r_2)$, a contradiction. So $S_1 = R$ or $S_2 = R$. So η is a ring homomorphism or a ring anti-homomorphism. □

Lemma 4.5.10 (Jacobson, Rickart)**.** *Let $\eta : R \mapsto D$ be a Jordan homomorphism from a ring to a domain, then for each $a, b \in R$, either $\eta(ab) = \eta(a)\eta(b)$ or $\eta(ab) = \eta(b)\eta(a)$. Thus η is a ring homomorphism or a ring anti-homomorphism..*

Proof.

$$\begin{aligned} & \eta((ab)ba + ab(ab)) = \eta(ab)\eta(b)\eta(a) + \eta(a)\eta(b)\eta(ab) \\ = \;& \eta(ab^2a + (ab)^2) = \eta(a)\eta(b)^2\eta(a) + \eta(ab)^2 \end{aligned} \tag{4.7}$$

So $(\eta(ab) - \eta(a)\eta(b))(\eta(ab) - \eta(b)\eta(a)) = 0$. So either $\eta(ab) = \eta(a)\eta(b)$ or $\eta(ab) = \eta(b)\eta(a)$. □

Theorem 4.5.11 (Hua)**.** *Let $\eta : D \mapsto D'$ be an additive group homomorphism between division rings that satisfies*

1. $\eta(1) = 1$
2. *For each $0 \neq a \in R$, $\eta(a) \neq 0$ and $\eta(a^{-1}) = \eta(a)^{-1}$.*

Then η is a ring homomorphism or a ring anti-homomorphism.

Proof. By Hua's identity, $\eta(aba - a) = \eta(((a - b^{-1})^{-1} - a^{-1})^{-1}) = ((\eta(a) - \eta(b)^{-1})^{-1} - \eta(a)^{-1})^{-1} = \eta(a)\eta(b)\eta(a) - \eta(a)$. So η is a Jordan homomorphism. □

4.5.2 Isomorphism Theorems

Theorem 4.5.12. *Let K be an ideal contained in I, which is an ideal of R. Then I/K is a ideal of R/K. Let f be a map from the ideals of R that contains K to the ideals of R/K, defined by $f(T) = T/K$. Then f is bijective. Further more, $R/I \cong (R/K)/(I/K)$.*

Theorem 4.5.13. *Let S be a subring of R, and I be an ideal in G. Then $S + I$ is a subring of R containing I as an ideal, $S \cap I$ is an ideal in S, and $(S + I)/I \cong S/(S \cap I)$.*

Proof. The isomorphism map is

$$f([h + k]_K) = [h]_{H \cap K} \tag{4.8}$$

□

4.6 Characteristic

Definition 4.6.1. *Let R be a ring, we have a natural homomorphism $f : \mathbb{Z} \mapsto R$ defined by*

$$f(n) = \underbrace{1 + \cdots + 1}_{n} \tag{4.9}$$

$$f(0) = 0 \tag{4.10}$$

$$f(-n) = -f(n) \tag{4.11}$$

where $n > 0$. Let $\ker f = (c)$. We define c to be the **characteristic** *of R.*

Example 4.6.2. *$\mathbb{Z}_p$ is of characteristic p. $\mathbb{Z}$ is of characteristic 0.*

Lemma 4.6.3. *The characteristic of an integral domain is a prime number.*

4.7 Relation of elements

In the following sections of this chapter we assume the ring to be commutative.

Definition 4.7.1. *Let R be a ring and $a, b \in R$. If $\exists c : b = ac$, then a* **divides** *b, denoted by $a|b$. We also say that a is a* **factor** *of b.*

Definition 4.7.2. *Let R be a ring and $a, b \in R$. If $\exists$ non-unit $c : b = ac$, then a* **divides properly** *b. We also say that a is a* **proper factor** *of b.*

Lemma 4.7.3. *Let R be a ring and $a, b \in R$. a divides b iff $b \in \langle a \rangle$ iff $\langle a \rangle \supseteq \langle b \rangle$.*

Definition 4.7.4. *Let R be a ring. $a \in R$ is* **prime** *if $\forall b, c \in R : a|bc \Rightarrow a|b \vee a|c$.*

Lemma 4.7.5. *Let R be a ring. $a \in R$ is prime iff $\langle a \rangle$ is a prime ideal.*

Definition 4.7.6. *Let R be a ring and $a, b \in R$. a* **associates with** *b, denoted by $a \sim b$, if there's a unit $u \in R$ such that $a = ub$.*

Lemma 4.7.7. *Let R be a ring and $a, b \in R$. $a \sim b$, iff $\langle a \rangle = \langle b \rangle$.*

Definition 4.7.8. *Let R be a ring. $a \in R$ is* **irreducible** *if $\forall b, c \in R : a = bc \Rightarrow b$ or c is unit.*

Lemma 4.7.9. *Let R be a domain. If $a \in R$ is prime, then a is irreducible.*

Lemma 4.7.10. *Let R be a p.i.d. If $a \in R$ is irreducible, then a is prime.*

Proof. If $a \in R$ is irreducible, then $\langle a \rangle$ is maximal. □

Definition 4.7.11. *Let R be a ring and $b_i \in R$. $a \in R$ is a* **greatest common divisor** *of $\{b_i\}$, denoted as $gcd(b_i)$, if $\forall i : a|b_i$ and for each $c \in R$ such that $\forall i : c|b_i$ we have $c|a$.*

Lemma 4.7.12. *Let R be a PID and $b_i \in R$. $a = gcd(\{b_i\})$ iff $\langle a \rangle = \langle \{b_i\} \rangle$.*

Lemma 4.7.13. $gcd(gcd(a_1, \ldots, a_n), b_1, \ldots, b_n) \sim gcd(a_1, \ldots, a_n, b_1, \ldots, b_n)$

Lemma 4.7.14. $gcd(a_1, \ldots, a_n)b \sim gcd(a_1 b, \ldots, a_n b)$

Lemma 4.7.15. *If $a = gcd(a_1, \ldots, a_n)$, then $\exists b_1, \ldots, b_n$ such that $a = a_1 b_1 + \cdots a_n b_n$.*

Definition 4.7.16. *Let R be a ring and $b_i \in R$. $a \in R$ is a* **least common multiplier** *of $\{b_i\}$, denoted as $lcm(b_i)$, if $\forall i : b_i|a$ and for each $c \in R$ such that $\forall i : b_i|c$ we have $a|c$.*

Lemma 4.7.17. *Let R be a PID and $b_i \in R$. $a = lcm(\{b_i\})$ iff $\langle a \rangle = \bigcap_i \langle b_i \rangle$.*

4.8 Polynomial Ring

Definition 4.8.1. *Let R be a ring. A* **formal power series** *over R is a series (r_i). The set of all formal power series form a ring $R[[x]]$, with addition and multiplication as*

1. $(a_i) + (b_i) = (c_i) \Rightarrow c_i = a_i + b_i$.
2. $(a_i) \cdot (b_i) = (c_i) \Rightarrow c_i = \sum_{j=0}^{i} a_j \cdot b_{i-j}$.

Definition 4.8.2. *Let R be a ring. The ring of* **polynomials** *$R[x]$ is a subring of $R[[x]]$*

$$R[x] = \{(r_i) \in R[[x]] | \exists n : m \geq n \to r_m = 0\} \tag{4.12}$$

There a natural embedding $\iota : R \hookrightarrow R[x]$ by defining $\iota(r) = (r, 0, \cdots)$. In this way we say $R \subseteq R[x]$.

Lemma 4.8.3. *Let R be an integral domain, $R[x]$ is also an integral domain.*

Lemma 4.8.4. *Let F be a field, $F[x]$ is a principle integral domain.*

Definition 4.8.5. *In $R[[x]]$ we define the* **indeterminate** *$x = (0, 1, 0, \cdots)$.*

Lemma 4.8.6. *$R[x]$ is generated by R and x. $(r_i) = \sum_i r_i x^i$. So we usually denote (r_i) by $u(x)$.*

Definition 4.8.7. *Let $\sigma = (r_i) \in R[x]$ be a non-zero polynomial. The* **degree** *of σ, denoted by $deg(\sigma)$, is n such that $r_n \neq 0$ and $r_m = 0$ for all $m > n$. Then we call r_n the* **leading coefficient** *of (r_i). (r_i) is called* **monic** *if its leading coefficient is 1.*

Lemma 4.8.8. *Let R and S be rings. For each $u \in S$ and each homomorphism $\eta : R \mapsto S$, there's a unique $\eta_u : R[x] \mapsto S$ such that $\eta_u(r) = \eta(r)$ and $\eta_u(x) = u$.*

Definition 4.8.9. *Let $R \subseteq T$ be rings. For each subset $S \subseteq T$, we define $R[S]$ to be the subring of T generated by R and S.*

Lemma 4.8.10. *Let $R \subseteq S$ be rings, and $u \in S$. Let i be the identity map on R. We usually write $i_u(p(x))$ as $p(u)$. It's easy to see that $\mathrm{im} i_u = R[u] \cong R[x]/\ker i_u$.*

Definition 4.8.11. *Let $R \subseteq S$ be rings, and $u \in S$. Let $f(x) \in R[x]$. If $f(u) = 0$, u is called a* **root** *of $f(x)$.*

Definition 4.8.12. *Let F be a field, and R be a ring that contains F. An element $u \in R$ is* **algebraic over** *F if $\exists f(x) \in F[x]$ such that $f(u) = 0$. Otherwise it's called* **transcendental**.

Definition 4.8.13. *Let u be algebraic over a field F. We define the* **minimal polynomial** *of u to be $f(x)$ if $\ker i_u = (f(x))$.*

Lemma 4.8.14. *Let u be algebraic over a field F with minimal polynomial $f(x)$. Then $f(x)$ is irreducible, and $F[u]$ is a field.*

Lemma 4.8.15. *Let F be a field. Let $f(x)$ be irreducible in $F[x]$. Then $F[x]/(f(x))$ is a field. Let $u = [x]$. Then (in $F[x]/(f(x)) \supseteq F$) $F[u] = F[x]/(f(x))$. And u is algebraic over F with minimal polynomial $f(x)$.*

4.9 Fraction Field

Definition 4.9.1. *Let R be a domain, we define the* **fraction field** *$Frac(R)$ of R as the ring $(R \times R/\sim, +, \cdot)$, where*

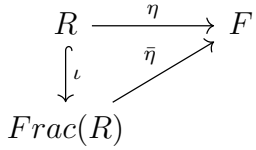
1. $(a, b) \sim (c, d) \Leftrightarrow ad = bc$
2. $(a, b) + (c, d) = (ad + bc, bd)$
3. $(a, b) \cdot (c, d) = (ac, bd)$

We sometimes denote (a, b) by a/b or $\frac{a}{b}$.

Lemma 4.9.2. *$Frac(R)$ is a field.*

Example 4.9.3. *$Frac(\mathbb{Z}) \simeq \mathbb{Q}$*

Lemma 4.9.4. *Let R be a domain, F be a field, and $\eta : R \mapsto F$ be a ring homomorphism. There's a unique ring homomorphism $\bar{\eta}$ to make the following diagram commute.*



4.10 Euclidean Domain

Definition 4.10.1. *A domain D is called* **Euclidean** *if there's a* **degree function** *$\delta : D - 0 \mapsto \mathbb{N}$, such that for all $a, b \neq 0 \in D \exists q, r \in D$ such that $a = bq + r$ where $r = 0$ or $\delta(r) < \delta(b)$.*

Example 4.10.2. *$\mathbb{Z}$ is an Euclidean domain with degree function id.*

Example 4.10.3. *Let F be a field. $\mathbb{F}[x]$ is an Euclidean domain with degree function deg.*

Lemma 4.10.4. *Every Euclidean domain is a PID.*

4.11 Unique Factorization Domain

Definition 4.11.1. *Let D be a domain. A* **factorization** *of $r \in D$ into irreducible elements is the equation $r = p_1 \cdots p_n$ where p_i is irreducible and non-unit for all i. A factorization $r = p_1 \cdots p_n$ is called* **essentially unique** *if for any other factorization $r = q_1 \cdots q_m$, we have $m = n$ and there's a permutation $\sigma \in S_n$ such that $p_i \sim q_{\sigma(i)}$ for all i.*

Definition 4.11.2. *A domain D is a* **unique factorization domain (UFD)** *if every non-zero non-unit of D has an essentially unique factorization into irreducible elements.*

Lemma 4.11.3 (primeness condition)**.** *In a UFD, every irreducible element is prime.*

Lemma 4.11.4 (divisor chain condition)**.** *A UFD contains no infinite sequences of elements $a_1, a_2, \ldots$ such that each a_{i+1} is a proper factor of a_i.*

Lemma 4.11.5. *If the divisor chain condition hold for a domain, then each element has a factorization into irreducible elements.*

Lemma 4.11.6. *A domain is a UFD iff the primeness condition and the divisor chain condition hold.*

Lemma 4.11.7 (gcd condition)**.** *In a UFD, any two elements have a greatest common divisor. Or equivalently, any n elements have a greatest common divisor.*

Lemma 4.11.8. *For a domain, the gcd condition implies the primeness condition.*

Proof. Let p be an irreducible. If $p \not| a$ and $p \not| b$, we have $gcd(p, a) \sim gcd(p, b) \sim 1$. Then $gcd(p, ab) \sim gcd(gcd(p, pa), ab) \sim gcd(p, gcd(ap, ab)) \sim gcd(p, a\, gcd(p, b)) \sim 1$. So $p \not| ab$. □

Corollary 4.11.9. *A domain is a UFD iff the gcd condition and the divisor chain condition hold.*

Lemma 4.11.10. *The divisor chain condition holds for a PID.*

Proof. If not, let $a_1, a_2, \ldots$ be the sequence. Let $\langle b\rangle = \bigcup_i \langle a_i\rangle$. Let $b \in \langle a_n\rangle$. Then $\langle b\rangle = \bigcup_{i=1}^{n} \langle a_i\rangle = \bigcup_{i=1}^{n+1} \langle a_i\rangle$. So $a_n | a_{n+1}$, a contradiction. □

Corollary 4.11.11. *A PID is a UFD.*

Corollary 4.11.12. *An Euclidean Domain is a UFD.*

4.12 Polynomial Ring of a UFD

Definition 4.12.1. *Let D be a UFD. In $D[x]$ the* **content** *$c(f)$ of a polynomial $f(x) = a_0 + \cdots + a_n x^n$ is the gcd of all non-zero elements in $a_0, \ldots, a_n$. $f(x)$ is called* **primitive** *if $c(f) = 1$.*

Lemma 4.12.2. *Let D be a UFD and $f(x) \in D[x]$. Then $f(x) = c(f)\tilde{f}(x)$ where $\tilde{f}(x)$ is primitive. If $f(x) = af'(x)$ where $f'(x)$ is primitive. Then $a \sim c(f)$ and $f'(x) \sim \tilde{f}(x)$.*

Lemma 4.12.3. *Let D be a UFD. In $D[x]$, the product of primitive polynomials is primitive.*

Proof. Let f_1, f_2 be primitive polynomials. If $f_1 f_2$ is not a primitive polynomials, let p be an non-unit irreducible element in D such that $p | f_1 f_2$. Clearly $p \not| f_1$. Let $f_1 = \sum_i a_i x^i$. Let $a_n \neq 0$ be the coefficient such that $p \not| a_n$ and $p | a_i$ for all $i > n$. Similarly $p \not| f_2$. Let $f_2 = \sum_i b_i x^i$. Let $b_m \neq 0$ be the coefficient such that $p \not| b_m$ and $p | b_i$ for all $i > m$. Let $f_1 f_2 = \sum_i c_i x^i$. Then $c_{n+m} = a_n b_m + \sum_{i>1} a_{n+i} b_{m-i} + \sum_{i>1} a_{n-i} b_{m+i}$. Clearly $p \not| a_n b_m$ and $p | \sum_{i>1} a_{n+i} b_{m-i} + \sum_{i>1} a_{n-i} b_{m+i}$. So $p \not| c_{n+m}$, a contradiction. □

Lemma 4.12.4. *Let D be a UFD and $f(x) \in D[x]$ be irreducible with positive degree. Then $f(x)$ is irreducible in $Frac(D)[x]$.*

