Notes for Group Theory and Representation Theory

Ting Gong

Started Mar. 14, 2019. Last revision August 7, 2019

Contents

Chapter 1

Review for Basic Terms

1.1 Basic Concepts of Groups and Morphisms

Definition 1.1.1. A nonempty set G with operation $*$ is a *group* if $x, y \in G$, the following properties are satisfied:
(i) Closure: $x * y \in G$
(ii) Associativity: $(x * y) * z = x * (y * z)$
(iii) Identity: $\exists e \in G$ such that $e * x = x * e = x$
(iv) Inverse: $\exists x^{-1} \in G$ such that $xx^{-1} = x^{-1}x$
A group is called *Abelian* if we have an extra property:
(v) Commutativity: $xy = yx$

Definition 1.1.2. Let $b = axa^{-1}$, where $x, a \in G$, we call b the conjugate of x by a

Remark 1.1.3. One can prove the following statements easily:
(i) inverses are unique in a group
(ii) identity is unique in a group
(iii) right and left cancellations holds in groups

It is natural to consider we do the operation multiple times on the same element, say n. We call n the power of the element.

Definition 1.1.4. A group of G is *finite* if G contains finitely many elements, and the number of elements, denoted as $|G|$, is called the *order* of G.

If a group G is of small order, one can try to draw a *Cayley Table*, where one lists all the possibilities of operations in a matrix, in order to observe some properties of the group.

Definition 1.1.5. A group G is *cyclic* if every element of G can be written as a power of an element $g \in G$. We say that g *generates* G, and we can denote $G = \langle g \rangle$.

One can try to show that all cyclic groups are Abelian by considering the operation of the powers of an element.

Definition 1.1.6. A nonempty $H \subseteq G$ is a *subgroup* of G if H is a group with respect to the operation in G. In this case, we only need to check Closure, Identity and Inverse.

Definition 1.1.7. Let H be a subgroup of G. If $H \neq G$, then H is a *proper* subgroup; if $H = \{e\}$, then H is a *trivial* subgroup; if the only subgroup of G contained in H is the trivial group, then H is a *minimal* subgroup; if the only subgroup of G contains H is G, then H is a *maximal* subgroup.

Theorem 1.1.8. *A nonempty finite $H \subseteq G$ is a subgroup if $\forall x, y \in H$, then $xy \in H$.*

Proof. We construct a automorphic mapping $\phi : u \mapsto ux$. Since H is finite, we see that this is a bijection. Now we check $1 = \phi^{-1}(x) \in H$, and $x^{-1} = \phi^{-1}(1)$. □

Definition 1.1.9. Let $A, B \subseteq G$, with G a group. The product of AB is defined as following

$$AB = \{ab|a \in A, b \in B\}$$

Note that A^{-1} is defined in a similar way:

$$A^{-1} = \{a^{-1}|a \in A\}$$

and the conjugate of B of g is written as $B^g = gBg^{-1}$, with $g \in G$. And B^A is defined as

$$B^A = \{B^a|a \in A\}$$

Theorem 1.1.10. *Let A, B be finite subgroups of G. Then*

$$|AB| = \frac{|A||B|}{|A \cap B|}$$

Proof. We define an equivalence relation $(a_1, b_1) \sim (a_2, b_2)$ iff $a_1b_1 = a_2b_2$. Then, we know that $|AB|$ is the number of conjugate classes here. Consider $a_1b_1 = a_2b_2 \Leftrightarrow a_1^{-1}a_2 = b_1b_2^{-1}$. Thus, we know that each equivalence classes contains $|A \cap B|$ elements. Thus, we have what we desired. □

Definition 1.1.11. Let H be a subgroup of G, and $g \in G$, then $Hg = \{hg|h \in H\}$ is called a *right coset*, and similarly $gH = \{gh|h \in H\}$ is called a *left coset*. And the number of right cosets of H in G is called the *index* of H in G, denoted as $|G : H|$.

Theorem 1.1.12. *(Lagrange's Theorem) Let H be a subgroup of finite group G. Then* $|G| = |H||G : H|$

Proof. We are going to show that the right cosets cover the whole group, and two cosets are either distinct or identical.

Let $x \in G$, we know that $x = e_Gx \in Hx$. Therefore, we know each x is in a coset of H.

We define an equivalence relation $x \sim y \Leftrightarrow xy^{-1} \in H$. Assume $Hx = Hy$, then $xy^{-1} \in H$. Therefore $x \in Hy$. Thus, if two sets are identical, then they are in the same equivalence class. Otherwise they are not. Thus the cosets are either distinct or identical. □

Definition 1.1.13. Let H be a subgroup of G, $K \subseteq G$. If K contains exactly one element of every right coset of H, then K is a *transversal* of G

Remark 1.1.14. Let H and K be subgroup of G with $G = HK$ and $H \cap K = 1$, then K is a transversal of H in G. And K is called a *complement* of H in G.

Theorem 1.1.15. *(Dedikind Identity) Let M, N be subgroups of G, and $G = MN$. Then every subgroup H with $M \subseteq H \subseteq G$ has the factorization $H = M(N \cap H)$.*

Proof. By Lagrange's Theorem, we know that G and H are both covered by cosets of M. And every coset of M contains an element of N. Thus we have the factorization. □

We are going to clarify some notations not mentioned above. Before talking about any morphisms, we are going to set stage for Sylow Theorems. Let $\pi(x)$ be the set of prime numbers that is divisible by X, and if G is a group, $\pi(G) = \pi(|G|)$. And $o(x) = |\langle x \rangle|$.

Definition 1.1.16. An element $x \in G$ is a *p-element* if $o(x)$ is a power of p. G is a *p-group* if $\pi(G) = \{p\}$. A *p-subgroup* is a subgroup which is a p-group.

Definition 1.1.17. Let G and H be group. A mapping $\phi : G \to H$ is a *homomorphism* if $\phi(xy) = \phi(x)\phi(y)$, $\forall x, y \in G$.