Lemma 4.12.5. *Let D be a UFD and $f(x) \in D[x]$ be primitive. A factorization of $f(x)$ in D is also a factorization in $Frac(D)$.*

Lemma 4.12.6. *Let D be a UFD and $f_1(x), f_2(x) \in D[x]$ are primitive. If $f_1(x) \sim f_2(x)$ in $Frac(D)[x]$, then $f_1(x) \sim f_2(x)$ in $D[x]$.*

Lemma 4.12.7. *Let D be a UFD, then so is $D[x]$.*

Proof. It's easy to see that the divisor chain condition holds for $D[x]$. So $\forall f(x) \in D[x]$, $f(x)$ has a factorization in D. We need only consider the part of elements with positive degree. It is also an essentially unique factorization in $Frac(D)$. So it is essentially unique in D. □

Lemma 4.12.8 (Eisenstein)**.** *Let D be a UFD. Let $f(x) = \sum_{i=0}^{m} a_i x^i \in D[x]$. If there's a prime in D such that $p \not| a_m$, $p | a_{m-1}, \ldots, a_0$ and $p^2 \not| a_0$. Then $f(x)$ is irreducible in $Frac(D)[x]$.*

Chapter 5

Galois Theory

5.1 Field

Lemma 5.1.1. *The characteristic of a field is a prime number.*

Example 5.1.2. *$\mathbb{Z}$ is of characteristic 0. $\mathbb{Z}_p$ is of characteristic p.*

Definition 5.1.3. *Let F be a subfield of K, then we call K the* **extension field** *of F, and write as K/F.*

Definition 5.1.4. *Let K/F be a field extension. Then K can be viewed as a linear space over F. We define $[K : F]$ to be the dimension of K. The extension K/F is called* **finite** *if $[K : F]$ is finite.*

Definition 5.1.5. *A field extension K/F is called an* **algebraic** *extension if every element of K is algebraic in F.*

Definition 5.1.6. *Let $F \subseteq T$ be fields. For each subset $S \subseteq T$, we define $F(S)$ to be the subfield of T generated by F and S.*

Lemma 5.1.7. *Let u be in E/F. u is algebraic in F if $[F(u) : F]$ is finite.*

Corollary 5.1.8. *A finite extension is algebraic.*

Lemma 5.1.9. *Let u be in E/F. If u is algebraic in F, then $F[u] = F(u)$. Let f be the minimal polynomial, $[F(u) : F] = deg(f)$.*

Proof. $F[u] \cong F[x]/(f)$ is a field □

Lemma 5.1.10. *Let E/F be an algebraic extension. If E is finite generated, then E/F is finite.*

Lemma 5.1.11. *Let $F \subseteq T \subseteq K$ be fields. $[K : F]$ is finite iff $[K : T]$ and $[T : F]$ is finite. In this case $[K : F] = [K : T][T : F]$.*

Definition 5.1.12. *A field F is called* **algebraically closed** *iff it satisfies one of the following equivalent conditions*

1. *For each algebraic extension E/F we have $E = F$.*
2. *Each polynomial in $F[x]$ has a root in F.*
3. *Irreducible polynomials in $F[x]$ have degree one.*

5.2 Splitting Field

Definition 5.2.1. *Let F be a field and $f(x)$ be a monic polynomial in $F[x]$. We say $f(x)$* **splits in** *an extension field E/F if $f(x) = \prod_i (x - r_i)$ in $E[x]$.*

Definition 5.2.2. *Let F be a field, and $f(x)$ be a monic polynomial in $F[x]$. Then an extension field E/F is called a* **splitting field** *over F of $f(x)$ if $f(x) = \prod_{i=1}^{n}(x - r_i)$ in $E[x]$, and $E = F(r_1, \ldots, r_n)$.*

Lemma 5.2.3. *Let F be a field, and $f(x)$ be a monic polynomial in $F[x]$. If $deg(f(x)) > 1$ there exists an extension field E/F such that $f(x)$ is reducible in $E[x]$.*

Proof. If $f(x)$ is not irreducible in $F[x]$, then $E = F$. If $f(x)$ is irreducible in $F[x]$, we define $E = F[x]/(f(x))$. We can view E as an extension field of F. Let $a = [x]$ in E, then $f(a) = 0$ in $E[x]$. So $f(x) = (x - a)f'(x)$ in $E[x]$. □

Corollary 5.2.4. *Let F be a field, and $f(x)$ be a monic polynomial in $F[x]$. If $deg(f(x)) > 1$ there exists an extension field E/F such that $f(x)$ splits in.*

Lemma 5.2.5. *Any monic polynomial $f(x) \in F[x]$ of positive degree has a splitting field E/F.*

Proof. Let E/F be an extension in which $f(x)$ splits. Let $f(x) = \prod_{i=1}^{n}(x - r_i)$. Then $F(r_1, \ldots, r_n)$ is the splitting field. □

Lemma 5.2.6. *Let E/F be an extension, $r \in E$ be algebraic over F with minimal polynomial $g(x) \in F[x]$. For each extension E'/F, there's a isomorphism $\eta : F(r) \mapsto E'$ iff $g(x)$ has a root in E'. The number of such isomorphisms is the number of distinct roots of $g(x)$ in E'.*

Chapter 6

Module

6.1 Left and Right Modules

Definition 6.1.1. *Let R be a ring. A* **left R-module** *(aka an* **R-mod***) is an additive abelian group M equipped with a scalar multiplication $R \times M \mapsto R$ denoted by $(r, m) \mapsto rm$ such that $\forall m, m' \in M$ and all $r, r' \in R$*

(i) $r(m + m') = rm + rm'$

(ii) $(r + r')m = rm + r'm$

(iii) $(rr')m = r(r'm)$

(iv) $1m = m$

Definition 6.1.2. *Let R be a ring. A* **right R-module** *(aka a* **mod-R***) is an additive abelian group M equipped with a scalar multiplication $R \times M \mapsto R$ denoted by $(r, m) \mapsto mr$ such that $\forall m, m' \in M$ and all $r, r' \in R$*

(i) $(m + m')r = mr + m'r$

(ii) $m(r + r') = mr + mr'$

(iii) $m(rr') = (mr)r'$

(iv) $1m = m$

Chapter 7

Commutative Algebra

7.1 Noether Ring and Noether Module

Definition 7.1.1. *A ring R is called a* **Noether ring** *if it satisfies one the equivalent conditions:*

1. *Any ideal of R is finitely generated.*
2. *R satisfies the* **ascending chain condition***: any ascending chain $I_1 \subseteq I_2 \subseteq \cdots$ of ideals in R is stable.*
3. *Any non-empty class of ideals in R must have a maximal element.*

Lemma 7.1.2. *The quotient ring of a Noether ring is a Noether ring.*

Theorem 7.1.3 (Hilbert Basis Theorem)**.** *If R is a Noether ring, $R[x]$ is a Noether ring.*

Definition 7.1.4. *A module M is called a* **Noether module** *if it satisfies one the equivalent conditions:*

1. *Any submodule of M is finitely generated.*
2. *M satisfies the* **ascending chain condition***: any ascending chain $M_1 \subseteq M_2 \subseteq \cdots$ of submodules in M is stable.*
3. *Any non-empty class of submodules in M must have a maximal element.*

Lemma 7.1.5. *Let M be a module, M' its submodule. Then M is Noetherian iff M' and M/M' is Noetherian.*

Corollary 7.1.6. *Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence, M is Noetherian iff M' and M'' is Noetherian.*

Corollary 7.1.7. *Finite direct sum of Noether module is Noetherian.*

Corollary 7.1.8. *R is a Noether ring iff any finitely generated R-module is Noetherian.*

7.2 Artin Ring and Artin Module

Definition 7.2.1. *A ring is called an* **Artin ring** *if it satisfies one of the equivalent conditions*

1. *R satisfies the* **descending chain condition***: any descending chain $M_1 \supseteq M_2 \supseteq \cdots$ of ideals in R is stable.*
2. *Any non-empty class of ideals in M must have a minimal element.*

Theorem 7.2.2. *Quotient ring of an Artinian ring is Artinian.*

Lemma 7.2.3. *Let R be an Artin ring, R has finitely many maximal ideals.*

Lemma 7.2.4. *Let R be an Artin ring, and M_1, M_2, ..., M_n be its maximal ideals. Let $J = M_1 \cap M_2 \cap \cdots \cap M_n$. Then $J = nil(M)$ and there exists m such that $J^m = 0$.*

Theorem 7.2.5. *An Artin ring is a Noether ring.*

Corollary 7.2.6. *There is a ring isomorphism*

$$R \simeq R/J \simeq R/M_1^m \oplus R/M_1^m \oplus \cdots \oplus R/M_1^m \tag{7.1}$$

Definition 7.2.7. *A module is called an* **Artin module** *if it satisfies one of the equivalent conditions*

1. *M satisfies the* **descending chain condition***: any descending chain $M_1 \supseteq M_2 \supseteq \cdots$ of submodules in M is stable.*
2. *Any non-empty class of submodules in M must have a minimal element.*

Theorem 7.2.8. *Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence, M is Artinian iff M' and M'' is Artinian.*

7.3 Localization of Ring

Definition 7.3.1. *Let R be a ring, S a submonoid of the multiplicative monoid $(R, \cdot, 1)$ and $0 \notin S$. We define the localization $S^{-1}R$ as $R \times S$ mod the equivalence relation*

$$(r_1, s_1) \sim (r_2, s_2) \iff \exists s \in S : s(r_1 s_2 - r_2 s_1) = 0 \tag{7.2}$$

We denote (r, s) as r/s.

$S^{-1}R$ forms a ring under

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 s_2 + r_2 s_1}{s_1 s_2}, \ \frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1 r_2}{s_1 s_2} \tag{7.3}$$

The zero element is $0 = 0/1$ and the unit element is $1 = 1/1$

Definition 7.3.2. *We define the homomorphism $\phi_S : R \to S^{-1}R$ as*

$$\phi_S(r) = \frac{r}{1} \tag{7.4}$$

Lemma 7.3.3. *ϕ_S is injective iff S doesn't contains any zero divisor.*

If $S \subseteq R^\times$, $S^{-1}R = R$.
If $S = R - 0$, $S^{-1}R = FracR$.
The localization $S^{-1}R$ has the following universal property

Theorem 7.3.4. *Let $f : R \to A$ be a ring homomorphism such that $f(S) \subseteq A^\times$. Then there exists a unique ring homomorphism $S^{-1}R$ such that $f = g \circ \phi_S$.*

Definition 7.3.5. *Let I be an ideal of R, $S^{-1}I \in S^{-1}R$ is defined as*

$$\{\frac{r}{s} | r \in I, s \in S\} \tag{7.5}$$

Clearly $S^{-1}I$ is an ideal of $S^{-1}R$.

Let J be an ideal of $S^{-1}R$, J^c is defined as $\phi_S^{-1}(J)$. Clearly J^c is an ideal of R.

Lemma 7.3.6.

$$S^{-1}(I_1 + I_2) = S^{-1}I_1 + S^{-1}I_2 \tag{7.6}$$
$$S^{-1}(I_1 I_2) = S^{-1}I_1 S^{-1}I_2 \tag{7.7}$$
$$S^{-1}(I_1 \cap I_2) = S^{-1}I_1 \cap S^{-1}I_2 \tag{7.8}$$
$$S^{-1}(R/I) = S^{-1}R/S^{-1}I \tag{7.9}$$

Lemma 7.3.7. *Let I be an ideal of R and J be an ideal of $S^{-1}R$. $J = S^{-1}J^c$ and $I \subseteq (S^{-1}I)^c$.*

Theorem 7.3.8. *If R is a Noether ring, then $S^{-1}R$ is a Noether ring.*

Theorem 7.3.9. *$\mathfrak{p} \to S^{-1}\mathfrak{p}$ is a 1-1 map from prime ideal $\mathfrak{p}$ in R such that $\mathfrak{p} \cap S = \emptyset$ to prime ideal in $S^{-1}R$, and $\mathfrak{p} = (S^{-1}\mathfrak{p})^c$*

Definition 7.3.10. *Let $\mathfrak{p}$ be a prime ideal of R. Define*

$$R_\mathfrak{p} = (R - \mathfrak{p})^{-1}R \tag{7.10}$$

Lemma 7.3.11. *$R_\mathfrak{p}$ has a unique maximal ideal $\mathfrak{p}R_\mathfrak{p} = (R - \mathfrak{p})^{-1}\mathfrak{p}$.*

Definition 7.3.12. *A ring is called* **local ring** *if it has a unique maximal ideal.*

R_p is a local ring.

Lemma 7.3.13. *Let R be a local ring with maximal ideal $\mathfrak{m}$. Then $\mathfrak{m} = R - R^\times$ and $1 + \mathfrak{m} \in R^\times$.*

Lemma 7.3.14. *Let R be a local ring with ideal $\mathfrak{m}$ such that $1 + \mathfrak{m} \in R^\times$. Then $\mathfrak{m} = R - R^\times$, so R is a local ring with maximal ideal $\mathfrak{m}$.*

Theorem 7.3.15. *Let R be a integral domain. We may view $R_\mathfrak{m}$ as a subring of $FracR$. We have*

$$R = \cap_\mathfrak{m} R_\mathfrak{m} \tag{7.11}$$

7.4 Localization of Module

Definition 7.4.1. *Let R be a ring, M a R module, and S a submonoid of the multiplicative monoid $(R, \cdot, 1)$ and $0 \notin S$. We define the localization $S^{-1}M$ as $M \times S$ mod the equivalence relation*

$$(m_1, s_1) \sim (m_2, s_2) \iff \exists s \in S : s(m_1 s_2 - m_2 s_1) = 0 \tag{7.12}$$

We denote (m, s) as m/s.

$S^{-1}M$ forms a $S^{-1}R$ module under

$$\frac{m_1}{s_1} + \frac{m_2}{s_2} = \frac{m_1 s_2 + m_2 s_1}{s_1 s_2}, \ \frac{r}{s_1} \cdot \frac{m}{s_2} = \frac{rm}{s_1 s_2} \tag{7.13}$$

and $S^{-1}M$ also forms a R module under

$$r \cdot \frac{m}{s} = \frac{rm}{s} \tag{7.14}$$

Definition 7.4.2. *We define the R-module homomorphism $\phi_S : M \to S^{-1}M$ as*

$$\phi_S(m) = \frac{m}{1} \tag{7.15}$$

The localization $S^{-1}M$ has the following universal property

Theorem 7.4.3. *Let M be a R-module and N a $S^{-1}R$-module (so also a R-module). Let $f : M \to N$ be a R-module homomorphism. There exists a unique $S^{-1}R$-module homomorphism $g : S^{-1}M \to N$ such that*

$$f = g \circ \phi_S \tag{7.16}$$

Lemma 7.4.4. *There is an $S^{-1}R$-module isomorphism $S^{-1}M \simeq S^{-1}R \otimes_R M$.*

Theorem 7.4.5. *Functor $M \to S^{-1}M$ is an exact functor from R-module to $S^{-1}R$-module. That is, if $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ is an R-module short exact sequence, $0 \to S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M'' \to 0$ is an $S^{-1}R$-module short exact sequence(and also an R-module short exact sequence).*

Corollary 7.4.6. *$S^{-1}R$ is a flat R-module.*

Lemma 7.4.7.

$$S^{-1}(M + N) = S^{-1}M + S^{-1}N \tag{7.17}$$
$$S^{-1}(M \cap N) = S^{-1}M \cap S^{-1}N \tag{7.18}$$
$$S^{-1}(M/N) = S^{-1}M/S^{-1}N \tag{7.19}$$
$$S^{-1}(M \oplus N) = S^{-1}M \oplus S^{-1}N \tag{7.20}$$
$$S^{-1}(M \otimes_R N) = S^{-1}M \otimes_{S^{-1}R} S^{-1}N \tag{7.21}$$

Definition 7.4.8. *Let $f : M \to N$ be a R-module homomorphism. We define R-module homomorphism and S^1R-module homomorphism $S^{-1}f : S^{-1}M \to S^{-1}N$ as*

$$S^{-1}f(\frac{m}{s}) = \frac{f(m)}{s} \tag{7.22}$$

Lemma 7.4.9. $\ker S^{-1}f = S^{-1}\ker f$ *and* $\operatorname{im} S^{-1}f = S^{-1}\operatorname{im} f$.