A homomorphism ϕ an *epimorphism* if $Im\phi = H$, and *endomorphism* if $H = G$, a *monomorphism* if ϕ is injective, an *isomorphism* if ϕ is bijective and an automorphism if ϕ is a bijective endomorphism.

If ϕ is an isomorphism, then we write $G \cong H$, and say G is isomorphic to H.

If $X \in G$, $Y \in H$, then we say $\phi(X)$ the *image* of X, and $\phi^{-1}(Y)$ the *preimage* of Y. And the *kernel* of ϕ is the set $\ker\phi = \{x|\phi(x) = e_H\}$.

One can try to prove the following claims. Most of them are trivial.

Remark 1.1.18. Let $\phi : G \to H$, G, H are groups.
(i) $\phi(e_G) = e_H$
(ii) $\phi(x^{-1}) = \phi(x)^{-1}$
(iii) If M is a subgroup of G, then $\phi(M)$ is a subgroup of H
(iv) If N is a subgroup of H, then $\phi^{-1}(N)$ is a subgroup of G
(v) $\phi(\langle X \rangle) = \langle \phi(X) \rangle$

Definition 1.1.19. Let G be a group. H is a *normal subgroup* of G if $\forall g \in G, gH = Hg$.

Theorem 1.1.20. *Let $\phi : G \to H$. $\ker\phi$ is a normal subgroup of G.*

Proof. $\forall x \in \ker\phi, g \in G$, consider gxg^{-1}. $\phi(gxg^{-1}) = \phi(g)\phi(x)\phi(g)^{-1} = e$. Therefore, $gxg^{-1} \in \ker\phi$. Checking the kernel is a subgroup should be easy. □

Definition 1.1.21. Let G be a group. If the only normal subgroup of G are e and G, then we call G a *simple group.*

Definition 1.1.22. Let G be a group, H be a normal subgroup of G. Then G/H forms a group (one can check this very quickly), we call it the *quotient group*.

Theorem 1.1.23. *(First Isomorphism Theorem) Let $\phi : G \to H$ be a homomorphism. Then $G/\ker\phi \cong Im(\phi)$*

Proof. By 1.1.20, we know that the kernel of ϕ is a normal subgroup of G. Consider map $\varphi : G/\ker\phi \to Im(\phi)$. We check it to be well-defined. Let $x, y \in G, x = y$. Then we have $\varphi(x\ker\phi) = \phi(x) = \phi(y) = \varphi(y\ker\phi)$.

Then we check homomorphism: $\varphi(x\ker\phi\ y\ker\phi) = \varphi(xy\ker\phi) = \phi(xy) = \phi(x)\phi(y) = \varphi(x\ker\phi)\varphi(y\ker\phi)$.

Next, we check injective, let $\varphi(x\ker\phi) = \varphi(y\ker\phi)$, then $\phi(x) = \phi(y) \Rightarrow \phi(xy^{-1}) = 1 \Rightarrow xy^{-1} \in \ker\phi$. Thus, $x\ker\phi = y\ker\phi$.

Then we check surjective. Let $k \in Im(\phi)$, then $\exists x, k = \phi(x) = \varphi(x\ker\phi)$. Thus we have $G/\ker\phi \cong Im(\phi)$. □

Theorem 1.1.24. *(Second Isomorphism Theorem) Let H be a subgroup, and N be a normal subgroup of G. Then*

$$H/(H \cap N) \cong HN/N$$

Proof. Consider $\phi : H \to HN/N$ with $\phi(x) = xN$. We observe $\ker\phi = H \cap N$. By First Isomorphism Theorem, we get what we desired. □

Theorem 1.1.25. *(Third Isomorphism Theorem) Let H and N be a normal subgroup of G, $N \subseteq H$. Then*

$$G/H \cong (G/N)/(H/N)$$

Proof. Consider $\phi : (G/N) \to G/H$ with $\phi(xN) = xH$. It is clearly well-defined and a homomorphism. Notice that H/N is the kernel. And G/H is the image. By First Isomorphism Theorem, we get this result. □

Definition 1.1.26. If $N \trianglelefteq H \trianglelefteq G$, then N is called a *subnormal subgroup* of G. If $N = N_1 \trianglelefteq N_2 \trianglelefteq \ldots \trianglelefteq N_n = G$ then we call this a *subnormal series* from N to G. Denoted as $N \trianglelefteq\trianglelefteq G$.

Note that if $N \trianglelefteq\trianglelefteq G$, it doesn't necessarily imply $N \trianglelefteq G$. One can prove the following easily

Remark 1.1.27. If N, H are subnormal subgroups of G, then the following are true

(i) if $N \trianglelefteq\trianglelefteq H \trianglelefteq\trianglelefteq G$, then $N \trianglelefteq\trianglelefteq G$

(ii) If K is a subgroup of G, then $H \cap K \trianglelefteq\trianglelefteq H$

(iii)$H \cap N \trianglelefteq\trianglelefteq G$

(iv) If $\phi : G \to H$, then the image of any subnormal subgroup of G is a subnormal subgroup in H.

1.2 Two Interesting Examples

Definition 1.2.1. Let G be a group. The set of all automorphisms G, denoted as $Aut(G)$, is a group, called *automorphism group.*

One can easily check our claim in the definition. We will not expand the calculation.

Definition 1.2.2. Let $\phi_a : G \to G$, with $\phi_a : x \mapsto axa^{-1}$, it is an automorphism of G, which we call the *inner automorphism* induced by a.

Proposition 1.2.3. *The set of inner automorphism of G, $Inn(G)$ is a normal subgroup of $Aut(G)$.*

Proof. We first show it is a subgroup. Let $\varphi : G \to Aut(G)$ with $a \mapsto \phi_a$. Since $x^{ab} = abxa^{-1}b^{-1} = (x^a)^b$, we know that $Inn(G)$ is a subgroup of $Aut(G)$.