Theorem 7.4.10. *Let M be an R-module. $M = 0$ if $M_{\mathfrak{m}} = 0$ for any maximal ideal $\mathfrak{m}$.*

7.5 Integrity

Definition 7.5.1. *Let R be the subring of S. An element $s \in S$ is said to be* **integral over** *R if there exists a monic polynomial $f(x) \in R[x]$ such that $f(s) = 0$. If s is integral over R for any $s \in S$, S is said to be integral over R, and S is also called to be an* **integral extension** *of R.*

Lemma 7.5.2. *Let R be the subring of S. $s \in S$ is integral over R iff there exists a subring T of S such that $R[s] \subseteq T$ and T is a finitely generated R-module.*

Proof. If $s \in S$ is integral over R, $T = R[s]$ satisfies the requirement. If $R[s] \subseteq T$ and T is a finitely generated R-module, assume T is generated by $\{t_1, \ldots, t_n\}$. We have

$$st_i = \sum_j a_{ij} t_j \tag{7.23}$$

So

$$\sum_j (s\delta_{ij} - a_{ij}) t_j = 0 \tag{7.24}$$

Let $A = (a_{ij})$, $B = sI - A$ and $t = (t_1, \ldots, t_n)$. We have

$$Bt = 0 \tag{7.25}$$

So

$$B^* Bt = (\det B)t = 0 \tag{7.26}$$

Since we have $\sum_i c_i t_i = 1 \in T$, we have

$$\det B = \det(sI - A) = 0 \tag{7.27}$$

So $s \in S$ is integral over R. □

Definition 7.5.3. *The* **integral closure** *of R in S is the set of all elements in S that is integral over R.*

Lemma 7.5.4. *Let R be the subring of S, and $s, t \in S$. If s and t are integral over R then $s + t$ and st are integral over R. So integral closer of R in S is the integral extension of R.*

Theorem 7.5.5. *Let R be the subring of S and S is integral over R. If S is an integral domain, S is a field iff R is a field.*

Theorem 7.5.6. *Let R be the subring of S and S is integral over R. If $\mathfrak{p}$ is a prime ideal of R, there exists a prime ideal $\mathfrak{q}$ of S such that $\mathfrak{p} = \mathfrak{q} \cap R$. Furthermore, $\mathfrak{p}$ is a maximal ideal iff $\mathfrak{q}$ is a maximal ideal.*

Definition 7.5.7. *R is said to be* **integral closed** *in S if the integral closer of R in S is R. R is said to be integral closed if it's integral closed in $FracR$.*

Lemma 7.5.8. *Let R be an integral ring, then the following statements are equivalent*

1. *R is integral closed.*
2. *$R_{\mathfrak{p}}$ is integral closed for any prime ideal $\mathfrak{p}$.*
3. *$R_{\mathfrak{m}}$ is integral closed for any prime ideal $\mathfrak{m}$.*

Definition 7.5.9. *Let K be a field extension of $\mathbb{Q}$. The integral closure of $\mathbb{Z}$ in K is called the ring of algebraic integers of K, denoted by $\mathcal{O}_K$. Elements of $\mathcal{O}_K$ are called algebraic integers.*

7.6 Radical Ideal and Primary Ideal

Definition 7.6.1. *Let I be an ideal of R, define the radical ideal of I as*

$$\sqrt{I} = \{a \in R | \exists n : a^n \in I\} \tag{7.28}$$

It's easy to see that $\sqrt{I}$ is also an ideal of R.

Definition 7.6.2. *Let R be a ring, define $nil(R) = \sqrt{(0)}$.*

Lemma 7.6.3. $\sqrt{I}/I = nil(R/I)$

Lemma 7.6.4. *Let R be a Noether ring, and I be an ideal of R. There exists m such that $(\sqrt{I})^m \subseteq I$.*

Definition 7.6.5. *Let I be an ideal of R. If $I = \sqrt{I}$, we call I a radical ideal.*

Lemma 7.6.6. *Prime ideals are radical ideals.*

Theorem 7.6.7. *Let I be an ideal of R. Then*

$$\sqrt{I} = \bigcap_{\text{prime ideal } \mathfrak{p} \supseteq I} \mathfrak{p} \tag{7.29}$$

Definition 7.6.8. *The* **Jacobson radical** *of a ring is the intersection of all of its maximal ideals, denoted as $JacR$.*

Lemma 7.6.9. *If I is a proper ideal of R then $(I, Jac(R)) \neq R$.*

Lemma 7.6.10.

$$x \in Jac(R) \iff \forall r \in R : 1 - rx \in R^\times \tag{7.30}$$

Lemma 7.6.11 (Nakayama)**.** *If M is a finitely generated R module and $Jac(R)M = M$ then $M = 0$.*

Definition 7.6.12. *Let Q be an ideal of R. Q is called* **primary ideal** *if $ab \in Q$ leads to $a \in Q$ or $b \in Q$ or $a, b \in \sqrt{Q}$.*

Lemma 7.6.13. *Let Q be an ideal of R. If Q is a primary ideal then $\sqrt{Q}$ is a prime ideal.*

Lemma 7.6.14. *Let Q be an ideal of R. If $\sqrt{Q}$ is a maximal ideal then Q is a primary ideal.*

7.7 Affine Algebraic Geometry

An n-dimensional affine space over field k is the set of n-tuples

$$\mathbb{A}^n = k^n \tag{7.31}$$

For each $f(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$ we define a polynomial function $f^b : k^n \to k$ by

$$f^b(a_1, \ldots, a_n) = f(a_1, \ldots, a_n) \tag{7.32}$$

We may not differentiate between f and f^b in the future.

Definition 7.7.1. *Let S be a subset of $k[x_1, \ldots, x_n]$. It's* **zero locus** *is defined as*

$$\mathcal{Z}(S) = \{a \in \mathbb{Z}^n | \forall f \in S : f(a) = 0\} \tag{7.33}$$

Example 7.7.2. *The followings are some examples of zero locus.*

1. $\mathcal{Z}(0) = \mathbb{A}^n$

Definition 7.7.3. *Let C be a subset of $\mathbb{A}^n$. C is called an* **affine algebraic set** *if*

$$C = \mathcal{Z}(S) \tag{7.34}$$

for some $S \subset k[x_1, \ldots, x_n]$.

Chapter 8

Linear Representation of Finite Group (remastered)

8.1 Semi-simple Module

Definition 8.1.1. *A module is called* **simple** *if it's non-zero and doesn't have any proper nontrivial submodule.*

Theorem 8.1.2. *Simple modules are cyclic and any non-zero element is a generator.*

Proof. Cyclic module generated by any non-zero element is a non-zero submodule. □

Lemma 8.1.3 (Schur)**.** *Non-zero homomorphism between simple modules is isomorphism.*

Proof. Since the kernel and image of a homomorphism are submodules. □

Definition 8.1.4. *A module M is called* **semi-simple** *if it is the direct sum of simple modules.*

Theorem 8.1.5. *A module M is semi-simple iff it is the sum of simple modules.*

Proof. If M is semi-simple, clearly it is the sum of simple modules.

If M is the sum of simple modules. Let $M = \sum_{j\in I} S_j$ such that each S_i is simple. Let J be the maximal subset of I such that $\sum_{i\in J} S_i$ is direct. Then $\forall i \in I : S_i \cap \sum_{j\in J} S_j = S_i$ or 0. If $\exists i_0 \in I : S_{i_0} \cap \sum_{j\in J} S_j = 0$. Then $S_{i_0} + \sum_{j\in J} S_j$ is direct and this leads to a contraction. So $\forall i \in I : S_i \cap \sum_{j\in J} S_j = S_i$. So $M = \sum_{j\in J} S_j = \oplus_{j\in J} S_j$. So M is semi-simple. □

Theorem 8.1.6. *A module M is semi-simple iff every submodule of M is a direct summand.*

Proof. If M is semi-simple, let $M = \oplus_{i\in I} S_i$ and M' be a submodule of M. Let J be the maximal subset of I such that $M' + \sum_{i\in J} S_i$ is direct. Then $\forall i \in I : S_i \cap (M' + \sum_{j\in J} S_j) = S_i$ or 0. If $\exists i_0 \in I : S_{i_0} \cap (M' + \sum_{j\in J} S_j) = 0$. Then $M' + \sum_{i\in J} + S_{i_0}$ is direct and this leads to a contraction. So $\forall i \in I : S_i \cap (M' + \sum_{j\in J} S_j) = S_i$. So $M = (M + \sum_{j\in J} S_j) = M' \oplus \oplus_{j\in J} S_j$. So M' is a direct summand of M.

If every submodule of M is a direct summand, let Σ be the class of submodules of M that are sum of simple modules. And in Σ, $U < V$ if $U \subseteq V$. It's easy to see that each chain in Σ is bounded.

So we have a maximal element $M_0 \in \Sigma$ and $M = M_0 \oplus M'$. If $M' \neq 0$, we prove that M' contains a simple module.

Let $0 \neq m \in M'$, and $f : R \mapsto M$ be an R-module homomorphism defined by $f(r) = rm$. Since $\ker f$ is a proper ideal of R, we have the maximal ideal $\mathfrak{m}$ that contains $\ker f$. Let $M = \langle m \rangle \oplus M_1 = f(\mathfrak{m}) \oplus M_2$. Since $f(\mathfrak{m}) \subseteq \langle m \rangle$, it's easy to see that $\langle m \rangle = f(\mathfrak{m}) \oplus (\langle m \rangle \cap M_2)$, and $\langle m \rangle \cap M_2 \simeq \langle m \rangle / f(\mathfrak{m}) \simeq R/\mathfrak{m}$ is simple. So M' contains a simple module $M_1 = \langle m \rangle \cap M_2$.

So $M_0 \oplus M_1 \in \Sigma$, which leads to a contraction. So $M' = 0$, and M is the sum of simple modules. So M is semi-simple □

Theorem 8.1.7. *The submodule and quotient module of a semi-simple module is semi-simple. The direct sum of semi-simple modules is semi-simple.*

Theorem 8.1.8. *Let M be a semi-simple R-module, and $M = \oplus n_i S_i$ be a simple decomposition. Then n_i and S_i are uniquely determined. (n_i can be ∞ and we assume $\infty = \infty$)*

Theorem 8.1.9. *Let M be a semi-simple module, the following statements are equivalent*

1. *M is finitely generated.*
2. *M is finite direct sum of simple modules.*
3. *M is Artinian.*
4. *M is Noetherian.*

Proof. $1 \to 2$: We can find a finite set of generators such that each lies in a simple submodule.
$2 \to 1$: Obvious.
$2 \leftrightarrow 3, 4$: Length of M is finite.
$1 \to 4$: Each submodule is a direct summand.
$4 \to 1$: Obvious. □

Theorem 8.1.10. *Let $M = \oplus_{i=1}^{n} M_i$ be an R-module. We define the ring $Mat_R(M)$ as an $n \times n$ matrix and its (i, j) entry $\in hom_R(M_i, M_j)$. We define $f : End_R(M, M) \mapsto Mat_R(M)$ as $f(\phi)_{ij} = \pi_j(\phi|_{M_i})$. Then f is a ring isomorphism.*

Corollary 8.1.11. *Let M be a finitely generated semi-simple R-module, and $M = \oplus n_i S_i$ be a simple decomposition. Then there's a ring isomorphism $End_R(M) \simeq \prod M(End_R(nS_i)) \simeq \prod M_{n_i}(End_R(S_i))$.*

Proof. Since $hom_R(n_i S_i, n_j S_j) = 0$ when $i \neq j$. □

8.2 Semiprimitive Ring, Semisimple Ring & Semisimple algebra

Theorem 8.2.1. *Let R be a ring, A be the class of simple R modules. Then we have an alternative definition of Jacobson radical*

$$Jac(R) = \bigcap_{M \in A} ann(M) \tag{8.1}$$

And $Jac(R)$ is a two-sided ideal.

Proof. Just observe each maximal ideal $\mathfrak{m}$ is the annihilator of simple module $R/\mathfrak{m}$, and each $ann(M)$ is a maximal ideal if M is a simple module. $Jac(R)$ is a two sided ideal since each $ann(M)$ is a two sided ideal. □

Definition 8.2.2. *A ring R is called* **semiprimitive** *if $Jac(R) = 0$.*

Theorem 8.2.3. *Let N be a two-sided ideal of R and $N \subseteq Jac(R)$, then $Jac(R/N) \simeq Jac(R)/N$.*

Proof. There is a 1-1 map $\mathfrak{m} \leftrightarrow \mathfrak{m}/N$ between maximal ideals of R and maximal ideals of R/N. □

Corollary 8.2.4. *$R/Jac(R)$ is semiprimitive.*

Definition 8.2.5. *A ring R is called semisimple if any finitely generated R-module is semi-simple. Especially, R as a finitely generated R-module is semi-simple.*

Theorem 8.2.6. *A Ring R is semi-simple if R as a finitely generated R-module is semi-simple.*

Proof. Any finitely generated R-module is a quotient module of R^n. □

Theorem 8.2.7. *A semi-simple ring is Noetherian and Artinian.*

Proof. It's finitely generated. □

Theorem 8.2.8. *Finite direct product of semi-simple rings is a semi-simple ring.*

Proof. Let $R_i = \oplus_j S_j^{[i]}$ be the simple ideal decomposition of semi-simple ring R_i. Then the simple ideal decomposition of $\prod_i R_i$ is $\prod_i R_i = \oplus_{i,j} S_j^{[i]}$. □

Definition 8.2.9. *A ring is called* **simple** *if it has only trivial two-sided ideals.*

Theorem 8.2.10. *Simple Artinian ring is semi-simple.*

Proof. Let R be a simple Artinian ring, and Σ be the sum of all simple ideals of R. R is Artinian $\Rightarrow$ R has a non-zero simple ideal $\Rightarrow$ Σ is not zero. It's easy to see that Σ is a two-sided ideal. By simplicity, $\Sigma = R$. So R is semi-simple. □

Lemma 8.2.11. *Let R be a semiprimitive ring. Then each simple ideal of R is a direct summand.*

Proof. Let I be a non-zero simple ideal of R. $\forall$ maximal ideal $\mathfrak{m} : \mathfrak{m} \cap I = 0$ or I. Since $Jac(R) = 0$, it's impossible that $\forall \mathfrak{m} : \mathfrak{m} \cap I = I$. So let $\mathfrak{m}$ be the maximal ideal such that $\mathfrak{m} \cap I = 0$. Clearly $\mathfrak{m} + I$ is an ideal of R. Since $\mathfrak{m}$ is maximal, $\mathfrak{m} + I = R$. So $R = I \oplus \mathfrak{m}$. □

Theorem 8.2.12. *A ring is semi-simple iff it's Artinian and semi-primitive.*

Proof. Let $R = \oplus_i S_i$ be a semi-simple ring. We have shown that it is Artinian. $x \in Jac(R) \Rightarrow \forall_i x S_i = 0 \Rightarrow xR = 0 \Rightarrow x = 0$. So $Jac(R) = 0$.