Then we check it is normal. Let $\beta \in Aut(G)$, we have $\beta\phi_a\beta^{-1} = \phi_{\beta(a)}$. Therefore, $Inn(G)$ is normal. □

Definition 1.2.4. The *center* of G is defined as $Z(G) := \{x \in G | axa^{-1} = x, \forall a \in G\}$.

Notice $Z(G)$ is exactly $\ker\varphi$. Therefore, by the first homomorphism theorem, we have $Inn(G) \cong G/Z(G)$.

Theorem 1.2.5. *If $G/Z(G)$ is cyclic, then G is Abelian.*

Proof. Assume $G/Z(G)$ is cyclic, then $\exists g \in G$, such that $G/Z(G) = \langle gZ(G)\rangle$. Therefore, $G = Z(G)\langle g\rangle$. Therefore, we see that G is Abelian because each pair of elements commute. □

Definition 1.2.6. A subgroup H of G is called a *characteristic subgroup* of G if $\forall\alpha \in Aut(G)$, $\alpha(H) = H$. We denote this as H *char* G

Proposition 1.2.7. *Let G be a group, N be a normal subgroup of G and H be a characteristic subgroup of N, then the followings are true:*

(i)H is normal in G.

(ii) If N is characteristic in G, then H is characteristic in G.

Proof. (i) Let $g \in G$. Then consider ϕ_g, the inner automorphism. Since N is normal in G, $\phi_g(N) \subseteq N$. Since H is characteristic of N, we have $\phi_g(H) = H$. Therefore, H is normal.

(ii) Consider $\phi \in Aut(G)$. Then since N is characteristic in G, we have $\phi(N) = N$. Thus, Therefore, $\phi \in Aut(N)$. Since H is characteristic in N, $\phi(H) = H$. Thus, H is characteristic in G. □

Now we are going to set up stage for representation theory. The following definitions will show up later in a more rigorous way.

Definition 1.2.8. Let G, H be groups, and $\phi : G \to Aut(H)$ be a homomorphism. Then *G acts on H.*

Definition 1.2.9. Let K be a subgroup of H, K is G-*invariant* if for all $g \in G$, we have $\phi_g(K) = \{\phi_g(k) | k \in K\} = K$.

Definition 1.2.10. Let $\rho : H \to K$, and G be a group acts on H and K. If $\forall h \in H, g \in G$ $\rho(\phi_g(h)) = \phi_g(\rho(h))$, then ρ is an G-*homomorphism.* Similarly, one can define G-isomorphism, G-automorphism etc. If H and K are G-isomorphic, we denote this as $H \cong_G K$

One can yield similar results on this notion as the ones we did on homomorphisms, such as the three isomorphism theorems, and some mapping relations. We will check some of these when we get to representations. Now, we are going to examine the case of cyclic groups.

Lemma 1.2.11. *A cyclic group of order n is isomorphic to $\mathbb{Z}/n\mathbb{Z}$*

Proof. Let $G = \langle g \rangle$ be a cyclic group of order n. Consider $\phi : \mathbb{Z} \to G$. Notice that $\ker \phi = n\mathbb{Z}$. Therefore, by the first isomorphism theorem, $G \cong \mathbb{Z}/n\mathbb{Z}$. □

Theorem 1.2.12. *Let $G = \langle g \rangle$ be a cyclic group of order n and $d_1, \ldots, d_k$ are divisors of n, and $U_i = \langle g^{d_i} \rangle$. Then $U_1, \ldots, U_k$ are the only subgroups of G. And the following are true:*
(i)if $n = n_i d_i$, then U_i is a subgroup of order n_i
(ii)Let $a \in \mathbb{Z}$. If $d_i = (a, n)$, then $\langle g^a \rangle = U_i$

Proof. By our lemma, we see that $G \cong \mathbb{Z}/n\mathbb{Z}$. We know that $n\mathbb{Z}$ is a subgroup of $m\mathbb{Z}$ iff m—n. (One can verify this by devision algorithm.) Therefore, we see the only subgroups are isomorphic to $\mathbb{Z}/d_i\mathbb{Z}$, which are the U_i's.

(a) We need to show that n_i is the smallest m such that $(g^{d_i})^m = 1$. Let m be the smallest number with such condition, then if we call $g^{d_i} = b$, if $b^c = b_d, 0 < c < d < m$, then $b^{c-d} = 1$, which contradict the minimality of m. Thus every power less than m is distinct. Since we know $z \in \mathbb{Z}$ can be factored into $z = qm + r$, thus $b^z = b^r$. Thus, it is clear that $m = n_i$.

(b) By Bezout, we have $a = na_1 + aa_2$. Thus $g^{d_i} = g^{na_1 + aa_2} = g^{aa_2} \in \langle g^a \rangle$. Also, $d_i | a$, we have $U_i = \langle g^a \rangle$ □

Corollary 1.2.13. *Let $G = \langle g \rangle$ be a cyclic group of order p^n, where p is a prime. Then $\{1\} \subset \langle g^{p^{n-1}} \rangle \subset \langle g^{p^{n-2}} \rangle \subset \ldots \subset \langle g^p \rangle \subset G$ are the only subgroups of G. Thus, G has only one maximal and minimal subgroup.*

Corollary 1.2.14. *The cyclic groups of prime order are the only Abelian simple groups.*

1.3 Commutators

We will have a more detailed survey on Commutators in the later chapters. But we will cover some basics.

Definition 1.3.1. Let $x, y \in G$, G is a group, define $[x, y] = x^{-1}y^{-1}xy$. Then we have $xy = yx[x, y]$. We call $[x, y]$ the *commutator* of x and y. Also, we have $[x, y]^{-1} = [y, x]$.

Definition 1.3.2. We call the subgroup generated by all commutators, G', the *commutator subgroup.*

Remark 1.3.3. Observe several facts from this definition. If ϕ is a homomorphism in G, $x, y \in G$. Then $\phi([x, y]) = [\phi(x), \phi(y)]$, and G' is characteristic in G.

Theorem 1.3.4. *Let N be a normal subgroup of G. Then G/N is Abelian iff G' is a subgroup of N*

Proof. Let $x, y \in G$, $xNyN = yNxN$ iff $xyN = yxN$. Therefore, we see that $[x, y] \in N$. □

Definition 1.3.5. G, a group, is *perfect* if $G = G'$.

Proposition 1.3.6. *Let N be an Abelian normal subgroup of G. If G/N is perfect, then G' is perfect.*

Proof. Since G/N is perfect, we have $G/N = (G/N)' = G'N/N$. Thus $G = G'N$. Also, $G'/N \cap G' \cong G/N$, thus it is perfect, we have $G' = G''(N \cap G')$. Thus, $G = G''N$, and $G/G'' \cong N/N \cap G''$. By 1.3.4, since N is abelian, we have $G' = G''$ □

Now we define $[x, y, z] = [[x, y], z]$, $[X, Y]$ be the group generated by all $[x, y]$. One can observe that if $X, Y \subseteq G$, $[X, Y] = 1$ iff $xy = yx, \forall x \in X, y \in Y$, and if X, Y are subgroups of G, then $[X, Y]$ is a subgroup of Y iff Y is X-invariant.

Proposition 1.3.7. *For $x, y, z \in G$, we have the following:*
(i)$[x, yz] = [x, z][x, y]^z$
(ii)$[xz, y] = [x, y]^z[z, y]$

The proof is trivial. One only needs to expand both sides.

Corollary 1.3.8. *Let H, K be subgroups of G. Then $[H, K]$ is normal in $\langle H, K\rangle$.*

Proof. Let $h, g \in H, k \in K$, then $[h, k]^g = [hg, k][g, k]^{-1} \in [H, K]$. If $h \in H, k, g \in K$, then $[h, k]^g = [h, g]^{-1}[h, kg] \in [H, K]$ □

1.4 Products of Groups

Definition 1.4.1. Let $G_1, \ldots, G_n$ be groups, the Cartesian product of G_i, $G_1 \times \cdots \times G_n = \{(g_1, \ldots, g_n)|g_i \in G_i\}$ forms a group with respect to dot product. This group is called the (external) *direct product* of group $G_1, \ldots, G_n$.

Remark 1.4.2. Let $G_j^* = \{(g_1, \ldots, g_n)|g_i = 1 for i \neq j\}$, $G = G_1 \times \cdots \times G_n$, then we have the following:
(i) $G = G_1^* \ldots G_n^*$
(ii)$G_i^* \trianglelefteq G$
(iii)$G_i^* \cap G_j^* = 1, i \neq j$.

Definition 1.4.3. Let G be a group with subgroups $G_1^*, \ldots, G_n^*$. If the above three properties holds, then we call G the *(internal) direct product* of the groups $G_1^*, \ldots, G_n^*$. Note that one can prove this group to be isomorphism to the external direct product of G. Therefore, we will not distinguish them. This means that our three properties are equivalent to direct product of G.

Remark 1.4.4. Let $G = G_1 \times \ldots \times G_n$. One can prove the following to be true:
(i) $Z(G) = Z(G_1) \times \ldots \times Z(G_n)$
(ii) $G' = G_1' \times \ldots \times G_n'$
(iii) Let N be a normal subgroup of G; $N_i = N \cap G_i$. Then we have

$$G/N \cong G_1/N_1 \times \ldots \times G_n/N_n$$

(iv) If $G_1, \ldots, G_n$ are characteristic subgroups of G, then

$$Aut(G) \cong Aut(G_1) \times \ldots \times Aut(G_n)$$

Theorem 1.4.5. *Let $G = G_1 \times \ldots \times G_n$ and N be a normal subgroup of G.*
(i) If N is perfect, then $N = (N \cap G_1) \times \ldots \times (N \cap G_n)$
(ii) If $G_1, \ldots, G_n$ are non-Abelian simple groups, then there exists a subset $J \subset \{1, \ldots, n\}$ with $N = \prod_{j \in J} G_j$ and $G_k \cap N = 1, k \notin J$

Proof. (i)Since G_i and N are normal in G, we have $[G_i, N]$ is a subgroup of $G_i \cap N$. Thus we have $[N, G] = \prod_i [N, G_i]$ is a subgroup of $\prod_i (N \cap G_i)$. Thus $[N, N]$ is a subgroup of $\prod_i (N \cap G_i)$. Also, since N is perfect, $N = N'$, we have $N = \prod_i (N \cap G_i)$.

(ii)We want to prove that N is perfect and apply (i). Assume $N \neq G$, $\exists k$, $N \cap G_k = 1$. Thus $NG_k = N \times G_k$. Consider G/G_k, it is equal to $\prod_{i \neq k} G/G_i$. And $N/N_k = (N/N_k)'$. Thus, $N \times G_k = N' \times G_k$, thus $N = N'$. □

Theorem 1.4.6. *(Chinese Remainder Theorem) Let $N_1, \ldots, N_n$ be normal subgroups of G, then $G/\cap_i N_i \cong G/N_1 \times \ldots \times G/N_n$.*

Proof. Consider $\phi : G \to G/N_1 \times \ldots \times G/N_n$. Notice $\ker \phi = \cap_i N_i$. Thus by the first isomorphism theorem, we have our claim. □

Proposition 1.4.7. *Let $G = \prod_i G_i$, with $G_1, \ldots, G_n$ are normal subgroups of G. If $\gcd(|G_i|, |G_j|) = 1, i \neq j$, then $G = G_1 \times \ldots \times G_n$.*