Let R be an Artinian ring and $Jac(R) = 0$. R is Artian $\Rightarrow$ each ideal of R contains a non-zero simple ideal. Let I_1 be a non-zero simple ideal of R, form the lemma we see that $\exists \mathfrak{m}_1 : R = I_1 \oplus \mathfrak{m}_1$. Let I_2 be a non-zero simple ideal of $\mathfrak{m}_1$, form the lemma we see that $\exists \mathfrak{m}_2 : R = I_2 \oplus \mathfrak{m}_2$. It's easy to see that $\mathfrak{m}_1 = I_2 \oplus (\mathfrak{m}_1 \cap \mathfrak{m}_2)$. So $R = I_1 \oplus I_2 \oplus (\mathfrak{m}_1 \cap \mathfrak{m}_2)$. Let I_3 be a non-zero simple ideal of $\mathfrak{m}_1 \cap \mathfrak{m}_2$... Repeating this procedure, we have $R = I_1 \oplus I_2 \oplus I_3 \oplus \cdots$. Since R is Artinian, it has finite length. So this procedure must stop somewhere, that is, $\exists n : \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \cdots \cap \mathfrak{m}_{n-1}$ is simple. Then $R = I_1 \oplus I_2 \oplus I_3 \oplus \cdots \oplus I_n$. □

Corollary 8.2.13. *Let R be an Artinian ring. Then $R/Jac(R)$ is a semisimple ring.*

Definition 8.2.14. *An algebra A is semi-simple if it is a semi-simple ring. An algebra A is simple if it is a simple ring.*

Theorem 8.2.15. *Let A be a finitely generated F-algebra. If A is simple, A is semi-simple.*

Proof. Just observe that A is Artinian. □

Theorem 8.2.16. *Let R be a semi-simple ring, and as R module $R = \oplus n_i S_i$. Let M be a simple R-module. Then $\exists i : M \simeq S_i$.*

Proof. $RM = M$, so $\exists m \in M : Rm \neq 0$. Since Rm is a submodule of M and M is a simple module, $Rm = M$. Define $\phi : R \to M$ as $\phi(r) = rm$. ϕ is a epimorphism. So $\exists i : \phi|_{S_i} \neq 0$. By Schur's lemma, $\exists i : \phi|_{S_i}$ is isomorphism. So $\exists i : M \simeq S_i$. □

8.3 Wedderburn Theorem

Theorem 8.3.1. *Let D be a division ring, then $M_n(D)$ is a simple ring. D^n is a simple $M_n(D)$-module, and as an $M_n(D)$ module $M_n(D) \simeq nD^n$.*

Proof. We define $E_{ij} \in M_n(D)$ such that the (i, j)-th entry is 1 and other entries are 0, and $P_{ij} = I - E_{ii} - E_{jj} + E_{ij} + E_{ij}$. Let I be a non-zero two-sided ideal of $M_n(D)$ and $m \neq 0 \in I$. Then $\exists i, j : m_{ij} \neq 0$. Then $E_{ij} = (m_{ij}^{-1} E_{ij}) \cdot m \in I$. Then $\forall pq : E_{pq} = P_{pi} E_{ij} P_{jq} \in I$. So $I = M_n(D)$. So $M_n(D)$ is simple.

Under matrix production, D^n can be viewed as an $M_n(D)$-module. We define $K_i \in D^n$ such that the i-th entry is 1 and other entries are 0. Let J be a non-zero submodule of D^n and $a \neq 0 \in J$. Then $\exists i : a_i \neq 0$. Then $K_i = (a_i^{-1} E_{ii}) \cdot a \in I$. Then $\forall p : K_p = P_{pi} K_i \in I$. So $J = D^n$. So D^n is simple.

Let $S_i = \{m \in M_n(D) |$ only i-th column is non-zero$\}$. Then it's easy to see that $S_i \simeq D^n$. So $M_n(D) = \oplus_i S_i \simeq nD^n$ □

Theorem 8.3.2. *Let R be a ring, there is a ring isomorphism $R^{op} \simeq End_R(R)$. If R is an algebra, then the isomorphism is an algebra isomorphism.*

Proof. For each $a \in R$ we define $\rho_a : R \to R$ as $\rho_a(b) = ba$. It's easy too see that $\rho_a \in End_R(R)$. Clearly $\rho_{ab} = \rho_b \rho_a$. So ρ is an anti-homomorphism $R \to End_R(R)$. So ρ is an homomorphism $R^{op} \to End_R(R)$. $a \in \ker \rho \Rightarrow \forall r \in R : ra = r \Rightarrow a = 1$ So ρ is injective. $\phi \in End_R(R) \Rightarrow \forall r \in R : \phi(r) = \phi(r \cdot 1) = r\phi(1) \Rightarrow \phi = \rho_{\phi(1)}$. So ρ is surjective. So ρ is an isomorphism $R^{op} \simeq End_R(R)$. □

Theorem 8.3.3. *Let F be an algebraic closed field, A a finitely generated F-algebra, S a finitely generated simple A-module. Then $\forall \phi \in End_A(S) \exists \lambda_\phi : \phi = \lambda_\phi id$, and $\phi \to \lambda_\phi$ is a ring isomorphism $End_A(S) \to F$. Thus $End_A(S) \simeq F$.*

Proof. $\forall \phi \in End_A(S)$. Let λ be an eigenvalue of ϕ viewed as a linear transformation. From Shur's lemma, $\phi - \lambda_\phi Id = 0$. So $\forall \phi \in End_A(S) \exists \lambda(\phi) \in F : \phi = \lambda(\phi) Id$. It's easy to see that λ is an ring isomorphism. So $End_A(S) \simeq F$. □

Theorem 8.3.4 (Wedderburn)**.** *Let R be a semi-simple ring, and as R module $R = \oplus n_i S_i$. Then there's ring homomorphism $R \simeq \prod End_{R_i}(R_i)^{op} \simeq \prod M_{n_i}(D_i)$ where $D_i = End_{R_i}(S_i)^{op}$ is division ring. As an R-module, $R_i = n_i S_i \simeq M_{n_i}(D_i) \simeq n_i D_i^{n_i}$. So $S_i \simeq D_i^n$. If R is an F-algebra, then the isomorphism is an algebra isomorphism. If F is algebraically closed, then $D_i \simeq F^{op} \simeq F$. So $R \simeq \prod_i M_{n_i}(F)$.*

Proof. This is the collection of several previous theorems. □

Corollary 8.3.5. *A semi-simple ring is simple iff it has only one isomorphism class of simple ideals.*

Corollary 8.3.6. *A semi-simple ring is simple iff it is isomorphic to $M_n(D)$ for some division ring D.*

Corollary 8.3.7. *A semi-simple ring is the finite direct product of simple rings. A semi-simple algebra is the finite direct product of simple algebras.*

8.4 Group Ring

Definition 8.4.1. *We define the group ring $R[G]$ of G over a ring R is the formal linear combinations of elements of G, with coefficients in R:*

$$\sum_{g \in G} a_g g \tag{8.2}$$

where $a_g \in R$, $g \in G$ and $a_g \neq 0$ for finite g.

$R[G]$ forms a ring under the addition

$$(\sum_{g \in G} a_g g) + (\sum_{g \in G} b_g g) = \sum_{g \in G} (a_g + b_g) g \tag{8.3}$$

and the multiplication

$$(\sum_{g \in G} a_g g) \cdot (\sum_{g \in G} b_g g) = \sum_{g \in G} \sum_{h \in G} (a_g b_h) gh = \sum_{g \in G} (\sum_{h \in G} (a_h b_{h^{-1}g})) g \tag{8.4}$$

$R[G]$ is an R module and an R algebra.

Theorem 8.4.2 (Maschke)**.** *Let G be a finite group and F be a field of character k that is 0 or not divides $|G|$. $F(G)$ is a semi-simple algebra.*

Proof. We only need to prove that any finitely generated $F(G)$ module V is semi-simple.

If V is simple, it's semi-simple.

If V is not simple, let U be a proper nontrivial submodule of V. Let $\pi : V \to U$ be F-linear projection. Define

$$\pi'(v) = \frac{1}{|G|} \sum_{g \in G} g \pi(g^{-1} v) \tag{8.5}$$

Since

$$\begin{aligned}\pi'(hv) &= \frac{1}{|G|}\sum_{g\in G} g\pi(g^{-1}hv) && (8.6)\\ &= h\frac{1}{|G|}\sum_{g\in G} h^{-1}g\pi((h^{-1}g)^{-1}v) && (8.7)\\ &= h\pi'(v) && (8.8)\end{aligned}$$

π' is a $F[G]$-homomorphism from V onto U and $\pi'|_U = id$. It's easy to see that $V = U \oplus \ker\pi'$. So U is a direct summand. □

Theorem 8.4.3. *Let $Z(F[G])$ be the center of $F[G]$. $Z(F[G])$ forms a F-linear space. Let C_i be the conjugacy class of G, $c_i = \sum_{g\in C_i} g \in F[G]$. $\{c_i\}$ is linear independent and forms a basis of $Z(F[G])$.*

Proof. Obviously $Z(F[G])$ forms a F-linear space, and $\{c_i\}$ is linear independent. Let $a = \sum_g a_g g \in Z(F[G])$.

$$\begin{aligned}\forall h \in G : hah^{-1} = a &\Rightarrow \forall g, h \in G : a_{hgh^{-1}} = a_g && (8.9)\\ &\Rightarrow \forall i, g, h \in C_i : a_g = a_h && (8.10)\\ &\Rightarrow a \in (c_i) && (8.11)\end{aligned}$$

So $\{c_i\}$ forms a basis of $Z(F[G])$. □

Corollary 8.4.4. *Dimension of $Z(F[G])$ equals number of conjugacy classes of G.*

Theorem 8.4.5. *$Z(F[G])$ is a subalgebra of $F[G]$.*

Proof.

$$\begin{aligned}&\forall c_1, c_2 \in Z(F[G]), g \in G : c_1c_2g = c_1gc_2 = gc_1c_2 && (8.12)\\ \Rightarrow\ &\forall c_1, c_2 \in Z(F[G])c_1c_2 \in Z(F[G]) && (8.13)\end{aligned}$$

□

Definition 8.4.6. *We define the structure of algebra $Z(F[G])$ as f_{ijk} if $c_ic_j = \sum_k f_{ijk}c_k$.*

8.5 Group representation

In the following sections, let $|G|$ be a finite group. Let F be an algebraically closed field with $char = 0$. Let V be a finite dimensional linear space over F.

Definition 8.5.1. *Let V be a F-linear space and ρ a group homomorphism $G \to GL(V, F)$. (ρ, V) is called a **linear representation** of a group G.*

Example (id, V) is a representation, called the **identity representation**.

Theorem 8.5.2. *Let (ρ, V) be a representation of group G. V is also an $F(G)$ module under the number multiplication*

$$(\sum_{g\in G} a_g g) \circ v = (\sum_{g\in G} a_g \rho(g))v \tag{8.14}$$

Theorem 8.5.3. *There's a 1-1 correspondence between group representation (ρ, V) and $F(G)$ module.*

Proof. Given a (ρ, V) pair, we have a $F(G)$ module by (8.5.2). Given a $F(G)$ module $\forall g \in G$, we define $\rho(g)$ as the map $v \to gv$. Clearly $\rho(g) \in End_F(V)$. Since $\rho(g^{-1})\rho(g) = 1$, $\rho(g) \in GL(V, F)$. It's easy to see that ρ is a group homomorphism. It's easy to see that this map from $F(G)$ module to group representation (ρ, V) is the inverse map of that in (8.5.2). □

In the future, by saying group representation, we may mean either a (ρ, V) pair or a $F(G)$ module.

Definition 8.5.4. *A representation V (as a $F[G]$ module) is said to be irreducible iff it's simple. Otherwise, V is called reducible.*

Theorem 8.5.5. *V is a finite generated $F(G)$ module iff its a finite dimensional F space.*

Definition 8.5.6. *Two group representations (ρ, V) and (ρ', V') are* **equivalent** *if they satisfies the following equivalent conditions:*

1. *They as $F(G)$ modules are isomorphic.*
2. *There's a isomorphism of linear space $T : V \to V'$ such that $\forall g \in G : \rho(g) = T^{-1}\rho'(g)T$.*

As a $F[G]$ module, we have ring and module isomorphism

$$F[G] \simeq \bigoplus_{i=1}^{r} M_{n_i}(F) \tag{8.15}$$

Each irreducible representation corresponds to a simple $F[G]$-module, isomorphic to some $F^{n_i} \subseteq M_{n_i}(\mathbb{C})$.

Definition 8.5.7. *We define the* **degree** *of a representation to be n_i if it is isomorphic to $\mathbb{C}^{n_i}$. We define the* **degree** *of representations of G as $\{n_i\}$ if $\mathbb{C}[G] \simeq \oplus_i M_{n_i}(\mathbb{C})$.*

Theorem 8.5.8.

$$\sum_i n_i^2 = |G| \tag{8.16}$$

Proof.

$$\sum_i n_i^2 = \dim F[G] = |G| \tag{8.17}$$

□

Theorem 8.5.9. *The number of different irreducible representations of $|G|$ equals the number of conjugacy classes.*

Proof. Let $F[G] \simeq \bigoplus_{i=1}^{r} M_{n_i}(F)$. $Z(F[G]) \simeq \bigoplus_{i=1}^{r} Z(M_{n_i}(F)) \simeq F^r$. So $\dim Z(F[G]) = r$. And dimension of $Z(F[G])$ also equals number of conjugacy classes of G. □

Theorem 8.5.10. *Let (ρ, S) be an irreducible representation of $F[G]$ and $\dim S = n$. Then $\bar{\rho}$ extends to a algebra epimorphism $F[G] \to M_n(F)$ and $Z(F[G]) \to F$. Actually, the map $\xi : Z(F[G]) \to F$ can be realized by $\bar{\rho}(c) = \xi(c)I$.*

Proof. Just observe that $a \to ca \in End_{F[G]}(S)$. □

Corollary 8.5.11. $\xi(c_i)\xi(c_j) = \sum_k f_{ijk}\xi(c_k)$

Theorem 8.5.12. *Let U and V be two $F[G]$-modules and (ρ_1, U) and (ρ_2, V) be the corresponding group representations. Then $U \oplus V$ corresponds to the representation $(\rho_1 \oplus \rho_2, U \oplus V)$. $U \otimes_F V$ forms a $F[G]$-module by*

$$g(u \otimes_F v) = gu \otimes_F gv \tag{8.18}$$

This corresponds to the representation $(\rho_1 \otimes_F \rho_2, U \otimes_F V)$.

Theorem 8.5.13. *Let U an $F[G]$-module. From the last theorem, $U \otimes_F U$ forms a $F[G]$-module. Then $U \otimes_F U = S(U \otimes_F U) \oplus A(U \otimes_F U)$ is $F[G]$-module direct sum, where S means the symmetric subspace and A means the anti-symmetric subspace.*

Theorem 8.5.14. *Let U and V be two $F[G]$-modules, $hom_F(U, V)$ forms a $F[G]$-module by*

$$(g\phi)(u) = g\phi(g^{-1}u) \tag{8.19}$$

Definition 8.5.15. *Let U be an $F[G]$-modules, $U^* = hom_F(U, F)$ (F as identity representation) forms a $F[G]$-module called* **dual representation**.

Theorem 8.5.16. *Let U and V be two $F[G]$-modules. We have $\bar{f} : U^* \times V \to hom_F(U, V)$ defined by $f(\phi, v)(u) = \phi(u)v$. $\bar{f}$ induce $f : U^* \otimes V \to hom_F(U, V)$, and f is an $F[G]$-module isomorphism.*

Proof. It's easy to see that f is an $F[G]$-module homomorphism

Let $\{e_i\}$ be the basis of U and $\{e_i^*\}$ be the dual basis. Define $g : hom_F(U, V) \to U^* \otimes V$ as

$$g(\phi) = \sum_i e_i^* \otimes_F \phi(e_i) \tag{8.20}$$

It's easy to see that $gf = fg = 1$. □

8.6 Characters

Let G be a group and $\{C_i\}$ its conjugacy classes, $c_i = \sum_{g \in C_i} g \in Z(F[G])$.