Proof. Let $H = \prod_{i \neq j} G_i \cap G_j$, then we know $|H| \big| |G_j|$ and $|H| \big| |\prod_{i \neq j} G_i|$. Thus $|H| = 1$. Thus H is a trivial group. Thus $G = G_1 \times \ldots \times G_n$ □

Corollary 1.4.8. *Let $a, b \in G$, $ab = ba$, $\gcd(o(a), o(b)) = 1$, then $\langle ab \rangle = \langle a \rangle \times \langle b \rangle$, $o(ab) = o(a)o(b)$.*

Definition 1.4.9. Let G be a group, K, H are subgroups of G. G is the *(internal) semidirect product* of K with H, if the following are satisfied:

(i)$G = KH$

(ii)$H \trianglelefteq G$

(iii)$K \cap H = 1$

One can easily prove the following:

Remark 1.4.10. Let H, K be subgroups of G and satisfy the above properties:

(i)$g \in G$ can be uniquely factored into $g = kh, k \in K, h \in H$

(ii)Let $k_1, k_2 \in K, h_1, h_2 \in H$, then $(k_1h_1)(k_2h_2) = (k_1x_2)(k_1^{x_2}h_2)$

Similar as the direct products, the converse of this statement is also valid.

Definition 1.4.11. Let $\phi : K \to Aut(H)$ be a homomorphism. Then K acts on H. Let $G = \{(k, h)|k \in K, h \in H\}$. Then G forms a group with multiplication $(k_1h_1)(k_2h_2) \mapsto (k_1k_2)(\phi_k(h_1)h_2)$. Then G is called the *(external) semidirect product* of K with H, denoted as $G = K \ltimes H$.

Definition 1.4.12. Elements of order 2 is called *involution*, a gourp generated by 2 involutions is a *dihedral group*.

Theorem 1.4.13. *Let G be a finite group of order $2n$. The following are equivalent:*

(i) G is a dihedral group

(ii)G is the semidirect product $K \ltimes H$ of two cyclic subgroups $K = \langle k \rangle$ and $H = \langle h \rangle$ such that $o(k) = 2, o(h) = n$, and $khk^{-1} = h^{-1}$

Proof. ($\Leftarrow$) Consider $x = kh$. We have $x^2 = khkh = khk^{-1}h = h^{-1}h = 1$. We see that x is an involution. Also we see that this mapping between x and h is bijective. Thus, $G = \langle x, k \rangle$ is a dihedral group.

($\Rightarrow$) Let k, x be involutions of G such that $G = \langle k, x \rangle$. Let $K = \langle k \rangle$, $H = \langle h \rangle$, $h = xk$. Consider $khk = kkxk = xk = h^{-1} = xkxx = xhx$. Therefore, $H \trianglelefteq G$. Also, it is clear $G = KH$. If $H \cap K \neq 1$, then $x, k \in H$, thus $x = k$. Thus, $h = 1$. Thus H is trivial. We have a contradiction. Thus we fulfilled the three of the properties. □

1.5 Minimal Normal Subgroups and Composition Series

We are going to briefly introduce these two concepts in the section title.

Definition 1.5.1. Let G be a group, $N \neq 1$ of G is a *minimal normal subgroup* if N is a simple normal subgroup of G.

There are several things we need to observe. Firstly, there might be many minimal normal subgroups of G. Next, every finite group is either a minimal normal subgroup or contains a minimal normal subgroup.

Lemma 1.5.2. *Let N be a minimal normal subgroup of G*

(i) For all subgroups H of G, N either is a subgroup of H or $N \cap H = 1$. Moreover, if $N \cap H = 1$, then $[N, H] = 1$

(ii) If N is abelian, $G = NH$, then N is a subgroup of H or $N \cap H = 1$

(iii)If $\phi : G \to K$ is an epimorphism, K is a group. Then $\phi(N) = 1$ or $\phi(N)$ is a minimal normal subgroup of H.

Proof. (i) Since N is minimal, we see that either N is a subgroup of H, or N is not a subgroup of H. If N is not a subgroup of H, let $n \in N \cap H$, then $gng^{-1} \in N \cap H$, thus $N \cap H \trianglelefteq G$. Since N is minimal, this has to be trivial. Therefore $[N, H] = 1$

(ii) Since N is abelian, we know that $H \cap N$ is normal in N. Moreover, it is also normal in H. Since the conjugate is closed in H and by normal it is in N. Since $G = HN$, $H \cap N$ is normal in G. Thus either $H \cap N = N$, where we get N is a subgroup of H, or $H \cap N = 1$

(iii) Let $K \neq 1$ be a normal subgroup of H and $K \subset \phi(N)$. We know that by (i), $\phi^{-1}(K) \cap N$ is a normal subgroup of G, and $\phi^{-1}(K) \cap N \neq 1$. Thus $\phi^{-1}(K) \cap N = N$. Therefore, $K = N$. Thus, there are no normal subgroups of H contained in N besides N itself. Thus, $\phi(N)$ is a minimal normal subgroup of H. Otherwise, if $K = 1$ then clearly $\phi(N)$ is 1. □

Lemma 1.5.3. *Let $\mathfrak{M}$ be a finite set of minimal normal subgroups of G, and $M = \prod_{N \in \mathfrak{M}} N$.*

(i)If H is a normal subgroup of G, then $\exists N_1, \ldots, N_n \in \mathfrak{M}$ with $HM = H \times N_1 \times \ldots \times N_n$

(ii)There exists $N_1, \ldots, N_n \in \mathfrak{M}$ such that $M = N_1 \times \ldots \times N_n$

Proof. (i) By our last lemma (i), $H \cap N = 1$ for $N \in \mathfrak{M}, N \not\subset H$. Therefore, $HN = H \times N$. Thus, continue doing this we get $H \prod_{i=1}^{n} N = H \times N_1 \times \ldots \times N_n$. Now we are going to show that there is a maximum n such that $H \prod_{i=1}^{n} N$ is HM. If n is a maximum, but $H \prod_{i=1}^{n} N$ is not HM, then $\exists N \in \mathfrak{M}$ with $N \not\subset H \prod_{i=1}^{n} N$, then we have $H \prod_{i=1}^{n} N \times N = H \times N_1 \times \ldots \times N_n \times N$. Therefore contradict the maximal n.