Definition 8.6.1. *Let (ρ, V) be a representation of G. Its character is a map $\chi : G \to F$ defined by*

$$\chi(g) = Tr(\rho(g)) \tag{8.21}$$

Definition 8.6.2. *The character of 1-D representation is called linear character. The character of irreducible representation is called irreducible character.*

Theorem 8.6.3. $\chi(g) = \chi(hgh^{-1})$. *So* $\chi(g)$ *take the same value over a conjugacy class. We may define* $\rho(C_i)$ *as* $\rho(g)$ *for some* $g \in C_i$

Theorem 8.6.4. *Let* (ρ, V) *be a* n*-dimensional representation of* G*,* ξ *be the function defined in (8.5.10). We have*

$$\chi(C_i) = \frac{n}{|C_i|}\xi(c_i) \tag{8.22}$$

Proof.

$$\chi(C_i) = \frac{1}{|C_i|}\sum_{g\in C_i} Tr(\rho(g)) = \frac{1}{|C_i|}Tr(\bar{\rho}(c_i)) = \frac{n}{|C_i|}\xi(c_i) \tag{8.23}$$

□

Corollary 8.6.5. $\frac{|C_i|}{n}\chi(C_i)\frac{|C_j|}{n}\chi(C_j) = \sum_k f_{ijk}\frac{|C_k|}{n}\chi(C_k)$

Corollary 8.6.6. $\frac{|C_i|}{n}\chi(C_i)$ *is an algebraic integer.*

Proof. Since it's the eigenvalue of integer matrix $(f_i)_{jk}$. □

Theorem 8.6.7. *Let* U *and* V *be two representations with characters* χ_U *and* χ_V*. Let* $\chi_{U\oplus V}$*,* $\chi_{U\otimes_F V}$*,* χ_{U^*} *and* $\chi_{hom_F(U,V)}$ *be the character of representation* $U\oplus V$*,* $U\otimes_F V$*,* U^* *and* $hom_F(U,V)$ *respectively. Then*

1. $\chi_{U\oplus V} = \chi_U + \chi_V$
2. $\chi_{U\otimes_F V} = \chi_U \cdot \chi_V$
3. $\chi_{U^*}(g) = \chi_U(g^{-1})$
4. $\chi_{hom_F(U,V)} = \chi_{U^*} \cdot \chi_V$

Proof. 1,2,4:

$$tr(A\oplus B) = tr(A) + tr(B),\ tr(A\otimes_F B) = tr(A)\cdot tr(B),\ hom_F(U,V) \simeq U^*\otimes_F V \tag{8.24}$$

3: Let $\{e_i\}$ be the basis of U and $\{e_i^*\}$ be the dual basis. Then

$$ge_i^* = \sum_j((ge_i^*)(e_j))e_j^* = \sum_j(e_i^*(g^{-1}e_j))e_j^* = \sum_{j,k}(e_i^*((\rho_U(g^{-1}))_{kj}e_k))e_j^* = \sum_j(\rho_U(g^{-1}))_{ij}e_j^* \tag{8.25}$$

So $\chi_{U^*}(g) = \sum_i(\rho_U(g^{-1}))_{ii} = \chi_U(g^{-1})$ □

Definition 8.6.8. Space of group functions *is the dual space of* $\mathbb{F}[G]$ *(as* F*-linear space).* **Space of class functions** *is the space of group functions such that takes constant value in each conjugacy class.*

Theorem 8.6.9. *Let V be a representation of G. We define $V^G = \{v \in V | \forall g \in G : gv = v\}$. Then V^G is a submodule of V and*

$$\dim_F(V^G) = \frac{1}{|G|}\sum_{g\in G}\chi_V(g) \tag{8.26}$$

Proof. It's easy to see that V^G is a submodule of V.

Let $a = \frac{1}{|G|}\sum_{g\in G}$. It's easy to see that $V^G = \{v \in V | av = v\}$. So V^G is the eigenspace of $\bar{\rho}(a)$ with eigenvalue 1. Since $\bar{\rho}(a)^2 = \bar{\rho}(a)$, $x^2 - x$ is an annihilating polynomial of $\rho(a)$. Since $x^2 - x$ have single roots 0 and 1, $\bar{\rho}(a)$ is diagonalizable, with eigenvalues 0 and 1. So $\dim_F V^G = tr(\rho(a)) = \frac{1}{|G|}\sum_{g\in G}\chi_V(g)$ □

Alternative proof. Let $a = \frac{1}{|G|}\sum_{g\in G}$, $\phi \in V^*$. It's easy to see that $a\phi \in hom_{F[G]}(V, F)$, and $\phi \mapsto a\phi$ is a $F[G]$-module homomorphism. It's easy to see that $\dim_F(V^G) = \dim_F hom_{F[G]}(V, F) = tr(a)$. □

Theorem 8.6.10. *Let U and V be a representation of G. Then*

$$\frac{1}{|G|}\sum_{g\in G}\chi_U(g^{-1})\chi_V(g) = \dim_F hom_{F[G]}(U, V) \tag{8.27}$$

Proof. It's easy to see that $hom_{F[G]}(U, V) = hom_F(U, V)^G$, where $hom_F(U, V)$ is a $F[G]$-module. So

$$\begin{aligned}
\dim_F hom_{F[G]}(U, V) &= \dim_F hom_F(U, V)^G && (8.28)\\
&= \frac{1}{|G|}\sum_{g\in G}\chi_{hom_F(U,V)}(g) && (8.29)\\
&= \frac{1}{|G|}\sum_{g\in G}\chi_U(g^{-1})\chi_V(g) && (8.30)
\end{aligned}$$

□

In the following we assume $F = \mathbb{C}$.

Theorem 8.6.11. *Let (ρ, V) be n-dimensional representation of G, and $g \in G$ is of order m. Then $\rho(g)$ is diagonalizable, and its eigenvalues are mth root of unity. So $\chi(g)$ is the sum of n mth roots of unity, and is an algebraic integer.*

Proof. $g^m = 1 \Rightarrow \rho(g)^m = I \Rightarrow x^m - 1$ is the annihilating polynomial of $\rho(g)$. Since $x^m - 1$ have no multiple roots, $\rho(g)$ is diagonalizable and its eigenvalues are mth root of unity. So $\chi(g)$ is the sum of n mth roots of unity, and is an algebraic integer. □

Corollary 8.6.12. *We have $\chi(g^{-1}) = \overline{\chi(g)}$.*

Proof. Since $\chi(g)$ is the sum of n mth roots of unity. □

Corollary 8.6.13. *We have*

1. $\chi_{U^*} = \overline{\chi_U}$

2. $\chi_{hom_F(U,V)} = \overline{\chi_U} \cdot \chi_V$

Definition 8.6.14. *Define the Hermitian inner product on space of class function as*

$$(\alpha, \beta) = \frac{1}{|G|} \sum_{g \in G} \alpha(g)\overline{\beta(g)} \tag{8.31}$$

Theorem 8.6.15. *Let $(\chi_1, \ldots, \chi_r)$ be all dissimilar irreducible characters of group G. Then*

$$(\chi_i, \chi_j) = \delta_{ij} \tag{8.32}$$

Proof.

$$(\chi_i, \chi_j) = \frac{1}{|G|} \sum_{g \in G} \chi_i(g^{-1})\chi_j(g) = \dim_F hom_{F[G]}(S_i, S_j) = \delta_{ij} \tag{8.33}$$

□

Corollary 8.6.16. *$(\chi_1, \ldots, \chi_r)$ is an orthogonal normalized basis of space of class functions.*

Corollary 8.6.17. *Let χ be a character of G. Then χ is a linear combination of $(\chi_1, \ldots, \chi_r)$ with integer coefficients as*

$$\chi = \sum_i (\chi, \chi_i)\chi_i \tag{8.34}$$

Corollary 8.6.18. *Let χ be a character of G. χ is irreducible iff $(\chi, \chi) = 1$.*

Theorem 8.6.19. *Let χ be a character of G, then*

$$\chi'(g) = (\chi(g)^2 \pm \chi(g^2))/2 \tag{8.35}$$

are two characters.

Proof. Let χ be the character of representation (ρ, U). $\forall g \in G$, let $\{e_1, \ldots, e_n\}$ be the basis on which $\rho(g)$ is diagonal. Let $\rho(g)e_i = \lambda_i e_i$. A basis of $A(U \otimes_F U)$ is $\{e_i \otimes_F e_j - e_j \otimes_F e_i\}$. Let the representation function in $A(U \otimes_F U)$ be ρ_A, and the character be χ_A. Then

$$\rho_A(g)(e_i \otimes_F e_j - e_j \otimes_F e_i) = \lambda_i\lambda_j(e_i \otimes_F e_j - e_j \otimes_F e_i) \tag{8.36}$$

So

$$\chi_A(g) = tr(\rho(g)) = \sum_{i<j} \lambda_i\lambda_j = ((\sum_i \lambda_i)^2 - (\sum_i \lambda_i^2))/2 = (\chi(g)^2 - \chi(g^2))/2 \tag{8.37}$$

Since

$$U \otimes_F U = S(U \otimes_F U) \oplus A(U \otimes_F U) \tag{8.38}$$

$$\chi = \chi_A + \chi_S \tag{8.39}$$

So the character of $S(U \otimes_F U)$ is

$$\chi_S(g) = \chi(g) - \chi_A(g) = (\chi(g)^2 + \chi(g^2))/2 \tag{8.40}$$

□

8.7 Character Table

Let G be a finite group. $\{\rho_1, \ldots, \rho_r\}$ be all of its dissimilar complex representations of dimension $\{n_1, \ldots, n_r\}$, and $\{\chi_i, \ldots, \chi_r\}$ be the corresponding characters. Let $\{C_i, \ldots, C_r\}$ be conjugacy classes of G. We usually require ρ_1 to be the identity representation and C_1 to be $\{e\}$.

Definition 8.7.1. *We define the* **character table** *of G as the matrix $\mathfrak{X}$ defined by $\mathfrak{X}_{ij} = \chi_i(C_j)$.*

To find $\mathfrak{X}$ for a given G, we may use the following rules

Theorem 8.7.2.

1. $\chi_1(C_j) = 1$, $\chi_i(C_1) = n_i$.
2. *If $n_i = 1$, then $\chi_i \in hom(G, S^1)$, where S^1 is the unit circle.*
3. $\sum n_i^2 = |G|$.
4. $n_i \big| |G|$.
5. $\frac{|C_i|}{n_a}\chi_a(C_i)\frac{|C_j|}{n_a}\chi_a(C_j) = \sum_k f_{ijk}\frac{|C_k|}{n_a}\chi_a(C_k)$
6. *Row orthogonality relation:* $\sum_i |C_i|\overline{\chi_a(C_i)}\chi_b(C_i) = |G|\delta_{ab}$
7. *Column orthogonality relation:* $\sum_a |C_i|\overline{\chi_a(C_i)}\chi_a(C_j) = |G|\delta_{ij}$
8. *The product of irreducible character and linear character is irreducible character.*

Proof. 4: From 6 we have

$$\sum_i \frac{|C_i|}{n_a}\overline{\chi_a(C_i)}\chi_a(C_i) = \frac{|G|}{n_a} \tag{8.41}$$

The LHS is algebraic integer, so is the RHS. And the RHS $\in \mathbb{Q}$. So the RHS is an integer.

7: Easy to see from 6.

8: Let χ be an irreducible character and χ' be an linear character. Then

$$\begin{aligned}(\chi\chi', \chi\chi') &= \frac{1}{|G|}\sum_{g\in G}\chi(g)\chi'(g)\overline{\chi(g)\chi'(g)} &(8.42)\\ &= \frac{1}{|G|}\sum_{g\in G}\chi(g)\overline{\chi(g)} &(8.43)\\ &= 1 &(8.44)\end{aligned}$$

□

The following are character table of some groups.

8.7.1 Character table of Abelian Group

Let G be a finite abelian group. $G \simeq Z_{m_1} \oplus \cdots \oplus Z_{m_s}$. Then each element forms a conjugacy class and $r = |G|$. So $n_i = 1$. Let ω_k be the kth root of unity. We have irreducible characters

$$\chi_{l_1,\ldots,l_s}(t_1,\ldots,t_s) = \rho_{l_1,\ldots,l_s}(t_1,\ldots,t_s) = \omega_{m_1}^{l_1 t_1} \cdots \omega_{m_s}^{l_s t_s} \tag{8.45}$$

where $(t_1,\ldots,t_s) \in Z_{m_1} \oplus \cdots \oplus Z_{m_s}$

Theorem 8.7.3. *Let G be a subgroup of S_N, then*

$$\chi(C_i) = (\#\text{ of } 1-\text{cycles of } C_i) - 1 \tag{8.46}$$

is a character of G.

Proof. Let $\{e_1,\ldots,e_N\}$ be the basis of N-dimensional linear space. We have the representation

$$\rho(g)e_i = e_{g(i)} \tag{8.47}$$

Its character is

$$\chi(g) = tr(\rho(g)) = \#\text{ of } 1-\text{cycles} \tag{8.48}$$

$\sum_i e_i$ is the submodule of G which is the identity representation. So

$$\chi = \chi_1 + \ldots \tag{8.49}$$

So

$$\chi(C_i) - 1 = (\#\text{ of } 1-\text{cycles of } C_i) - 1 \tag{8.50}$$

is a character of G □

8.7.2 Character table of S_3

We label the conjugacy class of S_3 by its cycle type:

1. $(1,1,1), |C_1| = 1$
2. $(1,2), |C_2| = 3$
3. $(3), |C_3| = 2$

$$n_1^2 + n_2^2 + n_3^2 = |S_3| = 6 \tag{8.51}$$

So

$$n_1 = 1, n_2 = 1, n_3 = 2 \tag{8.52}$$

χ_1 is the identity representation.
We have 1-D representation $\rho(g) = sgn(g)$. So $\chi_2(g) = sgn(g)$.
So the character table of S_3 is

	$C_1(1)$	$C_2(3)$	$C_3(2)$
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	a	b

$\chi_2\chi_3 = \chi_3$, so $a = 0$. From row orthogonality relation, we have $b = -1$.
So the character table of S_3 is

	$C_1(1)$	$C_2(3)$	$C_3(2)$
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

8.7.3 Character table of S_4

We label the conjugacy class of S_4 by its cycle type:

1. $(1,1,1,1), |C_1| = 1$
2. $(1,1,2), |C_2| = 6$
3. $(1,3), |C_3| = 8$
4. $(2,2), |C_4| = 3$
5. $(4), |C_5| = 6$

$$n_1^2 + n_2^2 + n_3^2 + n_4^2 + n_5^2 = |S_4| = 24 \tag{8.53}$$

So

$$n_1 = 1, n_2 = 1, n_3 = 2, n_4 = 3, n_5 = 3 \tag{8.54}$$

χ_1 is the identity representation.
We have 1-D representation $\rho(g) = sgn(g)$. So $\chi_2(g) = sgn(g)$.
So the character table of S_4 is

	$C_1(1)$	$C_2(6)$	$C_3(8)$	$C_4(3)$	$C_5(6)$
χ_1	1	1	1	1	1
χ_2	1	-1	1	1	-1
χ_3	2	a	b	c	d
χ_4	3				
χ_5	3				

$\chi_2\chi_3 = \chi_3$, so $a = d = 0$. From row orthogonality relation, we have

$$2 + 8b + 3c = 0 \tag{8.55}$$

$$4 + 8b^2 + 3c^2 = 24 \tag{8.56}$$

The solution is $b = -1, c = 2$.
So the character table of S_4 is

	$C_1(1)$	$C_2(6)$	$C_3(8)$	$C_4(3)$	$C_5(6)$
χ_1	1	1	1	1	1
χ_2	1	-1	1	1	-1
χ_3	2	0	-1	2	0
χ_4	3				
χ_5	3				

From (8.7.3) we have character $\chi = (3, 1, 0, -1, -1)$. Since $(\chi, \chi) = (9 + 6 + 3 + 6)/24 = 1$, χ is irreducible. We may let $\chi_4 = \chi$. Since $\chi_2\chi_4 \neq \chi_4$, we have $\chi_5 = \chi_2\chi_4$.
So the character table of S_4 is

	$C_1(1)$	$C_2(6)$	$C_3(8)$	$C_4(3)$	$C_5(6)$
χ_1	1	1	1	1	1
χ_2	1	-1	1	1	-1
χ_3	2	0	-1	2	0
χ_4	3	1	0	-1	-1
χ_5	3	-1	0	-1	1

8.7.4 Character Table of A_4

We label the conjugacy class of S_4 by its cycle type:

1. $(1, 1, 1, 1), |C_1| = 1$
2. $(1, 3), |C_2| = 4$
3. $(1, 3), |C_3| = 4$
4. $(2, 2), |C_4| = 3$

where we have used (1.11.4)

$$n_1^2 + n_2^2 + n_3^2 + n_4^2 = |A_4| = 12 \tag{8.57}$$

So

$$n_1 = 1, n_2 = 1, n_3 = 1, n_4 = 3 \tag{8.58}$$

χ_1 is the identity representation.
From (8.7.3) we have character $\chi = (3, 0, 0, -1)$, and $(\chi, \chi) = 1$.
So the character table of A_4 is

	$C_1(1)$	$C_2(4)$	$C_3(4)$	$C_4(3)$
χ_1	1	1	1	1
χ_2	1			a
χ_3	1			b
χ_4	3	0	0	-1

It's easy to see that $\chi_2\chi_4 = \chi_4$ and $\chi_3\chi_4 = \chi_4$. So $a = b = 1$
So the character table of A_4 is

	$C_1(1)$	$C_2(4)$	$C_3(4)$	$C_4(3)$
χ_1	1	1	1	1
χ_2	1	a	c	1
χ_3	1	b	d	1
χ_4	3	0	0	-1

From column orthogonality relation, we have $(c, d) = (1, -2)$ or $(-2, 1)$. Similarly, $(a, b) = (1, -2)$ or $(-2, 1)$. From row orthogonality relation, we can choose $a = -2, b = 1, c = 1, d = -2$.
So the character table of A_4 is

	$C_1(1)$	$C_2(4)$	$C_3(4)$	$C_4(3)$
χ_1	1	1	1	1
χ_2	1	-2	1	1
χ_3	1	1	-2	1
χ_4	3	0	0	-1

8.7.5 Character Table of S_5

We label the conjugacy class of S_5 by its cycle type:

1. $(1, 1, 1, 1, 1), |C_1| = 1$
2. $(1, 1, 1, 2), |C_2| = 10$
3. $(1, 1, 3), |C_3| = 20$
4. $(1, 2, 2), |C_4| = 15$
5. $(1, 4), |C_5| = 30$
6. $(2, 3), |C_6| = 20$
7. $(5), |C_7| = 24$

χ_1 is the identity representation.
We have 1-D representation $\rho(g) = sgn(g)$. So $\chi_2(g) = sgn(g)$.
So the character table of S_5 is

	$C_1(1)$	$C_2(10)$	$C_3(20)$	$C_4(15)$	$C_5(30)$	$C_6(20)$	$C_7(24)$
χ_1	1	1	1	1	1	1	1
χ_2	1	-1	1	1	-1	-1	1
χ_3							
χ_4							
χ_5							
χ_6							
χ_7							

From (8.7.3) we have character $\chi = (4, 2, 1, 0, 0, -1, -1)$, and $(\chi, \chi) = 1$. So $\chi_3 = (4, 2, 1, 0, 0, -1, -1)$ and $\chi_4 = \chi_3\chi_2$
So the character table of S_5 is

	$C_1(1)$	$C_2(10)$	$C_3(20)$	$C_4(15)$	$C_5(30)$	$C_6(20)$	$C_7(24)$
χ_1	1	1	1	1	1	1	1
χ_2	1	-1	1	1	-1	-1	1
χ_3	4	2	1	0	0	-1	-1
χ_4	4	-2	1	0	0	1	-1
χ_5							
χ_6							
χ_7							

From (8.6.19) we have characters $\chi_A = (6, 0, 0, -2, 0, 0, 1)$ and $\chi_S = (10, 4, 1, 2, 0, 1, 0)$. We have $(\chi_A, \chi_A) = 1$ and $(\chi_S, \chi_S) = 3$. We let $\chi_7 = \chi_A$
So the character table of S_5 is

	$C_1(1)$	$C_2(10)$	$C_3(20)$	$C_4(15)$	$C_5(30)$	$C_6(20)$	$C_7(24)$
χ_1	1	1	1	1	1	1	1
χ_2	1	-1	1	1	-1	-1	1
χ_3	4	2	1	0	0	-1	-1
χ_4	4	-2	1	0	0	1	-1
χ_5							
χ_6							
χ_7	6	0	0	-2	0	1	0

Furthermore, $(\chi_S, \chi_1) = 1$ and $(\chi_S, \chi_3) = 1$. So $\chi_5 = \chi_S - \chi_1 - \chi_3 = (5, 1, -1, 1, -1, 1, 0)$ is irreducible, and $\chi_6 = \chi_2\chi_5 = (5, -1, -1, 1, 1, -1, 0)$.

	$C_1(1)$	$C_2(10)$	$C_3(20)$	$C_4(15)$	$C_5(30)$	$C_6(20)$	$C_7(24)$
χ_1	1	1	1	1	1	1	1
χ_2	1	-1	1	1	-1	-1	1
χ_3	4	2	1	0	0	-1	-1
χ_4	4	-2	1	0	0	1	-1
χ_5	5	1	-1	1	-1	1	0
χ_6	5	-1	-1	1	1	-1	0
χ_7	6	0	0	-2	0	1	0

8.7.6 Character Table of A_5

We label the conjugacy class of A_5 by its cycle type:

1. $(1,1,1,1,1), |C_1| = 1$
2. $(1,1,3), |C_2| = 20$
3. $(1,2,2), |C_3| = 15$
4. $(5), |C_4| = 12$
5. $(5), |C_5| = 12$

$$n_1^2 + n_2^2 + n_3^2 + n_4^2 + n_5^2 = |A_5| = 60 \tag{8.59}$$

So

$$n_1 = 1, n_2 = 3, n_3 = 3, n_4 = 4, n_5 = 5 \tag{8.60}$$

So the character table of A_5 is

	$C_1(1)$	$C_2(20)$	$C_3(15)$	$C_4(12)$	$C_5(12)$
χ_1	1	1	1	1	1
χ_2	3				
χ_3	3				
χ_4	4				
χ_5	5				

From (8.7.3) we have character $\chi = (4,1,0,-1,-1)$, and $(\chi,\chi) = 1$. So $\chi_4 = (4,1,0,-1,-1)$
So the character table of A_5 is

	$C_1(1)$	$C_2(20)$	$C_3(15)$	$C_4(12)$	$C_5(12)$
χ_1	1	1	1	1	1
χ_2	3				
χ_3	3				
χ_4	4	1	0	-1	-1
χ_5	5				

From (8.6.19) we have characters $\chi_A = (6, 0, -2, 1, 1)$ and $\chi_S = (10, 1, 2, 0, 0)$. We have $(\chi_A, \chi_A) = 2$ and $(\chi_S, \chi_S) = 3$. We have $(\chi_S, \chi_1) = (\chi_S, \chi_4) = 1$. So $\chi_5 = \chi_S - \chi_1 - \chi_4 = (5, -1, 1, 0, 0)$. Since $(\chi_A, \chi_1) = 0$, $\chi_A = \chi_2 + \chi_3$.

So the character table of A_5 is

	$C_1(1)$	$C_2(20)$	$C_3(15)$	$C_4(12)$	$C_5(12)$
χ_1	1	1	1	1	1
χ_2	3	a	c	e	m
χ_3	3	b	d	f	n
χ_4	4	1	0	-1	-1
χ_5	5	-1	1	0	0

From column orthogonality relation, we have $a = b = 0$, $c = d = -1$, $(e, f) = (\frac{1\pm\sqrt{5}}{2}, \frac{1\mp\sqrt{5}}{2})$ and $(m, n) = (\frac{1\pm\sqrt{5}}{2}, \frac{1\mp\sqrt{5}}{2})$.

So the character table of A_5 is

	$C_1(1)$	$C_2(20)$	$C_3(15)$	$C_4(12)$	$C_5(12)$
χ_1	1	1	1	1	1
χ_2	3	0	-1	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$
χ_3	3	0	-1	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$
χ_4	4	1	0	-1	-1
χ_5	5	-1	1	0	0

8.8 Application to Group Theory

Lemma 8.8.1. *Let H be a normal subgroup of G, and let (V, ρ) be a representation of group G/H with character $\chi_{G/H}$. Then $(V, \rho \circ \pi)$ is a representation of group G with character $\chi_G(g) = \chi_{G/H}([g])$. And χ_G is irreducible iff $\chi_{G/H}$ is irreducible.*

Lemma 8.8.2. *Let H be a normal subgroup of G, and let (V, ρ) be a representation of group G with character χ_G, such that $H \subseteq \ker \rho$. Define $\rho'([g]) = \rho(g)$. Then ρ' is well-defined and (V, ρ') is a representation of group G/H with character $\chi_{G/H}([g]) = \chi_G(g)$. And χ_G is irreducible iff $\chi_{G/H}$ is irreducible.*

With these lemma, we can construct the character table of G/H from the character table of G.

8.8.1 Solvability

Definition 8.8.3. *Let (ρ, V) be a representation of G with character χ. We define*

$$K_\chi = \{g \in G | \chi(g) = \chi(e)\} \tag{8.61}$$

Theorem 8.8.4. *Let (ρ, V) be a representation of G with character χ. Then $K_\chi = \ker \rho$ and is therefore a normal subgroup of G.*

Definition 8.8.5. *Let $\{\chi_1, \dots, \chi_r\}$ be all irreducible characters of G. We define $K_i = K_{\chi_i}$.*

Theorem 8.8.6. *Let $H \triangleleft G$. Then $H = \cap_{i \in I} K_i$ where $I \subseteq 1, \dots, r$.*

Proof. Let $(\rho, \mathcal{C}[G/H])$ be the left regular representation of G/H with character $\chi_{G/H}$. This induce a representation of G as $(\rho \circ \pi, \mathcal{C}[G/H])$ with character χ_G. Since left regular representation has a trivial kernel, $K_{\chi_G} = \ker(\rho \circ \pi) = \ker \pi = H$. So $K_{\chi_G} = H$. Let $\{\chi_1, \dots, \chi_r\}$ be all irreducible characters of G, and $\chi_G = \sum_{i \in I} c_i \chi_i$ $(0 < c_i \in \mathbb{Z})$. It's easy to see that $\chi_G(g) = \chi_G(e) \Leftrightarrow \forall i \in I : \chi_i(g) = \chi_i(e) \Leftrightarrow g \in K_i$. So $H = K_{\chi_G} = \cap_{i \in I} K_i$. □

Method 8.8.7. *We can decide if G is solvable from its character table.*

8.8.2 Nilpotenty

Definition 8.8.8. *Let (ρ, V) be a representation of G with character χ. We define*

$$Z_\chi = \{g \in G | |\chi(g)| = \chi(e)\} \tag{8.62}$$

Theorem 8.8.9. *Let (ρ, V) be a representation of G with character χ. $g \in Z_\chi \Leftrightarrow \exists \lambda : \rho(g) = \lambda I$.*

Proof. Let V be of d dimension. Then $\forall g \in G : \chi(g) = \sum_{i=1}^{d} \lambda_i$, where λ_i are roots of unit. Clearly $|\chi(g)| = \chi(e) = n \Leftrightarrow \lambda_1 = \cdots = \lambda_n \Leftrightarrow \exists \lambda : \rho(g) = \lambda I$. □

Corollary 8.8.10. *Z_χ is a subgroup of G.*

Definition 8.8.11. *Let $\{\chi_1, \dots, \chi_r\}$ be all irreducible characters of G. We define $Z_i = Z_{\chi_i}$.*

Theorem 8.8.12. *$Z_i/K_i = Z(G/K_i)$*

Proof. Let (ρ_i, V_i) be the ith irreducible representation of G with character χ_i. $[g] \in Z(G/K_i) \Leftrightarrow \forall h \in G : [g][h] = [h][g] \Leftrightarrow \forall h \in G : \rho_i(g)\rho_i(h) = \rho_i(h)\rho_i(g) \Leftrightarrow x \to \rho_i(g)x$ is a $\mathbb{C}[G]$ module homomorphism. From (8.3.3) we see this $\Leftrightarrow \exists \lambda : \rho_i(g) = \lambda I \Leftrightarrow g \in Z_i \Leftrightarrow [g] \in Z_i/K_i$. □

Corollary 8.8.13. *If G is a non-abelian simple group, $\forall i \neq 1 : Z_i = \{e\}$*

Proof. If G is a non-abelian simple group, $\forall i \neq 1 : K_i = \{e\}$. So $\forall i \neq 1 : Z_i = Z(G) = \{e\}$ □

Theorem 8.8.14. *$Z(G) = \cap_i Z_i$.*

Proof. $\forall i : Z(G)K_i/K_i \subseteq Z(G/K_i) = Z_i/K_i$. So $\forall i : Z(G) \subseteq Z_i$. So $Z(G) \subseteq \cap_i Z_i$. On the other side, $g \in \cap_i Z_i \Rightarrow \forall h \in G, i : [g]_{K_i}[h]_{K_i}[g^{-1}]_{K_i} = [e]_{K_i} \Rightarrow \forall h \in G, i : ghg^{-1} \in K_i \Rightarrow \forall h \in G : ghg^{-1} \in \cap_i K_i = \{e\} \Rightarrow g \in Z(G)$. So $\cap_i Z_i \subseteq Z(G)$. So $Z(G) = \cap_i Z_i$. □

Method 8.8.15. *We can decide if G is nilpotent from its character table.*

Detail. Let $1 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots$ be an upper central series. From the character table of G we can decide $G_1 = Z(G) = \cap_i Z_i$. We can also decide the character table of G/G_1. Then we can decide G_2 and so on. □

8.8.3 Burnside Theorem

Lemma 8.8.16. *Let $\lambda_1, \cdots, \lambda_n$ be roots of unity. Then*

$$\frac{\sum_i \lambda_i}{n} \tag{8.63}$$

is an algebraic integer iff $\lambda_1 = \cdots = \lambda_n$.

Corollary 8.8.17. *Let χ be a character of G. $\chi(g)/\chi(e)$ is an algebraic integer iff $g \in K_\chi$.*

Lemma 8.8.18. *Let G be a group. If G contains a conjugacy class of order p^k (p prime and $k > 0$), G is not simple.*

Proof. Clearly G is non-abelian. Let C_j be the conjugacy class of order p^k. By column orthogonality relation $\sum_i \chi_i(g)\chi_i(e) = \sum_i \chi_i(g)n_i = 0$. So $\frac{1}{p} + \sum_{i=2}^r \frac{n_i}{p}\chi_i(g) = 0$. So $\exists 2 \leq i \leq r : \frac{n_i}{p}\chi_i(g)$ is not an algebraic integer. So $p \not| n_i$. Since $|C_j| = p^k$. $\exists a, b \in \mathbb{Z} : an_i + b|C_j| = 1$. So $\frac{\chi_i(g)}{n_i} = \frac{\chi_i(g)}{n_i}(an_i + b|C_j|) = \chi_i(g)a + \frac{\chi_i(g)}{n_i}b|C_j|$ is a an algebraic integer. So $g \in Z_i$. So Z_i is not $\{e\}$. Thus G is not simple. □

Theorem 8.8.19 (Burnside)**.** *Let p and q be prime. Group of order $p^a q^b$ is solvable.*

Proof. Let G be a group of $p^a q^b$. We prove this by induction on $a + b$. If $a + b = 0, 1$ G is abelian and thus solvable. If G is solvable when $a + b = 1 \cdots d$. When $a + b = d + 1$, if G is abelian, clearly G is solvable. If G is non-abelian (so $a, b > 1$), we want to find a proper normal subgroup of G.