(ii) Take $H = 1$. We have this argument □

Theorem 1.5.4. *Let N be a minimal normal subgroup of G, H be a minimal subgroup of N. Let $S = \{gHg^{-1} | g \in G\}$ be finite. Then H is simple, and $\exists H_1, \ldots, H_n \in S$ with $N = H_1 \times \ldots \times H_n$*

Proof. The group $\prod_{g \in G} gEg^{-1}$ is a normal subgroup of G, thus this is N. By our lemma, $N = E_1 \times \ldots \times E_n$. Since E_n are minimal in N, N is minimal in G, a normal subgroup of E_n will be normal in N. Therefore, E_n is simple. Thus, E is simple. □

Corollary 1.5.5. *Let N be an Abelian minimal subgroup of G, then $\exists p$ prime, such that N is a direct product of subgroups isomorphic to cyclic groups with order p.*

Now, let G be a finite group.

Definition 1.5.6. (A_i) is a *subgroup series* if $1 = A_0 \subset A_1 \subset \ldots \subset A_a = G$, with each a subgroup of the other. The *length* of this subgroup series is a. A series is a *normal series* if $A_i \trianglelefteq G$ and a *subnormal series* if $A_{i-1} \trianglelefteq A_i$, $\forall i$.

Definition 1.5.7. A normal series is a *chief series* if each A_{i-1} is maximal among the normal subgroups of G. A subnormal series is a *composition series* if each A_{i-1} is maximal among the proper normal subgroups of A_i.

Remark 1.5.8. Notice that the *composition factors* A_i/A_{i-1} of a composition series are simple groups.

Definition 1.5.9. Let G be a group acting on H, let A, B be G-invariant subgroups of H and that $B \trianglelefteq A$. Then G also acts on A/B, which we call a *G-section* of H.

Definition 1.5.10. A subnormal series (A_i) is a *G-composition seires* of H if all the subgroups of A_i are G-invariant, and there are no G-invariant normal subgroups of A_i strictly between A_{i-1} and A_i. We call the factors A_i/A_{i-1} G-simple.

Theorem 1.5.11. *(Jordan-Holder Theorem) Let G be a group acts on H, and let (A_i), (B_i) be two G-composition seires of H. Then $a = b$ and there exists a permitation π such that*

$$\pi(A_i/A_{i-1}) \cong_G B_i/B_{i-1}$$

Proof. Let N be the maximal G-invariant normal subgroup of H, say B_{b-1}. Then H/N is G-simple. Notice if A_i is not a subgroup of N, then $A_iN = \ldots = A_{a-1}N = H$ because N is maximal. Pick j to be the maximal number such that A_j is a subgroup of N, we have $A_j \trianglelefteq A_{j+1} \cap N \subset A_{j+1}$, thus $A_j = A_{j+1} \cap N$. Thus $A_j \cap N = A_j = A_{j+1} \cap N$. Now since $H/N = A_{j+1}N/N \cong_G A_{j+1}/A_{j+1} \cap N$. Thus, we have $A_{j+1}/A_j \cong_G H/N$.

Thus, for $k \geq j+2$, we have $A_k \cap N \cap A_{k-1} = N \cap A_{k-1}$, thus, $(A_k \cap N)/(A_{k-1} \cap N) \cong_G (A_k \cap N)A_{k-1}/A_{k-1} \trianglelefteq A_k/A_{k-1}$. Since A_k/A_{k-1} is G-simple, we have one of the following $(A_k \cap N)/(A_{k-1} \cap N) \cong_G A_k/A_{k-1}$ or $(A_k \cap N)/(A_{k-1} \cap N) = 1$. If $(A_k \cap N)/(A_{k-1} \cap N) = 1$, then $A_k \cap N = A_{k-1} \cap N$, however we have $A_k/(A_k \cap N) \cong_G H/N \cong_G A_{k-1}/(A_{k-1} \cap N)$. Thus, we have a contradiction.

Therefore, $(A_k \cap N)/(A_{k-1} \cap N) \cong_G A_k/A_{k-1}$, meaning that $1 = A_0 \cap N \subset \ldots \subset A_j \cap N \subset A_{j+2} \cap N \subset \ldots \subset A_a \cap N = N$. Also, $1 = B_0 \subset \ldots \subset B_{b-1} \subset N$. Therefore, we see that one is the permutation of the other. ◻

1.6 Study of Abelian Groups

In this section, we strive to prove the Fundamental Theorem of Abelian Groups, and give an example of automorphisms.

Lemma 1.6.1. *Let G be an Abelian group and H a cyclic subgroup of maximal order in G. Then $o(g) || H|, \forall g \in G$.*

Proof. Let $|H| = p^a m$, where $gcd(p, m) = 1$. Assume $k \in \langle g \rangle$ with $o(k) = p^b$, and $h \in H$ with $o(h) = m$. We have $o(kh) = p^b m$. Since H is maximal, $p^b m | p^a m$. Therefore, we know forall $p^l | o(g)$, $p^l || H|$. ◻

Proposition 1.6.2. *Let G and H be the same things in 1.6.1. Then there is a complement K of H in G, i.e. $G = H \times K$, $|G| = |H||K|$.*

Proof. Assume $H \neq G$ (or pick $K = 1$). We choose $y \in G - H$ such that $o(y)$ is minimal. We know that $y \neq 1$, and $\langle y^p \rangle \subseteq \langle y \rangle$, for all $p|o(y)$. Let $H = \langle h \rangle$. Then $o(y)||H|$, we know that there is a subgroup for every $p||H|$. Thus $\exists$ subgroup with order $o(y)/p$ in $\langle h^p \rangle$, which is $\langle y^p \rangle$. Let $h^{pi} = y^p$, we have $(yh^{-i})^p = 1$. But $yh^{-i} \notin H$. By minimality, $o(y) = p$. Thus $H \cap \langle y \rangle = 1$. Let $\overline{G} = G/\langle y \rangle$, $\langle \overline{x} \rangle \subset \overline{G}$, we have $o(\overline{x}) = o(x)$. Since $H\langle y \rangle \cong H/H \cap \langle y \rangle \cong H$, we have $|\overline{H}| = |H|$, we know $\overline{H}$ is a maximal cyclic subgroup in $\overline{G}$. Thus we can use induction to show that there is a complement $\overline{K}$ of $\overline{H}$ in $\overline{G}$. Thus, we see that K is a complement of H in G. □

By induction, we have the following theorem.

Theorem 1.6.3. *Every Abelian group is the direct product of cyclic groups.*

Corollary 1.6.4. *Let G be an Abelian group, m a divisor of $|G|$, then G contains a subgroup of order m.*

Lemma 1.6.5. *Let G be an Abelian group, p be a prime. Let $G_p = \{x \in G| \ x$ is a p-element$\}$. Then G_p is a characteristic p-subgroup of order $|G|_p$*

Proof. Let $x, y \in G$, then xy is a p-element. Thus G_p is a subgroup. Since automorphisms map p-elements to p-elements, G_p is characteristic. Since G contains a subgroup H of order $|G|_p$, then H is a p-group. Thus, every element of H is a p-element, thus $H \subseteq G_p$.

If $H \neq G_p$, then $k = [G_p : H] \neq 1$, and $gcd(p, k) = 1$. But now we have K a subgroup of G_p with order k. Thus, contradiction. □

Theorem 1.6.6. *Let G be an Abelian group. Then $G = G_p \times \ldots \times G_p$.*

Proof. Let G_1 be direct product of subgroups G_p, $p \in \pi(G)$. Then

$$|G_1| = \prod_{p \in \pi(G)} |G_p| = |G|$$

Thus, $G_1 = G$. □

Definition 1.6.7. An Abelian p-group is *elementary Abelian* is $x^p = 1, \forall x \in G$.

The following statements are clear.

Remark 1.6.8. Let G be a Abelian group. Then the following are equivalent:

(i) G is cyclic

(ii) $\forall p \in \pi(G), \exists$ exactly one subgroup of order p in G

(iii) G_p is cyclic $\forall p \in \pi(G)$

Corollary 1.6.9. *Let G be an elementary Abelian p-group of order $p^n > 1$, G is the direct product of n cyclic groups of order p.*

Consider a p-group of G, let $\Omega_i(G) = \langle x \in G | x^{p^i} = 1 \rangle$. $\Omega_i(G) \subseteq \Omega_{i+1}(G)$, and they are characteristic subgroup of G. Let $\Omega(G) = \Omega_1(G)$.

Proposition 1.6.10. *Let G be an Abelian p-group such that $G = C_1 \times \ldots \times C_n$, where $C_1, \ldots, C_n$ are cyclic. Then $|\Omega(G)| = p^n$.*

Corollary 1.6.11. *(Fundamental Theorem of Abelian Groups) Every finite generated Abelian group G is isomorphic to direct products of cyclic groups of prime power order.*

1.7 Group Action

Definition 1.7.1. Let G be a group and Ω be a non-empty set, $g \in G$, $\alpha \in \Omega$, $\alpha \cdot g$ is an *action* of G on Ω having the following properties,
(i)$\alpha \cdot 1 = \alpha$ for $\alpha \in \Omega$
(ii) $(\alpha \cdot g) \cdot h = \alpha \cdot (gh)$

Definition 1.7.2. Let G acts on Ω, if $g \in G$ arbitrary, then $\sigma_g : \Omega \to \Omega$ defined by $\sigma_g(\alpha) = \alpha \cdot g$ is a permutation of the set Ω, we call it a *permutation representation of* G, and we have a homomorphism from G into $Sym(\Omega)$

Definition 1.7.3. We let G act on G, $x \cdot g = xg$ for $x, g \in G$. We call it the *regular* action.

Definition 1.7.4. We call an action *faithful* if the kernel of this action is trivial.

Definition 1.7.5. Let G act on G, if $x \cdot g = g^{-1}xg$, then we call it the *conjugation action* of G on itself, clearly the kernel is $Z(G)$.

Definition 1.7.6. If G acts on some set Ω, and $\alpha \in \Omega$, we write $G_\alpha = \{g \in G | \alpha \cdot g = \alpha\}$ and we call it the *stabilizer of* α.

Remark 1.7.7. It is easy to see that if G has the regular action on itself, then the stabilizer of every point is trivial. If G has the conjugation action on itself, then the stabilizer of every point is the centralizer $C_G(x)$, and if G has the conjugation action on its subsets, then the stabilizer of a subset X is the normalizer $N_G(X)$.

Definition 1.7.8. If H is a subgroup of G, then we call the subgroup $\cap_{x \in G} H^x$ the *core* of H in G, and clearly it is normal in G.

Theorem 1.7.9. *Let H be a subgroup of G, and Ω is the set of right cosets of H in G. Then $G/core_G(H)$ is isomorphic to a subsgroup of $Sym(\Omega)$. If $|G : H| = n$, then it is isomorphic to a subgroup of S_n*

Proof. Let $\theta : G \to \Omega$ be a homomorphism defined by the action of G on Ω by right multiplication. We know $ker(\theta) = core_G(H)$, then by first isomorphic theorem, $G/core_G(H) \cong \theta(G)$ which is a subgroup of $Sym(G)$. If $|G : H| = n$, then $|\Omega| = n$, thus $Sym(\Omega) \cong S_n$ □

Corollary 1.7.10. *Let G be a group, H is a subgroup of G, $|G : H| = n$. Then G contains a normal subgroup N of G with $|G : N|$ divides $n!$*

Corollary 1.7.11. *Let G be a simple group and contains a subgroup of index $n > 1$, then $|G|$ divides $n!$*

Definition 1.7.12. Let G acts on Ω, $\alpha \in \Omega$. The set $O_\alpha = \{\alpha \cdot g | g \in G\}$ is called the orbit of α under the given action.