Let Q be a q-Sylow group. Q is a q-group. So $Z(Q) \neq 1$. Let $1 \neq g \in Z(Q)$. Then $Q \subseteq C_G(g)$. Let $g \in C_i$ is a conjugacy class. $|C_i| = [G : C_G(g)] = p^{m'}$. If $m' = 0$, $g \in Z(G)$. So G has a proper normal subgroup H. If $m' > 0$, by the previous lemma, G has a proper normal subgroup H. By the induction condition, H and G/H are solvable. So G is solvable. □

8.9 Restriction and Induced Representation

Definition 8.9.1. *Let H be a subgroup of G, and U be a $F[G]$ module. We define the* **restriction** *of U on H by U viewed as $F[H]$ module, denoted by $\mathrm{Res}^G_H U$. Let χ be the character of U. We denote the character of $\mathrm{Res}^G_H U$ by $\chi|_H$. Clearly $\forall h \in H : \chi|_H(h) = \chi(h)$.*

Definition 8.9.2. *Let H be a subgroup of G, and V be a $F[H]$ module. $F[G]\otimes H$ forms a $F[G]$-module by $g(x\otimes v) = gx\otimes v$. Let Y be a subspace of $F[G]\otimes H$ spanned by $\{gh\otimes v - g\otimes hv | g\in G, h\in H, v\in V\}$. It's easy to see that Y is a $F[G]$-submodule. We define the quotient module $F[G]\otimes H/Y$ as the* **induced representation** *of V to G, denoted by $\mathrm{Ind}_H^G V$. And we simply denote $[g\otimes v]\in \mathrm{Ind}_H^G V$ as $g\otimes v$. Let χ be the character of V. We denote the character of $\mathrm{Ind}_H^G V$ by χ^G.*

Theorem 8.9.3. $\dim_F(\mathrm{Ind}_H^G V) = [G:H]\dim_F V$. *And if $\{e_1,\dots,e_n\}$ is a basis of V and $t_1,\dots,t_m$ are representative elements of left cosets of H in G, then $\{t_i\otimes e_j\}$ forms a basis of $\mathrm{Ind}_H^G V$.*

Proof. let $g = t_i h'$, then $gh\otimes v - g\otimes hv = (t_i h' h\otimes v - t_i\otimes h'hv) - (t_i h'\otimes hv - t_i\otimes h'hv)$. So Y is spanned by $\{t_i h\otimes e_i - t\otimes he_i | 1\neq h\in H\}$. So $\dim_F Y \le [G:H](1-|H|)\dim_F V$. Since $\dim_F F[G]\otimes H = |G|\dim_F V$, $\dim_F(\mathrm{Ind}_H^G V)\ge [G:H]\dim_F V$. Since in $\mathrm{Ind}_H^G V$, $g\otimes v = t_i\otimes h'v$, $\{t_i\otimes e_i\}$ generates $\mathrm{Ind}_H^G V$. So $\dim_F(\mathrm{Ind}_H^G V) = [G:H]\dim_F V$, and $\{t_i\otimes e_j\}$ forms a basis of $[G:H]\dim_F V$. □

Theorem 8.9.4 (Frobenius)**.** *Let H be a subgroup of G, U be a $F[G]$ module and V be a $F[H]$ module. Then there's a F-linear isomorphism*

$$Hom_{F[H]}(V, \mathrm{Res}_H^G U) = Hom_{F[G]}(\mathrm{Ind}_H^G V, U) \tag{8.64}$$

Corollary 8.9.5. *Let H be a subgroup of G, U be a $F[G]$ module with character χ and V be a $F[H]$ module with character χ'. Then*

$$(\chi', \chi|_H)_H = (\chi'^G, \chi)_G \tag{8.65}$$

Theorem 8.9.6. *Let H be a subgroup of G, and (ρ, V) be a representation of H with character χ. Let $T = \{t_1,\dots,t_m\}$ be representative elements of left cosets of H in G. Then*

$$X^G(g) = \sum_{t\in T, t^{-1}gt\in H} \chi(t^{-1}gt) \tag{8.66}$$

Proof. Let $\{e_1,\dots,e_n\}$ is a basis of V. Then $\{t_i\otimes e_j\}$ forms a basis of $\mathrm{Ind}_H^G V$. Let $(\rho^G, \mathrm{Ind}_H^G V)$ be the representation of G.

$$\rho^G(g)(t_i\otimes e_j) = gt_i\otimes e_j = t_k(t_k^{-1}gt_i)\otimes e_j = t_k\otimes (t_k^{-1}gt_i)e_j \tag{8.67}$$

where $t_k^{-1}gt_i\in H$.

So

$$\chi^G(g) = tr(\rho^G(g)) = \sum_i \delta_{ki} tr(\rho(t_k^{-1}gt_i)) = \sum_i \delta_{ki}\chi(t_i^{-1}gt_i) = \sum_{t\in T, t^{-1}gt\in H}\chi(t^{-1}gt) \tag{8.68}$$

□

Corollary 8.9.7. *Let H be a subgroup of G, and (ρ, V) be a representation of H with character χ. Then*

$$X^G(g) = \frac{1}{|H|}\sum_{x\in G, x^{-1}gx\in H}\chi(x^{-1}gx) \tag{8.69}$$

Let C be the G-conjugacy class that contains g, and $B_1, \ldots, B_r$ be the H-conjugacy class in C, and $h_i \in B_i$. Then

$$X^G(g) = \frac{1}{|H|} \sum_i |B_i| C_G(g) \chi(h_i) = [G:H] \sum_i \frac{|B_i|}{|C|} \chi(h_i) \tag{8.70}$$

Proof. Let $X_i = \{x \in G | x^{-1} g x \in B_i\}$. It's easy to see that $|X_i| = |B_i| C_G(g)$. □

Example 8.9.8. *Decide the character of dihedral group $D_n = \langle \sigma\tau | \sigma^n = \tau^2 = 1, \tau\sigma\tau = \sigma^{-1} \rangle$ from the character of C_n.*

solution.

$$\begin{aligned}
\sigma^i \sigma^j (\sigma^i)^{-1} &= \sigma^j && (8.71)\\
\tau\sigma^i \sigma^j (\tau\sigma^i)^{-1} &= \sigma^{-j} && (8.72)\\
\sigma^i \tau\sigma^j (\sigma^i)^{-1} &= \tau\sigma^{-2i-j} && (8.73)\\
\tau\sigma^i \tau\sigma^j (\tau\sigma^i)^{-1} &= \tau\sigma^{2i+j} && (8.74)
\end{aligned}$$

So when n is odd, D_n have conjugacy classes: $\{1\}$, $\{\sigma^i, \sigma^{n-i}\}$ $(i = 1, \ldots, (n-1)/2)$ and $\{\tau, \ldots \tau\sigma^{n-1}\}$. When n is even, D_n have conjugacy classes: $\{1\}$, $\{\sigma^i, \sigma^{n-i}\}$ $(i = 1, \ldots, n/2-1)$, $\{\sigma^{n/2}\}$, $\{\tau, \tau\sigma^2, \ldots \tau\sigma^{n-2}\}$ and $\{\tau\sigma, \tau\sigma^3, \ldots \tau\sigma^{n-1}\}$.

The character of $C_n \subset D_n$ is $\chi_i(\sigma^m) = \zeta_n^{im}$. We can calculate the induced character

$$\begin{aligned}
\chi_i^G(\sigma^m) &= \zeta_n^{im} + \zeta_n^{-im} && (8.75)\\
\chi_i^G(\tau\sigma^m) &= 0 && (8.76)
\end{aligned}$$

It's easy to see that χ_i^G $(1 \le i \le (n-1)/2$ when i odd and $1 \le i \le n/2 - 1$ when i even) are irreducible characters of 2d representation.

The lacking linear characters are:

$$\begin{aligned}
&\chi_1(g) = 1 && (8.77)\\
&\chi_2(\sigma^m) = 1,\ \chi_2(\tau\sigma^m) = -1 && (8.78)
\end{aligned}$$

when n is odd and

$$\begin{aligned}
&\chi_1(g) = 1 && (8.79)\\
&\chi_2(\sigma^m) = 1,\ \chi_2(\tau\sigma^m) = -1 && (8.80)\\
&\chi_3(\sigma^m) = (-1)^m,\ \chi_3(\tau\sigma^m) = (-1)^m && (8.81)\\
&\chi_4(\sigma^m) = (-1)^m,\ \chi_4(\tau\sigma^m) = -(-1)^m && (8.82)
\end{aligned}$$

when n is even. □

Theorem 8.9.9. *Let p, q be prime and $p \equiv 1 \mod q$. There's a unique non-abelian group denoted by $F_{p,q}$ of order pq.*

Proof. First we prove the existence by giving an explicit construction. Let

$$G = \left\{ \begin{pmatrix} 1 & y \\ 0 & x \end{pmatrix} | x \in F_p^*, y \in F_p \right\} \tag{8.83}$$

Since $q \big| |F_p^*| = p-1$, there exists $r \in F_p^*$ of order q. Let

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 \\ 0 & r \end{pmatrix} \tag{8.84}$$

It's easy to see that

$$A^p = B^q = I, B^{-1}AB = A^r \tag{8.85}$$

Let H be the subgroup of G generated by A and B. It's easy to see that H is a non-abelian group of order pq.

Next we prove the uniqueness. Clearly $p > q$. So $F_{p,q}$ has a unique Sylow p-subgroup $H = \{a^i\}_{0 \le i \le p-1}$. So H is a normal subgroup. Let $T = \{b^i\}_{0 \le i \le q-1}$ be a Sylow q-subgroup. It's easy to see that $F_{p,q} = \{a^i b^j\}_{0 \le i \le p-1, 0 \le j \le q-1}$. Since $bab^{-1} \in H$, $bab^{-1} = a^r$. Since $F_{p,q}$ is non- abelian, $r \neq 1$. $b^q a b^{-q} = a^{r^q} = a$. So $r^q \equiv 1 \mod p$. So $r \in F_p^*$ is of order q, which exists. Since $x^q = 1$ has at most q roots, $r \in \{\omega, \ldots, \omega^{q-1}\}$, where ω is a qth root of unity. So if r and r' are of order q, $\exists n : r' = r^n$. If $F_{p,q} = \{a, b, : a^p = 1, b^q = 1, bab^{-1} = a^r\}$ and $F'_{p,q} = \{a, b, : a^p = 1, b^q = 1, bab^{-1} = a^{r^n}\}$, then $g : F_{p,q} \mapsto F'_{p,q}$ defined by $g(a) = a, g(b) = b^n$ is a group isomorphism. So $F_{p,q}$ is unique. □

Example 8.9.10. *Let p, q be prime and $p \equiv 1 \mod q$. Calculate the character table of $F_{p,q}$.*

Solution. Let $F_{p,q} = \{a, b, : a^p = 1, b^q = 1, bab^{-1} = a^r\}$. First we find the conjugacy class of $F_{p,q}$. Since

$$(a^i b^j)(a^x b^y)(a^i b^j)^{-1} = a^i b^j a^x b^{y-j} a^{-i} = a^{i(1-r^y)+xr^j} b^y \tag{8.86}$$

Let $K = \{1, r, \ldots, r^{q-1}\}$ be the subgroup of F_p^* of order q, and $S = \{s_i\}$ be the set of representative elements of cosets. It's easy to see that the conjugacy classes are

$$C_0 = \{1\} \tag{8.87}$$
$$C_i = \{a^{s_i r^j} | j = 1 \ldots q\} (i = 1 \ldots (p-1)/q) \tag{8.88}$$
$$C'_i = \{a^j b^i | j = 1 \ldots p-1\} (i = 1 \ldots q-1) \tag{8.89}$$

Let $H = \{a^i\}_{0 \le i \le p-1}$ be a normal subgroup of G. Then $G/H = \{[b]^i\}_{0 \le i \le q-1}$ has linear representations

$$\chi_{n,G/H}([b]^j) = e^{2\pi i n j/q} \tag{8.90}$$

This induce the linear representations of G

$$\chi_n(a^s b^t) = e^{2\pi i n t/q} \tag{8.91}$$

H has representations

$$\chi_{n,H}(a^j) = e^{2\pi i n j/p} \tag{8.92}$$

which induces representations of G as

$$\begin{aligned} \chi^G_{n,H}(1) &= p && (8.93)\\ \chi^G_{n,H}(a^x) &= \sum_k e^{2\pi i n x r^k/p} && (8.94)\\ \chi^G_{n,H}(a^x b^y) &= 0 && (8.95)\\ & && (8.96) \end{aligned}$$

It's easy to see that $\chi^G_{n,H} = \chi^G_{nr,H}$. So we may define $\chi'_n = \chi^G_{s_n,H}$ and

$$\begin{aligned} \chi'_n(1) &= p && (8.97)\\ \chi'_n(a^x) &= \sum_k e^{2\pi i s_n x r^k/p} && (8.98)\\ \chi'_n(a^x b^y) &= 0 && (8.99)\\ & && (8.100) \end{aligned}$$

It's easy to see that $\chi'_n|_H = \sum_k \chi_{s_n r^k,H}$. So by the Frobenius theorem,

$$(\chi'_n, \chi'_n)_G = (\chi^G_{s_n,H}, \chi'_n)_G = (\chi_{s_n,H}, \chi'_n|_H)_H = 1 \quad (8.101)$$

So χ'_n are irreducible characters. χ'_n and χ_n are all characters of $F_{p,q}$. □

Chapter 9

Lie Group & Lie Algebra

Mathematically a Lie group is a group which is also a N-D differentiable manifold. Physically, we normally care a concrete matrix group (which mathematicians call linear representations of a Lie group) more than an abstract Lie group. Thus in this introduction, we may define a Lie group to be a matrix group $T(g)$ which can locally be expressed as $T(x)$ where $x \in \mathbb{R}^N$ and T is differentiable.

When differentiability meets group, many interesting properties emerge. Sophius Lie pointed out that a simply-connected Lie group is uniquely determined by its property in the neighborhood if identity. That leads to the study of Lie algebra, which can be interpreted as the first order derivatives of Lie group at the identity.

For our matrix group, we pick a parameterization near identity, and choose the local coordinate such that $T(0) = I$. The Lie algebra is defined as the N dimensional linear space of matrices

$$V = c_i \partial_i T(0) \tag{9.1}$$

, that is, all the directional derivatives at identity.

We define the commuter of matrices as

$$[A, B] = AB - BA \tag{9.2}$$

By definition we have

$$[A, B] = -[B, A] \tag{9.3}$$

$$[[A, B], C] + [[B, C], A] + [[C, A], B] = 0 \tag{9.4}$$

The Lie algebra has many properties. A prominent one is that

$$\forall g, X \in V : T(g) X T(g)^{-1} \in V \tag{9.5}$$

This can be prove by analyze $T(g)T(x(a))T(g)^{-1}$ where $X = \partial_a T(x(a))|_{a=0}$ and $x(0) = 0$. We can choose a so small that $T(g)T(x(a))T(g)^{-1}$ is also in the neighborhood of identity, that is

$$T(g)T(x(a))T(g)^{-1} = T(x(f(a))) \tag{9.6}$$

Clearly $f(0) = 0$ and it can be proved that $f(a)$ is differentiable. So take the derivative on both sides, we have

$$T(g) X T(g)^{-1} \in V \tag{9.7}$$

If $T(g)$ is also near the identity, we can expressed is as $T(y)$. We have

$$T(y)XT(y)^{-1} = Y(y) \in V \tag{9.8}$$

Then take the derivative of y on both sides along some path, we have

$$[X, Y] \in V \tag{9.9}$$

which is a highly non-trivial result.

We can choose a basis X_i of the Lie algebra. Thus

$$[X_i, X_j] = f_{ijk} X_k \tag{9.10}$$

where $f_{ijk} = -f_{jik}$ is called the structure factor of the Lie algebra.

For physicists, Lie groups describe the continuous symmetry of physical systems. And $SU(2)$ Lie algebra sometimes enters the Hamiltonian when dealing with spin.

9.1 Lie Algebra

Definition 9.1.1. *Let L be a linear space over a field F with a bilinear operation $(x, y) \mapsto [x, y]$ that satisfies*

1. $[X, X] = 0$
2. **Jacobi identity***:* $[[X, Y], Z] + [[Y, Z], X] + [[Z, X], Y] = 0$

L is then called a **Lie algebra**.

Definition 9.1.2. *Let L be a Lie algebra with basis L_i (and dual basis L^i), and*

$$[L_i, L_j] = f_{ij}^k L_k. \tag{9.11}$$

f_{ij}^k is called the **structure factor** *of L. Actually $f_{ij}^k L^i L^k L_k$ is a tensor.*

Definition 9.1.3. *A* **linear representation** *is a non-singular map $T : L \mapsto hom(V)$ from Lie algebra to operator such that*

$$[T(X), T(Y)] = T([X, Y]) \tag{9.12}$$

For each Lie algebra, we define the **adjoint representatio**n as

$$ad(X) \cdot Y = [X, Y] \tag{9.13}$$

Under the basis we chosen

$$ad(X_i)_{jk} = f_{ikj} \tag{9.14}$$

Exercise 9.1.1

Check (9.12) for the adjoint representation.

From the adjoint representation we define the **Killing form**

$$B(X,Y) = \mathrm{Tr}[ad(X)\cdot ad(Y)] \tag{9.15}$$

Exercise 9.1.2

Test that $B[[X,Y]Z] = B[X,[Y,Z]]$.