Theorem 1.7.13. *(The Fundamental Counting Principle) Let G act on Ω, and O one of its orbits. Let $\alpha \in O, H = G_\alpha$, the stabilizer of α. Let $\Lambda = \{Hx | x \in G\}$ be the set of right cosets of H in G. Then there is a bijection $\theta : \Lambda \to O$ such that $\theta : Hg \mapsto \alpha \cdot g$, and $|O| = |G : G_\alpha|$.*

Proof. Let $y = hx$ for $h \in H$, then $\alpha \cdot y = \alpha \cdot (hx) = (\alpha \cdot h) \cdot x = \alpha \cdot x$. Therefore, $Hx = Hy$, then $\alpha \cdot x = \alpha \cdot y$.

Let $Hx \in \Lambda$, $\alpha \cdot x$ is in O, thus $\theta : \Lambda \to O$ is well-defined. Now we prove bijective: let $\beta \in O$, then $\beta = \alpha \cdot x$ for some $x \in G$. Thus, $Hx \in \Lambda$ has $\theta(Hx) = \alpha \cdot x = \beta$.

If $\theta(Hx) = \theta(Hy)$, we have $\alpha \cdot x = \alpha \cdot y$. Thus $\alpha = \alpha \cdot 1 = (\alpha \cdot x) \cdot x^{-1} = (\alpha \cdot y) \cdot x^{-1} = \alpha \cdot (yx^{-1})$. Therefore, yx^{-1} is in the stabilizer of H. Therefore, $y \in Hx$ and thus $Hy = Hx$. Thus injective. □

Corollary 1.7.14. *Let $x \in G$, G be finite, and let K be the conjugacy class of G containing x. Then $|K| = |G : C_G(x)|$*

Corollary 1.7.15. *Let H be a subgroup of G, G be finite. Then the number of distinct conjugates of H in G is $|G : N_G(H)|$*

Chapter 2

Sylow Theory

2.1 The Sylow Theorems

Definition 2.1.1. A subgroup S of G is called a *Sylow p-subgroup* if $|S|$ is a poiwer of p and the index $|G : S|$ is not divisible by p.

Lemma 2.1.2. *Let p be prime, $a \geq 0$, $m \geq 1$, $a, m \in \mathbb{Z}$, then* $\binom{p^a m}{p^a} \equiv m \mod p$

Proof. We expand the polynomial $(1+x)^p$, since p is prime, $\binom{p}{i}$, $1 \leq i \leq p-1$ are divisible by p, we see that $(1+x)^p \equiv 1 + x^p \mod p$. Continue in this fashion, we see that $(1+x)^{p^a m} \equiv (1+x^{p^a})^m \mod p$. Then we consider the coefficient of X^{p^a} to see the solution. □

Theorem 2.1.3. *(Sylow existence theorem) Let G be finite, p a prime, then G has a Sylow p-subgroup.*

Proof. Let $|G| = p^a m$, $a \geq 0, p$ doesn't divide m. Let Ω be the set of all subsets of G with cardinality p^a, and let G act on Ω, then Ω is partitioned into orbits, $|\Omega| = \sum |O|$. However, $|\Omega| = \binom{p^a m}{p^a} \equiv m \mod p$, we know there is at least one O such that $|O|$ doesn't divide p.

Let $X \in O$, let $H = G_X$ be the stablizer of X. Then we know that $|O| = |G|/|H|$. Since $p \nmid |O|$, $p^a \mid |G|$, we know that $p^a \mid |H|$. Thus, $p^a \leq |H|$

Also, since H is the stablizer of X, $xH \subseteq X$. Since $|X| = p^a$, we have $|H| \leq p^a$. Thus $|H| = p^a$. And since H is a subgroup of G, H is the Sylow subgroup of G. □

Corollary 2.1.4. *If $p \mid |G|$, p is a prime, G is finite, then $\exists g \in G$ such that $o(g) = p$.*

Theorem 2.1.5. *Let P be a p-subgroup of a finite group G, $S \in Syl_p(G)$, then $P \subseteq S^g$ for some $g \in G$*

Proof. Let $\Omega = \{Sg | g \in G\}$. We act G on Ω and we know that P acts on Ω in the same way. Since $p \nmid |\Omega|$, we know that there must exist O an orbit of P-action whose order doesn't divide p. However, $|O|$ is a power of p by the fundamental counting theorem since $|O| = |P|/|Q|$, where Q is a subgroup of P. Thus, $|O| = 1$.

Assume $O = Sg$. Then we know O fixes P. Thus $Sgu = Sg$ with $u \in P$. Therefore, $gug^{-1} \in S$. s ◻

Theorem 2.1.6. *(Sylow Conjugation Theorem) If S, T are Sylow p-subgroups of G, then $T = S^g$ for some $g \in G$.*

The proof of the theorem follows from the last theorem.

2.2 Classification of Groups

Chapter 3

Normal and Subnormal Structure

Chapter 4

Commutators

Chapter 5

Transfer

Bibliography

[1] Ash, *Abstract Algebra: the Basic Graduate Year* Open for online access, 2000

[2] Kurzweil and Stellmacher, *The Theory of Finite Groups: An Introduction* New York: Springer-Verlag, 2004

[3] I. Martin Isaacs, *Finite Group Theory* Providence, Rhode Island: American Mathematical Society, 2008