If we choose a new basis $X'_i = L_{ij}X_j$. Then

$$\begin{aligned} B(X'_i, X'_j) &= B(L_{im}X_m, L_{jn}X_n) && (9.16)\\ &= L_{im}L_{jn}B(X_m, X_n) && (9.17)\end{aligned}$$

This is a congruence transformation. thus we can choose a basis so that

$$B(X_i, X_j) = \lambda \mathrm{diag}(1\cdots 1, -1\cdots -1, 0\cdots 0)_{ij} \tag{9.18}$$

For the time being, we only care about the Lie algebra whose Killing form is negative definite. This is called compact Lie algebras, which are the Lie algebras for compact Lie groups. Thus $B(X_i, X_j) = -\lambda\delta_{ij}$.

Thus in this basis, it's easy to see that

$$\begin{aligned} f_{ijk} &= \frac{1}{\lambda}B([[X_i, X_j], X_k]) && (9.19)\\ &= \frac{1}{\lambda}B([X_i, [X_j, X_k]]) && (9.20)\\ &= f_{jki} && (9.21)\end{aligned}$$

Thus

$$f_{ijk} = f_{jki} = f_{kij} = -f_{jik} = -f_{ikj} = -f_{kji} \tag{9.22}$$

That is to say, f_{ijk} is antisymmetric.

For physicists, the definition of Lie algebra is a little different from the mathematics. The physicists generally deals with unitary representation of Lie groups, which acts on a Hilbert space with definite physical meaning. So they generally don't distinguish between a Lie group and its unitary representation. And Lie algebra enters as a natural candidate for observables. Physicists define observables to be Hermitian operators. But for mathematicians, the Lie algebra of a unitary representation of a Lie group is its derivative at unit, which is anti-Hermitian. Thus physicist adds an i to the mathematician Lie algebra to be what they called Lie algebra. That's to say:

$$X_{\mathrm{phy}} = iX_{\mathrm{math}} \tag{9.23}$$

And the Lie bracket for basis becomes

$$[X_i, X_j] = if_{ijk}X_k \tag{9.24}$$

9.2 The su(2) Lie Algebra

su(2) Lie algebra is a 3-D Lie algebra with Lie bracket of basis as (in physicists' notation)

$$[X_i, X_j] = i\epsilon_{ijk}X_k \tag{9.25}$$

Exercise 9.2.1

Test that the Killing form $B(-iX_i, -iX_j) = -2\delta_{ij}$. Thus the **su**(2) is a compact Lie algebra.

Then we want to derive all the inequivalent irreducible finite-dimensional Hermitian representations of **su**(2). For this purpose, we only need to reduce an arbitrary finite-dimensional representation of **su**(2) and see what we can get.

Assume H is the representation space for **su**(2), and we have a Hermitian inner product over H. We define the ladder operator:

$$X_\pm = \frac{X_1 \pm iX_2}{\sqrt{2}} \tag{9.26}$$

They are outside the original Lie algebra but we don't care. They satisfy the commutation rule

$$\begin{aligned} [X_3, X_\pm] &= \pm X_\pm & (9.27)\\ [X_+, X_-] &= X_3 & (9.28) \end{aligned}$$

Since X_3 is Hermitian, we can diagonalize it. For the eigenstate $|n\rangle$ of X_3 with eigenvalue n

$$\begin{aligned} X_3X_-|n\rangle &= X_-X_3|n\rangle + [X_3, X_-]|n\rangle & (9.29)\\ &= X_-n|n\rangle - X_n|n\rangle & (9.30)\\ &= (n-1)X_-|n\rangle & (9.31)\\ X_3X_+|n\rangle &= X_+X_3|n\rangle + [X_3, X_+]|n\rangle & (9.32)\\ &= X_+n|n\rangle + X_n|n\rangle & (9.33)\\ &= (n+1)X_+|n\rangle & (9.34) \end{aligned}$$

Thus $X_-|n\rangle$ (if not 0) is an eigenstate with eigenvalue $n-1$, and $X_+|n\rangle$ (if not 0) is an eigenstate with eigenvalue $n+1$.

Since H is finite-dimensional, we can find normalized eigenstate $|m\rangle$ with largest eigenvalue m of X_3. We may have many of them, but we only choose one. Clearly $X_+|m\rangle = 0$. Let's assume $X_-|m\rangle \neq 0$ and define $X_-|m\rangle = C_{m-1}|m-1\rangle$ where C_{m-1} is a real and positive factor such that $|m-1\rangle$ is normalized. We can repeat this procedure until we get $|m-s\rangle$ and $X_-|m-s\rangle = 0$, that is, $C_{m-s-1} = 0$ and $C_{m-n} \neq 0$ $(1 \leq n \leq s)$. This must happen somewhere since H is finite-dimensional.

Then we prove that $X_+|m-n\rangle = \alpha|m-n+1\rangle$ $(1 \leq n \leq s)$. Since

$$\begin{aligned} X_+|m-1\rangle &= C_{m-1}^{-1}X_+X_-|m\rangle & (9.35)\\ &= C_{m-1}^{-1}X_-X_+|m\rangle + C_{m-1}^{-1}[X_+, X_-]|m\rangle & (9.36)\\ &= mC_{m-1}^{-1}|m\rangle & (9.37) \end{aligned}$$

This holds for $n = 1$. Then if this holds for $n = 1, \cdots, t$, $1 < t < s$

$$\begin{aligned} X_+|m-t-1\rangle &= C^{-1}_{m-t-1}X_+X_-|m-t\rangle && (9.38)\\ &= C^{-1}_{m-t-1}X_-X_+|m-t\rangle + C^{-1}_{m-t-1}[X_+, X_-]|m-t\rangle && (9.39)\\ &= C^{-1}_{m-t-1}X_-\alpha|m-t\rangle + (m-t)C^{-1}_{m-t-1}|m-t\rangle && (9.40)\\ &= C^{-1}_{m-t-1}X_-\alpha|m-t+1\rangle + (m-t)C^{-1}_{m-t-1}|m-t\rangle && (9.41)\\ &= (\alpha C_{m-t} + (m-t))C^{-1}_{m-t-1}|m-t\rangle && (9.42) \end{aligned}$$

Thus by induction we have finished our proof. This is illustrated in Fig 9.1.

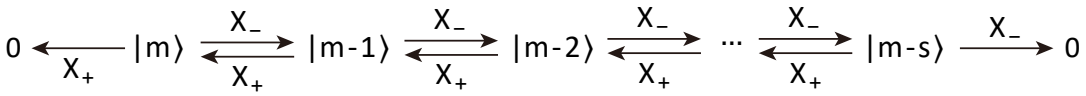


Figure 9.1: How X_+ and X_- acts in H_0.

Name the subspace spanned by $|m\rangle$ ...$|m-s\rangle$ as H_0. This means H_0 is an invariant subspace of the $\mathbf{su}(2)$ Lie algebra. We want to prove that Lie algebra restricted on H_0 is irreducible. We only need to prove there is no proper non-vanishing invariant subspace of H_0. Let there be one, say H_0'. We can find an eigenstate of X_3 with largest eigenvalue $|\psi\rangle = c_{m-n}|m-n\rangle$ and $X_+|\psi\rangle = 0$. This leads to $|\psi\rangle = c_m|m\rangle$. The we can use X_- to recover all basis of in H_0. Thus $H_0' = H_0$, which is a contradiction.

Since the Lie algebras are Hermitian operators, $H_0^\perp$ is also an invariant subspace. Then we can repeat this whole procedure in $H_0^\perp$. In this way we can reduce the original representation into irreducible representations.

Finally we calculate C_{m-n} and get the explicit matrix form of $\mathbf{su}(2)$ Lie algebra restricted in H_0. It's easy to see $C^2_{m-1} = m$, and when $2 \le n \le s$

$$\begin{aligned} C^2_{m-n} &= C^2_{m-n}\langle m-n|m-n\rangle && (9.43)\\ &= \langle m-n+1|X_+X_-|m-n+1\rangle && (9.44)\\ &= \langle m-n+1|X_-X_+|m-n+1\rangle + \langle m-n+1|[X_+, X_-]|m-n+1\rangle && (9.45)\\ &= \langle m-n+1|X_-|m-n+2\rangle\langle|m-n+2|X_+|m-n+1\rangle + m-n+1 && (9.46)\\ &= C^2_{m-n+1} + m-n+1 && (9.47) \end{aligned}$$

Thus $C^2_{m-n} = m + (m-1) + \cdots + (m-n+1) = \frac{1}{2}n(2m-n+1)$. From $C_{m-s} = 0$ we have $s = 2m+1$ which means m is an integer or half-integer. Then the basis of H_0 is $|m\rangle$ ...$|-m\rangle$, and

$$\begin{aligned} \langle n'|X_-|n\rangle &= C_{n'}\delta_{n',n-1} = \sqrt{\frac{(m-n+1)(m+n)}{2}}\delta_{n',n-1} && (9.48)\\ \langle n'|X_+|n\rangle &= C_n\delta_{n',n+1} = \sqrt{\frac{(m-n)(m+n+1)}{2}}\delta_{n',n+1} && (9.49)\\ \langle n'|X_1|n\rangle &= \frac{1}{2}\big(\sqrt{(m-n+1)(m+n)}\delta_{n',n-1} + \sqrt{(m-n)(m+n+1)}\delta_{n',n+1}\big) && (9.50) \end{aligned}$$

$$\langle n'|X_2|n\rangle = \frac{i}{2}\big(-\sqrt{(m-n+1)(m+n)}\delta_{n',n-1}+\sqrt{(m-n)(m+n+1)}\delta_{n',n+1}\big) \quad (9.51)$$

$$\langle n'|X_3|n\rangle = n\delta_{n',n} \quad (9.52)$$

This is also called by physicists the spin-m representation, expressed as (m). For small m, its matrix form is

1. $m=0$, $X_i=0$
2. $m=\frac{1}{2}$, $X_i=\frac{\sigma_i}{2}$
3. $m=1$,

$$X_1=\frac{1}{\sqrt{2}}\begin{pmatrix}0&1&0\\1&0&1\\0&1&0\end{pmatrix},\quad X_2=\frac{i}{\sqrt{2}}\begin{pmatrix}0&-1&0\\1&0&-1\\0&1&0\end{pmatrix},\quad X_3=\begin{pmatrix}1&0&0\\0&0&0\\0&0&-1\end{pmatrix} \quad (9.53)$$

4. $m=\frac{3}{2}$,

$$X_1=\begin{pmatrix}0&\frac{\sqrt{3}}{2}&0&0\\\frac{\sqrt{3}}{2}&0&1&0\\0&1&0&\frac{\sqrt{3}}{2}\\0&0&\frac{\sqrt{3}}{2}&0\end{pmatrix},X_2=\begin{pmatrix}0&-\frac{\sqrt{3}}{2}i&0&0\\\frac{\sqrt{3}}{2}i&0&-i&0\\0&i&0&-\frac{\sqrt{3}}{2}i\\0&0&\frac{\sqrt{3}}{2}i&0\end{pmatrix},X_3=\begin{pmatrix}\frac{3}{2}&0&0&0\\0&\frac{1}{2}&0&0\\0&0&\frac{1}{2}&0\\0&0&0&\frac{3}{2}\end{pmatrix} \quad (9.54)$$

Then the original space H can be reduced as in Fig 9.2. If we define D_m to be the dimension of eigenspace of X_3 with eigenvalue m. It's easy to see the recurrence of spin-m representation is just $D_m - D_{m+1}$.

9.2.1 Tensor products

If we have a spin-j and a spin-j' representation of $\mathbf{su}(2)$ with representation space H_1 and H_2. In each space, basis of $\mathbf{su}(2)$ can be viewed as operators $X_i^{(1)}$ and $X_i^{(2)}$. We define operators acting in $H_1\otimes H_2$ as

$$X_i = X_i^{(1)}\otimes I^{(2)} + I^{(1)}\otimes X_i^{(2)} \quad (9.55)$$

which is usually abbreviated as $X_i = X_i^{(1)} + X_i^{(2)}$.

Exercise 9.2.2

Test that X_i satisfy $\mathbf{su}(2)$ algebra, and thus can be viewed as basis of $\mathbf{su}(2)$ algebra.

Thus X_i is naturally a $\mathbf{su}(2)$ representation. It's generally a reducible representation, and can be reduced to irreducible representations by a similar transformation, whose matrix elements are called the Clebsh-Gordan coefficients. It's easier for us to derive the recurrence of each irreducible representations by dimension counting.

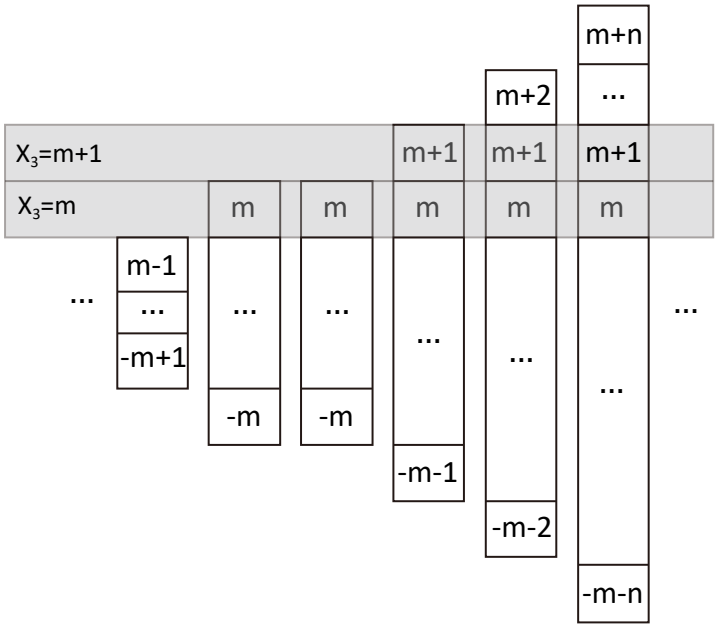


Figure 9.2: Reduction of H into irreducible representations.

Since

$$X_3|m_1, m_2\rangle = (m + m')|m, m'\rangle \tag{9.56}$$

D_m we just defined is the number of solutions of

$$m_1 + m_2 = m,\ |m_1| \leq j,\ |m_2| \leq j' \tag{9.57}$$

It's easy to see

$$D_m = \begin{cases} 0 & |m| > |j + j'| \\ j + j' - m + 1 & |j - j'| \leq |m| \leq |j + j'| \\ 2\min(j, j') + 1 & |m| < |j - j'| \end{cases} \tag{9.58}$$

Thus

$$D_m - D_{m+1} = \begin{cases} 0 & m > |j + j'| \\ 1 & |j - j'| \leq m \leq |j + j'| \\ 0 & 0 \leq m < |j - j'| \end{cases} \tag{9.59}$$

That's to say, the direct product of spin-j and a spin-j' representation can be reduced into direct sum of spin-$|j - j'|$ ...spin-$j + j'$ representation. It can also be expressed as

$$(j) \otimes (j') = (|j - j'|) \oplus \cdots \oplus (j + j') \tag{9.60}$$

This is called the Clebsh-Gordan series.

Exercise 9.2.3

Prove that for $\mathbf{su}(2)$ algebra

$$\left(\frac{1}{2}\right)^{\otimes 2N} = (0)^{g(0,N)} \oplus (1)^{g(1,N)} \oplus \cdots \oplus (N)^{g(N,N)} \tag{9.61}$$

$$\left(\frac{1}{2}\right)^{\otimes (2N+1)} = \left(\frac{1}{2}\right)^{g(\frac{1}{2},\frac{2N+1}{2})} \oplus \left(\frac{3}{2}\right)^{g(\frac{3}{2},\frac{2N+1}{2})} \oplus \cdots \oplus \left(\frac{2N+1}{2}\right)^{g(\frac{2N+1}{2},\frac{2N+1}{2})} \tag{9.62}$$

where

$$g(a,b) = \begin{cases} \begin{pmatrix} 2b \\ a+b \end{pmatrix} - \begin{pmatrix} 2b \\ a+b+1 \end{pmatrix} & (a<b) \\ 1 & (a=b) \end{cases} \tag{9.63}$$

Hint: Count the dimension of the subspace with definite total X^3.

Bibliography